INSIGHTS + NEWS

Client Alert: Employers Beware: 'Tis the Season for Data Theft

DECEMBER 18, 2018

Because cybercriminals don't take holidays, December is an appropriate time for all employers to take steps to protect tax data and identities (both their own and their employees') in advance of the 2019 tax-filing season. Earlier this month, the IRS hosted "**National Tax Security Awareness Week**," issuing press releases and updated publications with data-protection tips for taxpayers, tax professionals and businesses, and launching a special @IRSTaxSecurity Twitter handle to keep the public aware of emerging threats.

EMPLOYERS CAN BE VICTIMS OF IDENTITY THEFT, TOO.

The crime of identity theft may victimize businesses as well as individuals. Fraudsters steal business return data (such as EINs) to submit fraudulent corporate returns, such as Forms 1120 and 1120S, or fraudulent information documents, such as W-2s and 1099s, to support fraudulent individual return filings. If the compromised business return data includes Schedule K-1 links, criminals may also use the K-1 shareholder information to file fraudulent individual returns. In the past year, the IRS has noted a sharp increase in the number of fraudulent Forms 1120, 1120S and 1041, as well as Schedules K-1.

E-MAIL PHISHING SCAMS ARE THE MOST COMMON TACTIC USED BY CRIMINALS TO STEAL DATA.

E-mail is the most common tool that cybercriminals use to dupe people into sharing sensitive information, whether by posing as a trusted party and tricking the recipient into responding to the e-mail with certain information, or by inducing the recipient to click on a hyperlink or open an attachment that installs data-mining malware on the computer network. One particularly insidious **recent e-mail phishing scam** disguises an e-mail to make it appear as if it is from an organization executive and sends it to employees in the payroll or human resources departments, including a request to send a list of all employees and their Forms W-2.

EMPLOYEE EDUCATION IS CRITICAL IN PREVENTING A DATA BREACH.

Employees are ultimately your first line of defense against potential data breaches, but they may not realize that protecting business information and the security of your company network also means protecting their personal information as well. Businesses should educate their employees, including their HR and payroll staff, to spot and report any suspicious e-mails and to not respond to them, click on any links within them, or open any attachments they contain. The IRS recommends that businesses share **Publication 4524** with employees to provide some basic data security tips, and also maintains a **list of phishing and other schemes** perpetrated using the IRS name or logo for reference. As a reminder, the IRS does not initiate contact with taxpayers by e-mail, text messages, or social media channels to request personal or financial information.

GUIDANCE IN THE EVENT OF A BREACH.

The Federal Trade Commission has compiled some useful **guidance** for businesses responding in the aftermath of a data breach. Having a good plan in place in the event of a breach is important and can prevent an already troublesome situation from becoming even worse.

