KING & SPALDING

# Client Alert

Business Litigation Practice Group
Data, Privacy & Security Practice Group

February 7, 2017

## Employees Expecting Tax Refunds? So Are Your Hackers

With the beginning of the 2016 tax season, employers should be on high alert for the wave of W-2 spear phishing scams coming their way once again this year. Companies that fall victim to this type of scam likely will be faced with the unauthorized disclosure of their employees' W-2 information, which can result in a host of legal obligations, potential fraudulent tax returns filed in the names of their employees, a decrease in employee confidence and morale, as well as potential class actions.

### What Are Spear Phishing Scams?

This time last year, HR and payroll professionals across the country received spoofed e-mails designed to look like they were being sent by company executives who were asking for payroll data. These spoofed e-mails were typically framed as a request for W-2 forms, which contained social security numbers and other sensitive personal information. The fraudsters then used the information to submit false 2015 tax returns in order to steal tax refunds.

### Federal Agencies Raising Awareness

The IRS expects that this year will be even worse. On January 25, 2017, the IRS renewed its 2016 alert to HR and payroll professionals to be aware of the W-2 spear phishing scam, noting that in the first few weeks of the New Year the IRS already has received new notifications that the scam is once again making its way across the nation. In its alert, the IRS warned that these phishing e-mails may contain, for example, the actual name of the company Chief Executive Officer, and may contain messages such as:

- Kindly send me the individual 2016 W-2 (PDF) and earnings summary of all W-2 of our company staff for a quick review.

- Can you send me the updated list of employees with full details (Name, Social Security Number, Date of Birth, Home Address, Salary).

- I want you to send me the list of W-2 copy of employees wage and tax statement for 2016, I need them in PDF file type, can you send it as an attachment. Kindly prepare the lists and email them to me asap.

For more information, contact:

**Phyllis B. Sumner**
+1 404 572 4799
psumner@kslaw.com

**Nicholas A. Oldham**
+1 202 626 3740
noldham@kslaw.com

**Elizabeth D. Adler**
+1 404 572 3555
eadler@kslaw.com

**King & Spalding**
***Atlanta***
1180 Peachtree Street, NE
Atlanta, Georgia 30309-3521
Tel: +1 404 572 4600
Fax: +1 404 572 5100

**King & Spalding**
***Washington DC***
1700 Pennsylvania Avenue , NW
Suite 200
Washington, DC 20006-4707
Tel: +1 202 737 0500

**www.kslaw.com**

Relatedly, the FTC marked the week of January 30 to February 3 Tax Identify Theft Week. In conjunction with the IRS, the Department of Veterans Affairs, and the AARP Fraud Watch Network, the FTC offered several webinars, Twitter chats, and resources to companies, tax professionals, and consumers to raise awareness of the rise of stolen tax information and the filing of fraudulent tax returns.

Reflecting the fear and urgency relating to the scam, on February 2, 2017, the IRS issued a second "urgent alert" that scammers have expanded beyond the corporate world to school districts, tribal organizations, nonprofits, restaurants, staffing agencies, and healthcare organizations. In short, any organization that has payroll data is a target. The IRS also noted that the scammers are coupling their efforts to steal employee personal information with a follow-up fake e-mail from an "executive" to payroll requesting a wire transfer; combining the W-2 spear phishing scam with another ubiquitous fraud—colloquially known as the business e-mail compromise—in order to maximize theft from companies.

W-2 information is gold in the cyber underworld because the data can be used to commit identity theft in a variety of ways, over and over again. In addition to using the stolen information to file fraudulent tax returns, stealing your employees' refunds before they even have a chance to file a return, hackers also use the information to obtain loans or for proof of employment. Recent reports have shown that the stolen employee information often is posted for sale on the dark web, allowing even more criminals to access and use the information.

**What Can You Do?**

Companies should take immediate preventive security measures this tax season, including by restricting access to sensitive employee data and educating HR and payroll employees through information security awareness programs that highlight the importance of double-checking before sending any sensitive employee information. Companies need to also make sure that their information security programs require that any sensitive employee information be encrypted, especially before it is sent to another person through e-mail.

Should you find yourself the unfortunate victim of a W-2 spear phishing scheme, here are some initial, emergency steps to take:

- Contact experienced data security counsel who have handled W-2 spear phishing incidents and can quickly, efficiently, and effectively help you comply with your legal obligations and reduce your liability exposure.
- Initiate a privileged investigation to understand what happened and why.
- Review third party contracts that may impact your legal obligations.
- Contact the IRS criminal investigation division, which can help you take steps to protect employees' IRS accounts and assist with state tax authorities notifications.
- Protect your employees and comply with statutory notification obligations, including advising employees on steps they can take to prevent identity theft. These steps may include monitoring credit reports and account activity, filing an identity theft affidavit (IRS Form 14309) with the IRS, and taking steps to protect social security benefits, retirement plan accounts, and health care benefits.

W-2 spear phishing schemes are decidedly low-tech, but highly effective means for cybercriminals to steal sensitive personal information about your most valuable assets. Such low hanging fruit for criminals can lead to high costs for companies, both from a legal and reputational perspective, not to mention the impact on employees of fraudulent tax returns. This fraud scheme is not new – all companies should be aware and prepare.

**King & Spalding's Data, Privacy & Security Practice**

With more than 60 Data, Privacy & Security lawyers in offices across the United States, Europe, and the Middle East, King & Spalding is able to provide substantive expertise and collaborative support to clients across a wide spectrum of industries and jurisdictions facing privacy and cybersecurity-based legal concerns. We apply a multidisciplinary approach to such issues, bringing together attorneys with backgrounds in corporate governance and transactions, healthcare, intellectual property rights, complex civil litigation, e-discovery, government investigations, government advocacy, insurance recovery, and public policy. Our Data, Privacy & Security Practice has unparalleled experience in areas ranging from providing regulatory compliance advice, to responding to security incidents including data breaches and cybersecurity incidents, interfacing with stakeholders and the government, engaging in complex civil litigation (such as class actions), handling state and federal government investigations and enforcement actions, and advocating on behalf of our clients before the highest levels of state and federal government.

* * *

*Celebrating more than 130 years of service, King & Spalding is an international law firm that represents a broad array of clients, including half of the Fortune Global 100, with 900 lawyers in 19 offices in the United States, Europe, the Middle East and Asia. The firm has handled matters in over 160 countries on six continents and is consistently recognized for the results it obtains, uncompromising commitment to quality and dedication to understanding the business and culture of its clients. More information is available at www.kslaw.com.*