Wolters Kluwer CCH
IntelliConnect® Faster Answers, Better Results
May 13, 2013

TAX NEWS AND HIGHLIGHTS
Reprinted with permission from FEDERAL TAX DAY (May 13, 2013)

ABA MAY MEETING: Business Identity Theft Results in $50 Billion in Losses Per Year; EINs Too Easy to Find

The impact of taxpayer identity theft on businesses is a growing problem often overshadowed by the intense discussion of individual identity theft, said panelists during a May 10 session of the 2013 May Meeting of the American Bar Association's Section of Taxation in Washington, D.C. Fraudulent usage of employer identification numbers (EINs) and other employer information resulted in approximately $50 billion of losses to small businesses and consumers nationwide in 2012, said panelist Claudia Hill, EA, TaxMam, Inc., and Editor in Chief of CCH's *Journal of Tax Practice and Procedure*. Because the various processes and offices set up to assist victims of identity theft are mainly focused on assisting individual taxpayers, victimized businesses may be left in the dark about how to rectify the situation. "In each case, when you try to notify the IRS of identity theft, they are still only set up for individuals. And so, there isn't a system as there is for individuals for entities to use to come forward," Hill said. Nevertheless, she stated that the IRS could be very helpful. "It's just that there's no system set up. There's no tracking."

The IRS has taken some steps to prevent EIN fraud, panelists said. However, in some cases, these measures prove ineffectual or serve mainly prevent fraud perpetrated against larger businesses, which are victimized on a larger scale than small businesses. Panelists suggested several best practices that small business practitioners can follow first to prevent EIN theft or, if it has already occurred, to try to resolve the issue with the IRS.

How EIN Fraud Is Perpetrated

Identity thieves steal EINs for purposes such as filing false tax returns in the employer's name to obtain a refund, obtaining a loan, setting up a credit card account or filing false Forms W-2 that report withholding from the fabricated income of individual taxpayers whose identities will be used on fraudulent individual tax returns filed to obtain refunds.

"EINs are easy to obtain," said Hill. Thieves may obtain them from Forms W-2 sent to employees and then discarded without being shredded, said Maxine Aaronson, attorney, Dallas, Tex. "That EIN is on every single employee's W-2. And the employer can't control what the employees do with their copies of the Form W-2," said Aaronson.

EINs are also publicly available on many Securities and Exchange Commission (SEC) documents, such as the Form 10-K or annual reports. "There are cases out there where criminals were going to the prison library, researching publicly held companies and getting out of their annual reports their EINs," Aaronson said.

Other sources include public databases, for example, those hosted by the Secretary of State, or private databases, such as Guidestar.org. which houses information on net profits and salaries of nonprofit companies. Thieves may even be able to obtain an EIN from the IRS website database of public charities or to steal one from a legitimate source, such as a Form W-9.

Once a criminal has an EIN, he or she can create a similarly named entity and/or change the entity's address, then use the EIN to apply for a loan or credit, or commit credit card processing fraud, or file false Forms W-2 in preparation for a larger tax filing fraud scheme involving individual taxpayers.

What the IRS Is Doing

"The EIN is controlling tax activity not just in the IRS accounts but, if you go to a state department of revenue website, every one of them posts warnings about their tax scams and their problems with EINs," said Debera Salam, director, Payroll Information and Process Services, Ernst & Young LLP. Salam mentioned that the IRS had established a matching and verification program under which the Service would suspend any potentially suspicious Forms 1040. Salam explained that, under the program, the IRS would proactively identify large companies that would potentially become victims of EIN theft and ask them for a copy of their Forms W-2 early in the year before they file with the Social Security Administration. The IRS would have the actual employer W-2 file and would run all the suspicious 1040s against the W-2 file to see if there was any indication that someone had stolen the employer's W-2 file. "That is a wonderful program," said Salam. "Unfortunately, there is no information out on the website. There is no way for a company to say, "Hey, I'm vulnerable; I want to volunteer.""

National Taxpayer Advocate Nina Olson stated that the program had been in existence for several years. However, the IRS lacks the manpower and budgetary resources to extend the program to small businesses. "We lost $1 billion from our budget since 2010…and there just aren't the human beings to do that work," Olson said.

Best Practices

Businesses could take numerous precautions to prevent EIN theft, panelists said. Olson advised small businesses that had hire payroll companies to check the IRS Electronic Federal Tax Payment System (EFTPS) to verify that the payroll company had actually made the payments. "It's very important for your clients to check regularly," she said. "Check that those payments have in fact been made. That's another way of just making sure that, even if this entity looks very reputable, that they're not doing something with your payments and embezzling them."

Aaronson referred businesses to the Business Identity Theft Resource Guide published by the Colorado Secretary of State. The guide suggests several best practices for businesses seeking to protect both themselves and their clients. Among them:

- Shred unnecessary business records to prevent identity theft from taking place offline;
- Keep documents and records in a secured location, possibly in a locked filing cabinet;
- Sign up to receive electronic alerts from bank accounts, credit cards and other parties;
- Do not share EINs with unverified parties;
- Do not send unencrypted financial documents, account numbers, or other taxpayer information through the Internet; and
- Monitor your business's credit report.

If a business does find that its EIN has been stolen, Hill suggested to still notify the IRS. "Go through the normal process that you would for the individual," she advised.

Hill suggested first contacting the IRS Accounts unit to make sure that the returns filed using the EIN were correct. Next, she recommended going to the EIN unit, which is responsible for issuing the EINs in the first place, and have an alert put on the account. Third, she suggested using the Form 14039, Identity Theft Affidavit, used by individual identity theft victims, but indicating on the form that it concerns entity identity theft. Fourth, Hill stated the business should contact the Federal Trade Commission (FTC) and look at the resources on the FTC website.

If possible, a victim should fill out a police report. Hill acknowledged, however, that many local law enforcement officials do not generally pay much attention to an identity theft claim. "Many local municipalities don't have extra resources to take a police report when they believe there is no crime that has been committed

against you because it hasn't hit your pocket yet," she said. Finally, Hill suggested that a business change its EIN at the end of the fiscal year. "You don't change your EIN in the middle of a tax year," she said.

Salam reminded businesses that the IRS had just issued final regulations requiring EIN holders to provide updated information to the IRS (TAXDAY 2013/05/06, I.1). The regulations are intended to help the IRS obtain and maintain more accurate information on employers. ■

By Jennifer J. Rodibaugh, CCH News Staff