Crowell

CLIENT ALERT

Act Now to Protect Against Tax-Related Liabilities for Identity Theft

December 6, 2013

Tax identity theft is rampant and can create significant costs for businesses. First, companies may be liable to the individual victims for careless handling of their personal information. Second, the companies may themselves be the victims of identity theft. This client alert discusses how the problems arise and what companies can do to minimize their exposure. This is the time to act, because a new round of thefts is certain to begin with tax filing season in January. This could also be a good time to improve communications among the legal, information systems, accounting, and tax functions on this subject.

Individual Tax Identity Theft and Corporate Liability

Individual identity theft can occur when the thief acquires personal information (e.g., name and Social Security number) to file a tax return in the name of the victim. Income and deduction figures are made up, a fake Form W-2 is attached to support the income and tax withheld reported on the return, and a refund is claimed. Often, these returns are filed early in tax filing season,[1] before the IRS has received Form W-2 information (which is sent to the Social Security Administration, not the IRS) from employers. Thus, the IRS cannot verify the income and tax withholding information on the false tax return when the refund is made.[2] Although the IRS has established numerous filters to detect false returns,[3] many still slip through, and the claimed refunds are diverted to the thief.

When the real taxpayer tries to file later, he or she is informed by the IRS that a return has already been received. This begins a sometimes arduous process of establishing that the first return was false. Although the taxpayer may eventually receive a refund, this can take more than a year,[4] during which the taxpayer invests his or her own time, incurs costs and may become quite distressed. Treasury Inspector General for Tax Administration (TIGTA) estimated that the IRS mistakenly refunded over $4 billion on false returns that were either filed in the name of taxpayers who had no actual filing requirement or were filed prior to the legitimate return.[5]

A company may be at risk for liability if it is determined that the identity thieves obtained the personal information from the company. For example, the United States Court of Appeals for the Sixth Circuit recently held that, under Michigan law, a company could be liable to its customers for economic damages and emotional distress if false tax returns were filed as a result of its negligent handling of personal information.[6] Similarly, a class sued a firm when an employee stole personal information for the purpose of filing false refund claims.[7]

Corporate Identity Theft

Businesses are themselves at risk of "identity" theft through fraudulent use of their Employer Identification Numbers (EINs). These numbers are freely available for publicly traded corporations through their filings with the Securities and Exchange Commission. For private companies, they are available to recipients of Forms W-2 and 1099, and they may also be available from other sources.

Identity thieves misuse these EINs by including them on the false Forms W-2 filed with fraudulent individual tax returns. TIGTA found that for the 2011 tax year, 285,670 EINs were stolen for use on 767,071 false returns claiming over $2.2 billion in refunds.[8] Years later, the IRS may reconcile withholding reported on Forms W-2 with the withholding reported on the company's own employment tax return, Form 941. The sum of the Form W-2 amounts will be greater because of the false filings. At that point, the IRS may send the company a bill for the difference, plus interest and penalties. The company often will have limited resources to pursue this issue and may not realize that it is the victim of fraud. It may assume that some errors are inevitable in a large payroll operation and that the IRS is correct, and may simply pay the amount that the IRS asserts is due.

Additionally, instances have been reported in which EINs have been misused to file a return claiming a refund directly in the name of the victimized corporation.[9]

What You Can Do

With regard to individual identity theft, the first step, of course, is to take reasonable measures—through policies, procedures and technologies—to assure that personal information in your possession is not compromised.

Second, the IRS has proposed regulations permitting the truncation of Social Security numbers on copies of some types of information returns that are provided to payees.[10] This may be a "best practice," to the extent permitted by the IRS, to prevent identity theft in case the information returns are stolen in the mail. Although the proposed regulations have not yet been adopted, the IRS has issued instructions for many information returns[11] to be filed in the beginning of 2014 (and relating to the 2013 year) that permit truncation. At present, full Social Security numbers are required by law on Forms W-2 and may not be truncated. However, there are pending proposals to permit truncation of Social Security numbers on W-2 forms.[12]

Third, the IRS has introduced an informal program to help alleviate fraud, by invitation only, to ask very large employers to provide the IRS with Form W-2 information as soon as it is available.[13] This permits the IRS to compare that information with filed tax returns before issuing refunds. However, there are several potential complications with the proposed program. First, the IRS historically has made its requests for the Form W-2 information by fax. For security purposes, any participant invited to join should confirm through IRS channels that such a fax is legitimate and does not come from an imposter.[14] Also, there is potential risk of liability to the individuals if the business voluntarily provides sensitive personal information to the IRS in a situation where it is not legally required to do so. Finally, the business must consider how this sensitive information can be secured in transit; encryption could be mandated by some state laws, and is certainly the developing standard when it comes to transmission over the Internet.

