LABOR & EMPLOYMENT/CORPORATE/TAX

HR, PAYROLL, FINANCE DEPARTMENT *BEWARE*: RENEWED IRS W-2 PHISHING SCAM ALERT

by David J. Houston

The Internal Revenue Service and other agencies recently issued an urgent reminder Alert warning of a sophisticated scam to obtain confidential information and in some cases, fraudulent cash wire transfer payments. Scammers appear originally to have targeted corporate HR and payroll departments, and have moved on to other employer groups. The IRS warning is directed at Schools, Restaurants, Hospitals and Tribal Groups.

IRS Commissioner John Koskinen is quoted in the Alert as warning: "This is one of the most dangerous email phishing scams we've seen in a long time. It can result in the large-scale theft of sensitive data that criminals can use to commit various crimes, including filing fraudulent tax returns." The IRS is asking for assistance in responding to this criminal initiative, and provides recommendations to employers to protect themselves, their data, and their workers.

What To Look For

Human Resources and Payroll department managers and employees are specifically advised to look for emails requesting employee names or lists of workers, or W-2 information regarding all or groups of employees of the organization. The IRS reports that scammers will typically use business email spoofing ("BES") or business email compromise ("BEC") to send a counterfeit inquiry appearing to come from a manager or executive who might legitimately have need for the information requested.

More recently according to the IRS, scammers have used purloined employee or W-2 information successfully to direct fraudulent wire transfers, which are immediately converted to cash by the scammer and therefore unrecoverable.

Proactive Measures

Because the tactic relies on taking advantage of otherwise legitimate-appearing requests, or reporting workers' understandable inclination to be prompt and helpful in responding to senior manager requests, avoidance tactics must rely on *employee awareness* and willingness to *question data requests*. Internal communication of, or training about, such scamming tactics and hazards, will increase awareness. Instilling a willingness within targeted employee groups (HR/payroll/finance department) to question data inquiries or demands, regardless of the source of the inquiry, is also key. *Reasonable reminders* are advised and necessary to drive home the importance of the threat of a breach, particularly when workers with access to confidential data may be performing relatively routine tasks, may be relatively lower-compensated, and may be in areas of significant employee turnover.

A second level of protection may be to develop and adopt written policies or protocols that are to be followed when certain alerts or triggers occur. So for example, and depending on many factors, requests for confidential personnel (W-2, social security, insurance, health, address, identification), financial, or business information might, by policy, be subject to a verification email or second-person approval before even *internal* disclosure of critical information or data.

Remedial Measures

Once data is gone, specific prophylactic measures, such as disclosing the loss to affected worker or others, are clearly appropriate. Recommended actions where data is compromised or lost to scammers is available from a Federal Trade Commission website resource, www.irs.gov/identitytheft.

The IRS requests that organizations that receive a W-2 scam or related contact or email should forward it to phishing@irs.gov with the subject line: "W-2 Scam."

Reports of criminal activity should also be reported to the Federal Bureau of Investigation at its Internet Crime Complaint Center link, https://www.ic3.gov/default.aspx.

The IRS Alert is available at:

In English, at:
https://www.irs.gov/uac/dangerous-w-2-phishing-scam-evolving-targeting-schools-restaurants-hospitals-tribal-groups-and-others

En español en:
https://www.irs.gov/spanish/evoluciona-peligrosa-estafa-de-phishing-relacionada-a-los-w-2

This client alert is published by Dickinson Wright PLLC to inform our clients and friends of important developments in the field of employment law. The content is informational only and does not constitute legal or professional advice. We encourage you to consult a Dickinson Wright attorney if you have specific questions or concerns relating to any of the topics covered in here.

FOR MORE INFORMATION CONTACT:

David J. Houston is a Member in Dickinson Wright's Lansing office. He can be reached at 517.487.4777 or dhouston@dickinsonwright.com.