LOS ANGELES & SAN FRANCISCO

Daily Journal

www.dailyjournal.com

WEDNESDAY, APRIL 3, 2024

GUEST COLUMN

A new twist on coverage for losses from 'spoofed' emails

By Peter S. Selvin

Shutterstock

The facts are frequently the same. A company that has retained the services of a vendor receives an authentic-looking email from the vendor's CFO which advises that the vendor has changed its bank account or method of payment. Believing that the email is genuine, the company wires funds as directed by the vendor's CFO. It then turns out that a hacker has impersonated the vendor's CFO and the company's payment has gone to an overseas account controlled by the vendor.

In due course, the vendor sues the company demanding payment. The question then arises whether the company's insurance company will make good on the loss.

A number of cases have found coverage for the insured company in these circumstances under the computer fraud portion of its crime policy. *See, e.g., Am. Tooling Ctr., Inc v. Travelers Cas. & Sur. Co. of Am.*, 895 F. 3d 455 (6th Cir. 2018); *Cincinnati Ins. Co. v. Norfolk Truck Ctr., Inc.*, 430 F. Supp. 116 (E. D. Va. 2019); *City of Unalaska v. Nat'l Union Fire Co.*, 2022 US Dist. LEXIS 51387 (D. Alaska March 18, 2022). Coverage was afforded under those cases because the pertinent coverage grant was broad, as it insured against the loss of money resulting from "the use of any computer" to fraudulently cause the transfer of money from the insured's premises to a person outside the company.

The problem is that in newer policies the definition of computer fraud has been tightened so as to require the actual penetration of an insured's computer system as a prerequisite for coverage. A fraudulent email from a third party to the insured may not necessarily meet this new threshold.

A recent case from the US District Court for the Southern District of California, decided March 18, 2024, took an intriguing approach to this problem. *Bridlewood Estates Property Owners Association v. State Farm General Insurance Company*, Case No. 23-cv-00195-AJB-AHG. There the insured was defrauded by a hacker who impersonated the company's vendor. The genuine appearing (but fraudulent) email advised that the vendor was moving away from receiving check pays to direct electronic wire transfers. This email was forwarded to the plaintiff's Treasurer, who wired funds from plaintiff's bank account using the wire transfer instructions provided by the hacker.

The company's vendor, having not been paid, sued plaintiff alleging breach of contract and related claims. The plaintiff tendered the suit to its D & O carrier, who denied the claim. This insurance coverage suit then ensued.

The D & O carrier filed a motion to dismiss essentially raising two points: first, it asserted that there had been no "wrongful act" within the meaning of the D & O policy; and second, because the vendor's claims all sounded in breach of contract, there would be no coverage under plaintiff's liability insurance policy. *See, e.g., August Entertainment, Inc. v. Philadelphia Indemnity Ins. Co.*, 146 Cal. App. 4th 565 (2007).

In a victory for policyholders, the Court rejected both of these arguments.

As to the carrier's argument that there had been no "wrongful act," the Court ruled that extrinsic facts known to State Farm suggested that there was a potential claim for coverage based on plaintiff's Treasurer's

error, negligence, or breach of duty in authorizing the payment as directed by the fraudulent email. The Court found that the extrinsic evidence known to State Farm "support a finding that plaintiff's Treasurer committed a 'wrongful act' when he transmitted payment of the vendor's invoice to the wrong bank account, which in turn gave rise to the vendor's complaint for breach of contract." *Id.* at * 7.

As to State Farm's argument that breach of contract claims are not covered by liability insurance, the Court distinguished the August Entertainment case by noting that in that case, the insured had simply refused to make a payment under a contract and looked to its D & O insurer for a bailout. The Court noted held that "because the instant case is not one where a plaintiff is merely attempting to pass on its contractual obligations to its insurer, the Court does not find that it falls within the purview of California case law finding that failure to pay amounts due under a contract does not constitute a wrongful act for purposes of directors and [officers] liability coverage." *Id.* at * 8.

The decision in *Bridlewood* is notable for several reasons.

First, it is the first case to the author's knowledge where coverage was found under a D & O policy for what is essentially computer fraud committed by a third-party hacker. Unlike the three cases cited at the beginning of this article, the focus in *Bridlewood* was the *conduct of the plaintiff in approving payment* rather than whether the *conduct of the hacker amounted to a penetration of the insured's computer system* or otherwise constituted computer fraud.

Second, the Court's holding that an insured's failure to pay under a contract may constitute a "wrongful act" under a D & O policy is important. In essence, the Court looked at the conduct of the plaintiff's Treasurer in concluding that such conduct could be characterized as negligent or otherwise in breach of some duty. In this context, the vendor's characterization of its own claims as sounding in contract was less important in the Court's analysis.

Peter S. Selvin *is a partner with Ervin, Cohen & Jessup and head of the firm's insurance coverage and recovery department.*