HUNTON ANDREWS KURTH

Lawyer Insights

March 4, 2019

It's Time to File Taxes—and Protect Tax Information

By Paul M. Tiao and Eric Hutchins

Published in Legaltech News

Theft of W2s and other tax information has become an annual occurrence. Companies need to not only to prevent such breaches from occurring, but also to position themselves to act quickly to protect their employees.

It's 5:00 on a Friday evening in a human resources division. An employee receives an email from his supervisor demanding that W2 "Wage and Tax Statements" forms for all executives and managers be sent to her immediately. The email's urgent tone is not typical of the supervisor. But mindful of upcoming performance reviews and thinking about weekend plans, the employee dutifully sends the W2s anyway.

Not long after, the company's CEO and general counsel attempt to file their personal taxes, only to learn from the Internal Revenue Service (IRS) that tax returns have already been filed in their name. An urgent investigation reveals that the email from the "supervisor" was actually a phishing email with a spoofed email address from an untraceable IP address. Worse, unknown assailants are now filing fraudulent tax returns on behalf of senior executives, and collecting inflated refunds in their names.

With tax season now here, this scenario has almost certainly played out in multiple companies across the country. W2 breaches can cause employers significant harm by undermining employee trust. They are even more damaging for employees. W2s contain sensitive personal information that can be subject to tax fraud, as well as other forms of identity theft, such as social security fraud.

Unfortunately, theft of W2s and other tax information has become an annual occurrence. Companies need to understand this trend, not only to prevent such breaches from occurring, but also to position themselves to act quickly to protect their employees.

Sophisticated social engineering techniques are central to most W2 breaches. Cyber-criminals carefully research targets before sending "spear-phishing" emails to trick employees into unwittingly disclosing W2s. These emails commonly purport to be from actual company employees, with addresses that may even look as though they come from employees' specific managers. They are often sent with a sense of immediacy to pressure the target into disclosing the requested information.

Companies should train their employees, particularly those identified as handling confidential or sensitive information, to recognize and avoid falling victim to these tactics. This could be part of a coordinated company phishing training program designed to reduce employee click rates on fraudulent email.

It's Time to File Taxes—and Protect Tax Information
By Paul M. Tiao and Eric Hutchins
Legaltech News | Month 4, 2019

Cyber threat vectors are relentless. Companies must also prepare to quickly respond to a breach, whether it be loss of W2s or any other compromise to sensitive information or information systems. Well in advance of an attack, companies should develop a coherent and effective incident response plan. Such a plan should be designed to quickly escalate compromises of sensitive information, so that Legal, IT security, Human Resources, and any other appropriate department can quickly act to mitigate the fallout from a breach. As part of their incident response planning, companies should consider establishing a relationship with outside counsel before an incident in order to fully leverage their specialized breach experience.

The loss of W2 forms triggers requirements in most states to notify impacted individuals. Even if not required to do so, companies should consider providing employees who had their W2s breached with credit monitoring services. However, this may not be enough. Cyber-criminals in possession of W2s can quickly cause significant financial harm to impacted employees, so time is of the essence.

The IRS provides steps for companies to respond to a breach of W2 forms on its website, including instructions on reporting such breaches to the IRS. The IRS recommends that even when a company receives a W2 phishing email and does not fall victim, the email should be reported, along with its header information, to phishing@irs.gov. Impersonations of IRS officials on the telephone can be reported to the IRS at tigta.gov. Companies experiencing an actual W2 data loss should report the incident to the IRS by emailing dataloss@irs.gov, as well as the FBI's Internet Crime Complaint Center at ic3.gov, so that the incident can be investigated.

Cyber-criminals may seek to file fake tax returns with state tax agencies. Therefore, companies experiencing a W2 breach should also email the Federation of Tax Administrators at StateAlert@taxadmin.org to get information on how to report victim information to the states. Some states may be able to monitor tax returns of employees residing in their state for fraudulent activity.

Where an employee knows of identity theft caused by breached W2 forms, the IRS recommends the following steps:

1. The employee should respond immediately to any IRS notice and call the number provided.

2. In the event an e-filed return is rejected because of a duplicate filing under the employee's social security number, or if the IRS has otherwise notified the employee that they are the victim of tax-related identity theft, the employee should complete and submit the IRS Form 14039, "Identity Theft Affidavit."

3. The employee should continue to pay taxes and file tax returns, even if by paper.

4. The employee should contact the IRS for specialized assistance at (800) 908-4490.

The Social Security Administration (SSA) also recommends measures for individuals who suspect their social security numbers have been compromised from a W2 breach or otherwise. Specifically, the SSA recommends setting up an online account through its "my Social Security" web portal in order to prevent a thief from setting up an account to steal benefits. Where an individual knows they have been a victim of social security fraud, they can block electronic access to SSA records.

As with any other information security incident, whether through a phishing email, cyber intrusion, or other means, responding to a W2 breach should be done through an enterprise-wide approach. Collaboration between key business units and advanced preparation is critical. In doing so, companies can position themselves to act quickly to protect employees from identity theft in the wake of a W2 breach.

Paul M. Tiao *is a partner at Hunton Andrews Kurth in the Washington, DC office, and founder and co-chair of the firm's Energy Sector Security Team. With experience in government and the private sector, Paul brings in-depth knowledge of cyber and physical security, internal investigations, law enforcement and national security to every client matter. He can be reached at +1 202 955 1618 or* ptiao@HuntonAK.com.

Eric Hutchins *is principal attorney at H2 Legal, P.C. in Chicago where he partners with Hunton Andrews Kurth to help companies achieve their security-related goals.*