IRS Issues Alert on Phishing Scheme to Obtain Payroll Data

Skadden

03/23/16

If you have any questions regarding the matters discussed in this memorandum, please contact the following attorneys or call your regular Skadden contact.

Diane Ryan
Chicago
312.407.0517
diane.s.ryan@skadden.com

Fred T. Goldberg, Jr.
Washington, D.C.
202.371.7110
fred.goldberg@skadden.com

Roland Barral
New York
212.735.3708
roland.barral@skadden.com

Emily M. Lam
Palo Alto
650.470.4680
emily.lam@skadden.com

Stuart D. Levi
New York
212.735.2750
stuart.levi@skadden.com

Four Times Square
New York, NY 10036
212.735.3000

skadden.com

The Internal Revenue Service (IRS) recently issued an alert regarding a phishing email scheme in which cybercriminals pose as governmental officials or company executives and request employee payroll and tax data, including W-2s and Social Security numbers, from company payroll and human resources professionals.[1] Where successful, the cybercriminals then attempt to monetize the stolen information by filing fraudulent tax returns seeking refunds on behalf of the individual taxpayers whose data was compromised.

According to the IRS commissioner, this latest phishing scheme is "a new twist on an old scheme using the cover of the tax season and W-2 filings" to trick people into sharing personal tax data.[2] Until recently, tax-based phishing emails largely have been directed at tricking individual taxpayers into releasing their information. By targeting corporations and partnerships holding taxpayer information, hackers can now potentially access far greater amounts of data with a single phishing attack. For companies that inadvertently disclose this information, the fallout can range from reputational harm to liability for damages.

The phishing emails in this scheme typically are drafted as urgent requests by either governmental officials or company executives designed to elicit an immediate response from company payroll and human resources employees. For example, the IRS notes that in some cases, the email will appear to come from the company CEO requesting that employees' W-2s and earnings summaries be forwarded for "a quick review."[3] Like most phishing attacks, these emails appear legitimate, and many already have fallen victim to them.[4]

Practice Points

Companies should — as always — be vigilant of phishing attacks and engage in comprehensive cybersecurity training. Employees who have access to taxpayer information should be directly informed of the IRS alert and instructed to verify any requests they receive for taxpayer information, regardless of how legitimate the message appears. Since these attacks likely will continue for as long as they prove successful, regular and ongoing training is crucial.

Our experience suggests that those engaging in this kind of attack are able to file false tax returns shortly after obtaining the ill-gotten taxpayer information, making it critical that employers take action during the first 24 to 48 hours after a successful cyberattack. While the IRS recently received additional funding to address cybersecurity issues and is focused on meeting this challenge, it remains severely resource-constrained, making it difficult, for example, for the IRS to independently assess the validity of tax returns. For this reason it is important to reach out quickly to the right contacts at the IRS to apprise them of the scam and work with them to flag potentially affected taxpayer accounts. We also advise companies to help individual employees whose information has been compromised seek tax-related identity theft protection, particularly under the IRS' new identity theft safeguards.[5]

Please contact us if you would like additional information on how to protect against inadvertent disclosure of taxpayer information and what steps to take in response to potential data breaches.

[1] "IRS Alerts Payroll and HR Professionals to Phishing Scheme Involving W-2s," IR-2016-34 (Mar. 1, 2016).

[2] The alert comes on the heels of the IRS renewing its wider consumer alert for phishing email schemes after observing an approximate 400 percent surge in phishing and malware incidents leading up to the 2016 tax season. *See id.*

[3] *See id.*

[4] *See id.*

[5] *See* "Identity Protection: Prevention, Detection, and Victim Assistance."