BROOKS PIERCE

Of Course I Meant to Send the Email, But Not to the Criminal – Court Rules that Companies Have a Duty to Train Employees on Cybersecurity Practices

04.11.2018

With the April 17 tax deadline fast approaching, businesses need to remain vigilant for employee reports (or more likely questions) about fraudulent tax returns being filed in their names. Multiple employee reports of fraudulent tax returns could be an indicator that a business has been the victim of the Form W-2 phishing scam that has struck hundreds of companies despite repeated warnings from the IRS and state tax agencies, including one earlier this year.

The scam works when a cybercriminal, posing as a company executive or other person in authority, successfully tricks someone with access to sensitive employee payroll information to send that information to the cybercriminal. Once the information is disclosed, it can be used to commit tax or other financial fraud or sold on the Dark Net.

Discovering that your business has been victimized by this scam will trigger notifications to affected employees and state government regulators. This can be a daunting task in itself, but a recent order in *Curry v. Schletter, Inc.*, 1:17-cv-0001-MR-DLH, 2018 U.S. Dist. LEXIS 49442 (W.D.N.C. Mar. 26, 2018), serves as a stark reminder that your troubles may not end there.

The case was filed in 2017 by current and former employees of Schletter, Inc., a western North Carolina-based manufacturer and distributor of solar mounting systems. The company fell victim to the W-2 scam in 2015 when an employee believed she was sending this confidential information to the company CEO. The company discovered the disclosure in April 2016 and notified its current and former employees a week later.

In January 2017, plaintiff representatives of a putative class filed claims against the company for negligence, invasion of privacy, breach of implied contract, breach of fiduciary duty, and violation of the N.C. Identity Theft Protection Act ("ITPA"), which also triggers a violation of the N.C. Unfair and Deceptive Trade Practices Act.

The company sought to have all plaintiffs' claims dismissed pursuant to Rule 12(b)(6) for failure to state a plausible claim for relief. The Court granted the motion to dismiss with respect to the breach of fiduciary duty claim but allowed all of the other claims to go forward. *Id*. at *16-17.

Ever since the infamous North Korean hack of Sony, we've been anxious to see if a court would place a heightened duty on an employer regarding safeguarding employee data. After all, we all provide our employers some of our most sensitive personal information. The *Curry* plaintiffs alleged that that the employer had a duty to protect their data, and that such duty sounded in both contract and tort. Critically, the Court allowed both theories to proceed.

Regarding the contract claim, the employer argued that there was no contract, implied or written, between the employer and employee that addressed personal information. By contrast, the employees alleged that they were required to provide their employer with certain personal information as a condition of their employment, which was sufficient to allow their contract claim to survive a motion to dismiss. *Id.* at *9-10. Further, the fact that the employees' personal information was disclosed by the company to unauthorized persons was "highly offensive" enough behavior to allow the invasion of privacy claim to move forward. *Id.* at *12-13.

The employees also asserted a negligence claim. Importantly, the Court noted that the employer had failed to adequately train its employees about "even the most basic of cybersecurity protocols," and it failed to train relevant employees about the particular, well-known scam that lead to the data disclosure at issue. *Id.* at *5-6. In response, the employer asserted the economic loss doctrine, which prohibits a tort claim for economic losses where a contract exists. The Court, however, allowed both theories to proceed, noting that ultimately the evidence will reveal whether the employer's duty sounds in contract or from another source.

The *Curry* plaintiffs' ITPA claim focused on two provisions that prohibit public disclosure of a person's social security number. Addressing the company's argument that the disclosure was to a scammer and not the public, the Court noted that there was no way to no how many cybercriminals were involved with the scam or whether the information was further disseminated after being disclosed. *Id.* at *16. This uncertainty was enough to make out a plausible claim that the information was made available to the general public. *Id.* at 15-16.

The company also argued that its actions could not violate the ITPA because it had no intent to disclose the SSNs to an unauthorized party. Notably, the Court declined to accept this argument, finding instead that the employee who was duped by the scam had "intentionally" communicated the information to a third party—even if the communication was under false pretenses. *Id.* at *16.

In so holding the Court made a significant and previously unrecognized in law distinction between a data breach and a data disclosure stating that for purposes of intent "a data *breach*, wherein a hacker infiltrated the [company] computer systems and stole [personal] information" without company knowledge is different from a "data *disclosure*, wherein the [company] intentionally responded to an email request with an unencrypted file containing highly sensitive information." *Id.*

This new distinction has the potential to open the gates much wider on ITPA claims following inadvertent data disclosures and raises the bar for any business that holds the personal information of North Carolina residents.

While most of these email phishing scams can be caught with a little common sense, this case confirms that employers must undertake specific and ongoing efforts to ensure that employees with access to sensitive information know how to properly handle such information and know what scams to be on the lookout for while at work.

Here are a few tips for employees with access to sensitive information to follow:

- Before responding to a request for personal information be sure that you are sending the information to someone with a legitimate business reason for possessing the data. If there is any question about the request, pick up the phone and call the requesting person to verify.
- Instead of responding to a request for personal information by hitting "reply" to the request, create a new email and type out the email address of the recipient as it appears in the company address book—don't copy and paste from the requesting email!
- Best of all, instead of sending such information via email, utilize encrypted internal file transfer systems and other protocols to avoid any possibility of inadvertently disclosing information to an unauthorized third-party.

PEOPLE

Will Quick

Bryan Starrett

SERVICES

Privacy