Collection

Combating Tax-Related Identity Theft

By Carol M. Luttati

Overview

Identity theft, in general, and tax-related identity theft and refund fraud, in particular, have quickly become major areas of focus and concern for both the IRS and taxpayers alike. Tax-related identity theft occurs when a third-party surreptitiously uses a taxpayer’s stolen Social Security number to file a tax return in order to secure a fraudulent refund.¹

Currently, an ever-increasing amount of resources and manpower are being devoted by the Criminal Investigation Division (CI) of the IRS to investigating identity theft, as compared to pure criminal tax violations. The statistics confirm this upward trend. Whereas in 2010, the IRS identified 338,753 incidents of identity theft, this number grew to over 2.5 million by 2013. Indeed, by 2014, identity-theft investigations accounted for 24.7 percent—1,063 of the total 4,297 criminal investigations launched by the IRS.²

In 2014, CI’s enforcement efforts culminated in 748 sentencing, as compared to 438 in 2013—representing a 75-percent increase. Further, the incarceration rate for those convicted rose by 7.1 percent to 87.7 percent, with an average jail time in 2014 being 43 months versus 38 months in 2013.³

Between 2011 and October 2014, the IRS thwarted the processing of 19 million suspicious returns and safeguarded the erroneous issuance of more than $63 billion in fraudulent refunds.⁴ It did so utilizing its pre-refund fraud filters. For 2015 and the foreseeable future, tax-related identity theft will continue to be a top priority for the IRS.

Inasmuch as the stolen information that identity thieves use in attempting to obtain a refund comes, by and large, from security breaches that occur outside the tax system, the IRS, in many instances, may be the first party to inform the taxpayer that their identity has been compromised. Recently, a number of my clients have been contacted by the IRS for this very reason. Clients, who are unaware that their personal information has been compromised by a data breach, are often skeptical and question the authenticity of any purported communication from the IRS, believing it to be a bogus phishing scam. This column is intended to describe the manner in which the IRS is legitimately endeavoring to prevent tax-related identity theft aimed at claiming fraudulent refunds.

Carol M. Luttati is an Attorney in New York City specializing in federal and state civil and criminal tax controversies. Ms. Luttati is also Collections Liaison Chair of the ABA Tax Section’s Administrative Practice Subcommittee on Small Business/Self-Employed.
The Identity Protection PIN and Notices CP01A and CP01F

As an initial matter, clients should unequivocally know that under no circumstances does the IRS initiate taxpayer contact by e-mail, fax, text message or through social media. Taxpayers should report any unsolicited e-mail that claims to be from the IRS to phishing@irs.gov. To report phishing scams made by phone, fax or mail, taxpayers should call 1-800-366-4484. IRS impersonation scams can be reported to the Treasury Inspector General for Tax Administration. For additional information as to any questionable communication purportedly from the IRS, log onto irs.gov and enter the search phrase “Fake IRS Communications.”

How the IRS contacts taxpayers, with respect to identity theft, occurs as follows. The typical fact pattern begins with the taxpayer attempting to e-file his/her return. The IRS rejects the e-filing because another return, filed by the identity thief, was received and processed earlier in the filing season by the IRS under the taxpayer’s Social Security number. As a result, the taxpayer is issued Notice CP01A. Notice CP01A is generally sent to the following taxpayers:

- Those who themselves have reported that they have been the victim of identity theft
- Those whom the IRS has identified as being a victim of identity theft
- Those who participated in the IRS’s Identity Protection Personal Identification Number (IP PIN) Pilot Program for residents of Florida, Georgia or the District of Columbia

All taxpayers who receive a Notice CP01A must obtain an IP PIN. An IP PIN is a six-digit number assigned to eligible taxpayers that is designed to prevent the misuse of their Social Security number on a fraudulent federal income tax return—the Form 1040, U.S. Individual Income Tax Return; 1040A, U.S. Individual Income Tax Return; 1040EZ, Income Tax Return for Single and Joint Filers With No Dependents; or 1040 PR/SS. The IP PIN is assigned, on an annual basis, to victims of identity theft to use in filing their federal income tax returns. Its use establishes to the IRS that the taxpayer is the rightful filer of the return. For taxpayers who receive the Notice CP01A, their initial IP PIN is prominently set forth in bold in the Notice.