Fourth, businesses should be alert to the fact that their own identities might have been stolen through misuse of their EINs. Companies should confirm that their tax and payroll departments are aware of this issue and are devoting appropriate resources to any IRS notices claiming that tax was underpaid.

---

[1] IRS Publication 4535, *Identity Theft Prevention and Victim Assistance* (2012).

[2] In 2011, the IRS issued 50% of refunds by the end of February, but had received only 3% of information returns by that time. *Tax Refunds: IRS Is Exploring Verification Improvements, but Needs to Better Manage Risks*, U.S. Government Accountability Office, GAO-13-515 (2013).

[3] For the 2012 year, the IRS stopped refunds on 1.8 million identity-theft tax returns claiming $12.1 billion in refunds. Treasury Inspector General for Tax Administration (TIGTA), *Detection Has Improved; However, Identity Theft Continues to Result in Billions of Dollars in Potentially Fraudulent Tax Refunds*, Reference No. 2013-40-122 (2013).

[4] TIGTA, *Most Taxpayers Whose Identities Have Been Stolen to Commit Refund Fraud Do Not Receive Quality Customer Service*, Reference No. 2012-40-050 (2012).

[5] *Examining the Skyrocketing Problem of Identity Theft Related Tax Fraud at the IRS: Before the Subcomm. on Government Operations of the H. Comm. on Oversight and Government Reform*, 113th Cong., 1st Sess. (2013) (statement of Michael E. McKenney, Acting Deputy Inspector General for Audit, TIGTA).

[6] *Stacy v. HRB Tax Group, Inc.*, No. 11-2012 (Mar. 6, 2013). Although the case involved a tax preparation firm, any business might be liable under the court's rationale; *see Andrews v. Medical Excess, LLC*, 863 F. Supp. 2d 1137 (M.D. Ala. 2012) (dealing solely with federal jurisdiction, but plaintiffs alleged liability against an insurance company). *Compare Harmon v. H&R Block Tax and Business Services, Inc.*, No. 4:13CV116 JCH (E.D. Mo., Apr. 24, 2013) (Block held not liable for identity theft by employee).

[7] *Identity Thieves Infiltrated Tax Office in Bronx, a Suit Says*, The New York Times, April 8, 2010.

[8] TIGTA, *Stolen and Falsely Obtained Employer Identification Numbers Are Used to Report False Income and Withholding*, Reference No. 2013-40-120 (2013).

[9] http://www.itworld.com/it-managementstrategy/293399/despite-warnings-most-states-slow-confront-corporate-id-theft

[10] *See* REG-148873-09, 2013-7 I.R.B. 494, 78 Fed. Reg. 913 (2013), *corrected*, 78 Fed. Reg. 6273 (2013). The proposed regulations would extend a prior truncation pilot program; *see* Notice 2011-38, 2011-20 I.R.B. 785.

[11] E.g., Form 1099 instructions available at http://www.irs.gov/pub/irs-pdf/i1099gi.pdf.

[12] *Summary of Staff Discussion Draft: Tax Administration, S. Comm. on Finance*, 113th Cong., 1st Sess. (2013). The proposal would also require Forms W-2 and 1099 to be filed with the government by February 21, rather than the current filing date (March 31 for electronic filing).

[13] In 2012, there were 999 businesses in this program. That year, the program identified 92,616 fraudulent returns claiming refunds of over $400 million. TIGTA, supra note 8.

[14] The Treasury testimony, supra note 5, referred to a criminal posing as an IRS agent to gain access to confidential information, used to file false returns, from a company.

IRS Circular 230 Disclosure: To comply with certain U.S. Treasury regulations, we inform you that, unless expressly stated otherwise, any U.S. federal tax advice contained in this communication, including attachments, was not intended or written to be used, and cannot be used, by any taxpayer for the purpose of avoiding any penalties that may be imposed on such taxpayer by the Internal Revenue Service. In addition, if any such tax advice is used or referred to by other parties in promoting, marketing or recommending any partnership or other entity, investment plan or arrangement, then (i) the advice should be construed as written in connection with the promotion or marketing by others of the transaction(s) or matter(s) addressed in this communication and (ii) the taxpayer should seek advice based on the taxpayer's particular circumstances from an independent tax advisor. To the extent that a state taxing authority has adopted rules similar to the relevant provisions of Circular 230, use of any state tax advice contained herein is similarly limited.

Howard M. Weinman is admitted to practice only in the District of Columbia and before the Internal Revenue Service. Practice limited to matters before the Internal Revenue Service.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Jeffrey L. Poston
Partner – Washington, D.C.
Phone: +1.202.624.2775
Email: jposton@crowell.com