LOS ANGELES & SAN FRANCISCO
Daily Journal
www.dailyjournal.com
TUESDAY, JUNE 21, 2022

PERSPECTIVE

GUEST COLUMN

Third-party email fraud covered by insurance policies

By Peter Selvin

In *Medidata Solutions, Inc. v. Federal Insurance Company*, 268 F. Supp. 3d 471 (S. D. N. Y. 2017), aff'd, 729 Fed. Appx. 117 (2nd Circuit 2018), the Court found that there was insurance coverage where a company had been victimized by an email spoofing scheme that resulted in the company wiring funds to a fraudster's account. More recent cases have also found insurance coverage for losses arising from similar incidents of this kind. See, e.g., *Ernst & Haas v. Hiscox, Inc.*, 23 F. 4th 1125 (9th Cir. 2022)

In *Medidata*, the spoofed email came in the form of an email purportedly coming from the company's president which instructed that payment be made to a certain outside account. Believing the email to be genuine, a subordinate in the company wired the funds to the fraudster's account.

Coverage for the company's loss was found in *Medidata* because the Court determined that the fraudster's entry into and manipulation of the company's email system satisfied the policy's requirement that there was a "fraudulent entry of data into a computer system and change to data elements or program logic of a computer system."

But what if the spoofed email purportedly comes from someone impersonating an outside vendor, as opposed to someone impersonating an executive within the victimized company? In the case of an email impersonating an outside vendor, the argument that the company's own email system had been manipulated may be less strong, depending on the specific policy language. Nevertheless, three recent cases have affirmed coverage where a vendor has been impersonated and as a result the company sustained a loss.

In *Am. Tooling Ctr., Inc. v. Travelers Cas. & Sur. Co. of Am.*, 895 F. 3d 455 (6th Cir. 2018), a company was victimized by a fraudster impersonating one of the company's Chinese vendors. The company received a series of emails, purportedly from its Chinese vendor claiming that the vendor had changed its bank accounts and the company should wire its payments to these new accounts. After transferring $834,000, the company learned that the emails were fraudulent.

The company was insured by Travelers under a business insurance policy, which included coverage for computer fraud. The coverage grant for computer fraud provided that Travelers would indemnify the company for any losses arising from "the use of a computer to fraudulently cause a transfer of Money…from inside [the company's] premises …to a person …outside [the company's] premises…"

The company submitted the claim to Travelers, but it was denied, and the trial court granted summary judgment to Travelers.

The Court of Appeals reversed. As it did in front of the trial court, Travelers argued on appeal that computer fraud coverage required that a computer be used to fraudulently cause the transfers. In other words, Travelers argued that the coverage under the computer fraud grant should be limited to "hacking and similar behaviors in which a nefarious party somehow gains access to and/or controls the insured's computer." The Court rejected this policy interpretation and held that the company's loss was covered by the Travelers policy.

In *Cincinnati Ins. Co. v. Norfolk Truck Ctr., Inc.*, 430 F. Supp. 3d 116 (E. D. .Va. 2019), the Court dealt with a similar fact pattern. There the victimized company received an email from an unidentified imposter who represented himself to be an employee of the company's vendor. The imposter gave fraudulent payment instructions via email and thereafter the company authorized its bank to issue a wire transfer of $333,724 in accordance with the imposter's instructions.

The coverage grant for computer fraud policy at issue in *Cincinnati Ins.* was substantially similar to the one in *Am. Tooling*, except that the *Cincinnati Ins.* policy required that the loss result "directly" from the use of any computer to fraudulently cause the transfer of funds. In that case, the carrier argued that the loss did not arise "directly" from the imposter's email because the company and its employees took subsequent steps to implement the underlying transfer after receiving the fraudulent email. This argument was in essence a variation on Traveler's argument in Am. Tooling that in order to be covered the loss had to arise from the imposter's actual entry into and manipulation of a company's computer system.

Both carriers in essence argued that because the imposters in those cases had not penetrated or manipulated the companies' computer systems, and had not therefore effectuated the transfers of funds themselves, there would be no coverage. As in many other cases in this area, the Court rejected this argument and determined that the company's reliance on the fraudulent email provided a sufficient nexus to satisfy the "directly" requirement in the coverage grant. See also *Principle Sols. Grp. V. Ironshore Indem., Inc.*, 944 F. 3d 886 (11th Cir. 2019); *Ernst & Haas v. Hiscox, Inc.*, supra.

Finally, in *City of Unalaska v. Nat'l Union Fire Ins. Co.*, (3:21-CV-00096-SLG, 2022 WL

826501, Mar. 18, 2022), the city's accounts payable assistant received an email purportedly sent by one of the City's regular vendors, requesting a copy of the City's ACH/EFT form in order to change its method of receiving payments for invoices from paper checks to payments electronic ACH transfers. The email was not from the City's vendor but from a fraudster, but in reliance thereon the City made substantial disbursements.

The City had an insurance policy with National Union which included a computer fraud insuring agreement. That policy included grants for Impersonation Fraud as well as Computer Fraud. The latter grant stated that National Union would pay for the loss of money "resulting directly from the use of any computer to fraudulently cause a transfer [of money] from inside [the company's] premises to a person outside [the company's] premises…"

Following National Union's partial denial of coverage the City brought suit and the City filed a motion for summary judgment, while National Union brought a motion for judgment on the pleadings. Relying on two unpublished Fifth Circuit decisions, *Apache Corp. vs. Great Am. Ins. Co.*, 662 Fed. App'x 252 (5th Cir. 2016) and *Mississippi Silicon Holdings, LLC vs. Axis Ins. Co.*, 843 Fed. App'x 581 (5th Cir. 2021), National Union argued that the City's loss was not covered under the computer fraud grant because the use of a computer was not the "direct cause" of the loss. Like the insurers in *Am. Tooling and Cincinnati Ins.*, National Union argued that coverage would only be triggered if "the Fraudster's use of a computer …directly bring[s] about the funds transfer."

The District granted the City's motion and denied National Union's motion. In doing so, the Court held that the email from the imposter caused the transfer of funds from the City to the fraudster's bank account. The Court noted that "the ubiquity of computer usage does not alter the fact that a reasonable layperson would consider the phrase "use of a computer" to encompass a broad range of activities, including sending emails, rather than being limited to instances of computer hacking."

While all three of the foregoing cases found coverage for losses occasioned by persons impersonating a company's vendor, the determining factor in all cases will be the policy language itself. In policies defining "computer fraud" in the same manner as the policies at issue in those cases, coverage will most likely be found in similar circumstances.

Peter Selvin *is a partner at Ervin, Cohen & Jessup.*

Reprinted with permission from the *Daily Journal*. ©2022 Daily Journal Corporation. All rights reserved. Reprinted by ReprintPros 949-702-5390.