Taxpayers who instead receive a Notice CP01F may voluntarily, if they so choose, obtain an IP PIN. Unlike taxpayers who are issued a Notice CP01A, those who are issued a Notice CP01F are simply being invited to opt in and obtain an IP PIN because:

- their federal return for last year was filed showing an address in Florida, Georgia or the District of Columbia; or
- the IRS has identified their account as having indications of identity theft.

These taxpayers can secure their first IP PIN online at irs.gov by clicking on “Get an IP PIN.” Once a taxpayer has either been issued an IP PIN by the IRS or gone online to obtain an IP PIN, there is no opting out. The IP PIN must be used to confirm the taxpayer’s identity on his/her federal income tax return for the current year. Thereafter, every December, the IRS will mail the taxpayer an IP PIN, by mail, to use in filing his/her return for that year. Failure to use the IP PIN on an electronically filed return will result in the return being rejected. Failure to use the IP PIN on a paper-filed return will result in a delay in processing the return and in issuing any refund to which the taxpayer may be entitled.

The Form 14039 and Other Protective Measures

In addition to availing yourself of an IP PIN, taxpayers (1) who know or suspect that they have been the victim of tax-related identity theft, (2) who have received either a Notice CP01A or CP01F, (3) whose Social Security number has been compromised, or (4) whose e-filed return has been rejected, should also complete and submit to the IRS the Form 14039, Identity Theft Affidavit. The Form 14039 recites that it is to be used “if you are an actual or potential victim of identity theft and would like the IRS to mark your account to identify questionable activity.” Section A of the form requires all filers to specify one of two stated reasons for filing the form. The first reason states that you are the victim of identity theft and it is affecting your federal tax records (“Reason 1”). The second reason states that you have experienced an event involving your personal information that may, at some future time, affect your federal tax records (“Reason 2”). Besides checking the appropriate box that best describes why you are filing the...
and required documentation to (855) 807-5720. Beyond filing the Form 14039, the IRS encourages victims of identity theft to also take the following protective measures:

- File a police report.
- File a complaint with the Federal Trade Commission (FTC) at www.ftc.gov or the FTC Identity Theft Hotline at (877) 438-4338.
- Contact the three major credit card bureaus to place a "fraud alert" on your account:
  - Equifax—at www.equifax.com or (800) 525-6285
  - Experian—at www.experian.com or (888) 397-3742
  - TransUnion—at www.transunion.com or (800) 680-7289.
- Contact your financial institutions and close any accounts that were opened without your permission. Lastly, if you have already contacted the IRS and your matter has not been resolved, you can call the Identity Protection Specialized Unit at (800) 908-4490 for further assistance or the Taxpayer Advocate Service at (877) 777-4778.

**Final Thoughts**

Given the upsurge in cyber-security data breaches, safeguarding your personal tax and financial information, especially your Social Security number, is vitally important. Taxpayers have a variety of avenues at their disposal—both at the IRS and outside of the IRS—to protect themselves. By securing an IP PIN, filing the Form 14039 and taking advantage of the additional protective measures outlined above, taxpayers may avoid becoming victims of tax-related identity theft. Toward that end, heeding the IRS’s principal tip will greatly help—don’t readily give out your Social Security number just because it is asked for; only provide your Social Security number if you are legally required to do so. For more proactive tips IRS suggests taxpayers follow to reduce their risk of being the victim of identity theft, go to Publication 5027, Identity Theft Information for Taxpayers.

**ENDNOTES**

4. Id.
5. See IRS Pub. 5027, Identity Theft Information for Taxpayers.
7. See Understanding Your CP01A Notice.
9. Id., at Q&A 9.
10. See Understanding Your CP01F Notice.
11. See Frequently Asked Questions about the Identity Protection Personal Identification Number at Q&A 14 and 15.
12. See Understanding Your CP01A Notice, Understanding Your CP01F Notice.

**Practice**

**Summary**

In civil tax audits that include potentially sensitive issues, counsel will often engage a team of representatives, including a forensic accountant. The protections afforded by Code Sec. 7525 are not available when truly needed the most—when a civil tax proceeding moves into the criminal arena. It also may not be available in state-related tax proceedings or nontax civil litigation. Although Code Sec. 7525 extends...