COAN, PAYTON & PAYNE, LLC
ATTORNEYS AT LAW

Business identity theft: Is your company's EIN safe?

By: Daniel W. Jones, Esq.
Coan, Payton & Payne, LLC

This article was originally published in the November 15, 2013 Guest Column Section of BizWest.

To combat identify theft, most of us have learned to be very careful with our personal information. We are protective of our individual bank statements, credit card information and Social Security numbers.

Similarly, most businesses are aware of the need to thoroughly protect their customers' personal information. Televised stories of misplaced laptop computers and hacked databases from banks, government agencies and merchants remind us all of the need to protect information that can subject clients to identity-theft concerns. Security failures pose threats not only to clients, but also to the reputation of any business from which such information is obtained.

It is critical that businesses not forget that they too can have their identities stolen. Business identity theft is an increasingly common development, one which can take several forms. Even relatively "small" cases of business identity theft can have potentially catastrophic results for businesses. Online searches for the phrase "business identity theft" pull up pages of stories.

For example, a couple's business was a victim of identity theft when a criminal wrote fraudulent checks where the name and address of the couple's business appeared on some of the checks possessed and passed by the criminal. The account number on the checks actually did not belong to the business, and the bank account of the business had not actually been attacked.

While relieved to find that their business's bank account had not been drained, the couple soon found that because fraudulent checks totaling in excess of $12,000 had been written in the name of their business, check verification companies such as Telecheck had blacklisted their business. They were required to fill out countless forms and police reports detailing each forged check before they could get their business removed from the blacklists. The potential harm to reputation and the time required to make things right could be a devastating blow to a fledgling or otherwise struggling business.

Other criminals may attempt to obtain credit by stealing the Employer Identification Number of a business, creating and even recording false corporate documents such as authorizations to act on behalf of the business, and then using that information to obtain merchandise, credit cards or lines of credit in the victim company's name. Small businesses can be a great avenue to realize criminal gains. Business owners can have access to larger credit lines than individuals, and can be slower to realize and resolve a problem.

For example, a law firm in San Diego found that criminals had moved into its building, ordered and received $70,000 worth of computers and furniture in its name, hired a moving truck and disappeared before the law firm actually received the bill. In a different extreme case in 2006, authorities overseas discovered a sophisticated ring of criminals who had established a

complete counterfeit NEC-branded company, including more than 50 factories producing a full line of counterfeit NEC products. The factories even boldly displayed the NEC name. Thankfully for NEC, the counterfeit products were not so inferior as to create havoc for their reputation, but the counterfeit operation certainly succeeded in stealing a great deal of income from the legitimate company. Had the counterfeit products been substantially inferior, it could have been disastrous for NEC.

Colorado's secretary of state and attorney general have worked to warn businesses about identity theft risks. Together with the ID Theft Unit from the Colorado Bureau of Investigation, they also have prepared the "Business Identify Theft Resource Guide – A Guide to Protecting Your Business and Recovering from Business Identity Theft." This guide can be found online at www.sos.state.co.us/pubs/business/ProtectYourBusiness/BITresourceguide.html.

A particular area of concern for all business owners that I wish to highlight here involves the secretary of state's system for receiving business records. Nearly all of the business-related forms required by the secretary of state now are submitted online. The secretary of state's office has warned that since the system relies on the honesty of those submitting documents it can be abused by criminals who enter false records for existing businesses to give themselves the appearance of propriety when applying for credit or completing other transactions with unsuspecting third parties.

Because most business owners check the accuracy of their records at the secretary of state's office only rarely (for example, perhaps only once each year when submitting an Annual Report), a business record revised by a criminal might go unnoticed for months. Additionally, such revised records might create problems for the actual business owners if clients or lenders check the site.

Fortunately, business owners may monitor any changes made to their online records by receiving automatic email notification whenever any change is made to a business's record. The system does not limit the number of persons who can be notified in the event of a change to your business's online records. Additionally, the secretary of state's office also now permits businesses to set up "Secure Business Filing" accounts, where the online business record is password-protected, providing additional control over who is able to make changes.

To subscribe to the email notification system or to set up a Secure Business Filing account, there are links to do so within the Business Identity Theft Resource Guide described above.

In any event, I encourage you to educate yourself further about the threats identity thieves pose to businesses, and to review the resource guide to become familiar with ways to prevent suffering the untold harms identity thieves can cause you.

Daniel W. Jones, Esq. is an attorney at Coan, Payton and Payne, LLC. He can be reached at 970-339-3500 or djones@cp2law.com.