BOTZ, DEAL & COMPANY, P.C.
CERTIFIED PUBLIC ACCOUNTANTS AND ADVISORS
TWO WESTBURY DRIVE • ST. CHARLES, MO 63301 • (636) 946-2800 • FAX (636) 946-2975
4 EAST PIERCE BLVD. • WENTZVILLE, MO 63385 • (636) 332-8299
318-C MID RIVERS MALL DRIVE • ST. PETERS, MO 63376 • (636) 397-5200

Business Identity Theft, Tax Consequences And Best Practices

Facilitated by the speed, ubiquity, and anonymity of the Internet, criminals are able to easily steal valuable information such as Social Security numbers and use it for a variety of nefarious purposes, including filing false tax returns to generate refunds from the IRS. The victims are often unable to detect the crime until it is too late, generally after the IRS receives the legitimate tax return from the actual taxpayer. By that time the first return has often been long accepted and the refund processed. Because of the ease, speed, and difficulty involved in policing cybercrime, identity theft has grown rapidly. One estimate from the National Taxpayer Advocate Service has calculated that individual identity theft case receipts have increased by more than 666 percent from fiscal year (FY) 2008 to FY 2012.

There is, however, another dangerous facet of identity theft that costs the government, taxpayers, and businesses millions of dollars each year. That is business identity theft, which like its consumer counterpart involves the theft or impersonation of a business's identity. To add insult to injury, business identity theft can have crippling federal tax consequences. The following summarizes the problem of business taxpayer identity theft, the methods employed by thieves, and the means by which you can protect your business.

Business v. Individual Identity Theft

Businesses generally deal with larger transactions, have larger account balances and credit lines than individual taxpayers, and can set up and accept merchant credit card payments with numerous banks. Business information regarding tax identification numbers, profit margins and revenues, officers, and even officer salaries are often public and easily accessed. At the same time remedies and enforcement tend to focus more on individual identity theft. Thus, business identity theft can be more lucrative and arguably less dangerous to engage in than individual taxpayer identity theft.

Methods Used

Only some of the many business identity theft schemes relate to tax. Nevertheless, such schemes can be devastating for businesses, resulting in massive employment tax liabilities for fictitious wages or huge deficiencies in reported income. Identity thieves can use a business's employer identification number (EIN) to initiate merchant card payment schemes, file false tax returns, and even generate hundreds of fake Form W-2s in furtherance of more individual taxpayer identity theft. Some examples of schemes are described below, but they are by no means an exhaustive list:

Example

The owners of a business dissolved it. Subsequently identity thieves reinstated the business and filed a tax return in its name, on which they claimed a $140,000 fuel aviation tax credit and obtained a tax refund. The actual business owner discovered the scheme after the IRS sought the return of the refund.

Example

Criminals stole a restaurant franchise's EIN and used it to create 100 fake Form W-2s, reporting to the IRS approximately $4 million paid in salaries. The thieves used the fake Form W-2s to file individual tax returns and claim fraudulent refunds. Meanwhile, after the IRS saw the W-2s, it assessed a deficiency against the restaurant franchise for $800,000 in unpaid payroll taxes.

Example

Criminals set up more than 100 fake businesses, with names similar to legitimate businesses and mailing addresses located within the same vicinity to avert suspicion. After establishing merchant payment accounts with local banks, they began making thousands of small charges from stolen credit cards. When it came time for the local banks to prepare their Forms 1099-K, Payment Card and Third Party Network Transactions, the thieves produced the legitimate business's name, address, and EIN. Since the actual businesses had no knowledge of what turned into more than $9.5 million in total credit card income generated over a four-year period, none of the legitimate businesses included the amounts on their tax returns for those years.

How They Do It

Business identity theft can require less effort than individual identity theft because less information is required to establish a business or open a line of credit than is required of individuals. In general, the thief needs to obtain the business's EIN, which is easy to acquire. Common sources for an EIN include:

- Filings made to the Securities and Exchange Commission (SEC) such as the Form 10-K, which includes the EIN on its first page;

- Public databases that enable users to search for business entities sometimes also display the employer's EIN;
- Websites specifically designed to search for EINs, such as EINFinder.com;
- Business websites sometimes openly display the EIN; and
- Forms W-2, W-9, or 1099.

The problem presented by issuing paper copies of W-2s or 1099s is that you hand these things out—in some cases by the thousands to employees—and you don't have any control on whether or not they safeguard the information that is on it. When they put themselves at risk they are also putting their employer at risk.

Once a thief has the EIN, he or she may file reports with various state Secretaries of State to change registered business addresses, registered agents' names, or even appoint new officers. In some cases the thief will apply for a line of credit using this new information. Since the official Secretary of State records display the changed information, potential creditors will not be alerted to the fraud. In one case, however, criminals changed the names of a business's officers by filing with the Secretary of State's office and then sold the whole business to a third party. In the end, however, once an identity thief has established a business name, EIN, and address information, he or she has all the basic tools necessary to perpetrate business identity theft.

Best Practices

Businesses should also review their banks' policies and recommendations regarding fraud protection. They should know what security measures are being offered and, if commercially reasonable, take them. In a recent U.S. district court case from Missouri, the court found that a bank was not liable for a fraudulent $440,000 wire transfer because it had offered the business a commercially reasonable security procedure, and the business had rejected it. The decision cited Uniform Commercial Code Article 4A-202(b), as adopted by the Missouri Code. Many other states have also adopted the UCC, meaning victimized businesses might find themselves without recourse against their banks in the event of a large fraudulent wire transfer.

It is recommended that businesses monitor their accounts on a daily basis and follow up immediately on any suspicious activity. Enroll in email alerts so that you would immediately be apprised of any change in your account name, address, or other information. Monitor the information on your business's registration frequently, whether or not your business is active or inactive. A lot of people don't go through the formal dissolution process, which terminates all of the corporate authority, and instead they let the charter get forfeited by the Secretary of State. Forfeited charters are pretty easy to reinstate. Those are the ones most susceptible to hijacking,

After Fraud Occurs

If it is too late, and a fraudulent transaction has occurred in your business's name, take immediate action by contacting your bank, creditors, check verification companies, and credit reporting companies. Report the crime to your local law enforcement authorities and your state's secretary of state business division. Finally, whenever possible, memorialize all correspondence in writing and keep it in your records.

Business identity theft schemes can be devastating for businesses, resulting in massive employment tax liabilities for fictitious wages or huge deficiencies in reported income.