LOS ANGELES & SAN FRANCISCO
Daily Journal
www.dailyjournal.com
WEDNESDAY, FEBRUARY 16, 2022

PERSPECTIVE

9th Circuit says computer-fraud policies may cover 'spoofing'

By Peter S. Selvin

Consider the following two scenarios resulting in identical losses — but potentially two entirely different insurance coverage outcomes:

Scenario 1: A thief hacks or gains unauthorized entry into an insured's computer system and causes that computer system to execute a bank transfer to the thief's offshore account.

Scenario 2: A thief uses a process called "spoofing" in which an authentic-looking but fraudulent email is created to trick the insured into wiring funds to the thief's offshore account. The "spoofing" process tricks the insured's email server into recognizing the fraudulent email as one that actually originated from the insured's client or other trusted source.

Computer-fraud policies often provide coverage in the first scenario. In that instance, the thief actually obtained access to the insured's computer and "used" that computer, in the words of typical policy language, "to fraudulently cause a transfer of property from inside the insured's premises to a person outside those premises."

In the second scenario, some courts have been unreceptive to finding coverage because an insured's acting on or treating as genuine a fraudulent email directing the payment of funds has not been considered the equivalent of the "use of a computer" in a manner that fraudulently "caused" a transfer of money or other property. As stated by one court, "[t]o interpret the computer-fraud provision as reaching any fraudulent scheme in which [a computer] communication was part of the process would ... convert the computer-fraud provision to one for general fraud." *Apache Corp. v. Great Am. Ins. Co.*, 662 Fed. Appx. 252, 258 (5th Cir. 2016); *see also Taylor &Lieberman v. Federal Insurance Company*, 681 Fed. Appx. 627 (9th Cir. 2017).

However, a recent 9th U.S. Circuit Court of Appeals case joins several other decisions in finding that damages arising from "spoofing" may be covered under an insured's computer-fraud policy. *Ernst and Haas Management Company v. Hiscox, Inc.*, 23 F.4th 1195 (9th Cir. 2022); *see also Medidata Solutions, Inc. v. Federal Insurance Company*, 268 F. Supp. 3d 471 (S.D.N.Y. 2017), aff'd, 729 Fed. Appx. 117 (2d Cir. 2018); *Am. Tooling Ctr., Inc. v. Travelers Cas. & Sur. Of America*, 895 F.3d 455 (6th Cir. 2018).

In *Ernst and Haas*, an account payable clerk received emails purportedly from her superior directing her to make several payments to Zang Investments, LLC. In fact, the emails were from a fraudster who was impersonating her superior. Believing the emails were genuine, the clerk approved and processed the payments to Zang by wire transfer.

After the fraud was discovered, Ernst tendered the loss to insurance company Hiscox under the company's crime policy. That policy provided coverage for losses arising from computer fraud, which included losses "resulting directly from the use of any computer to fraudulently cause a transfer" of funds to a third party. The policy also provided coverage for losses arising from funds transfer fraud, which included losses resulting from a fraudulent instruction directing a financial institution to pay funds from an account maintained by the insured.

Hiscox denied coverage for the claim and Ernst brought suit. Relying on an earlier 9th Circuit case (*Pestmaster Servs., Inc. v. Travelers Cas. & Sur. Co. of Am.*, 656 Fed. App'x 332 (9th Cir. 2016)), the district court granted Hiscox's motion to dismiss. The Court of Appeals reversed.

The 9th Circuit distinguished the facts of the case from those in *Pestmaster*, which involved the embezzlement of funds by a third-party contractor who had been authorized to disburse from the insured's accounts to pay taxes. In *Ernst and Haas*, by contrast, the court was focused on an email fraud scheme in which the company's account payable clerk had been fraudulently authorized to wire the funds.

The 9th Circuit also rejected the district court's view that the loss did not result "immediately" and "directly" from computer fraud because Ernst, through its account payable clerk, authorized its bank to initiate the wire transfers from its account. Citing the 6th Circuit's decision in *American Tooling Center*, the 9th Circuit held that Ernst's loss arose "directly" from the fraud because its account payable clerk acting pursuant to the fraudulent instruction "directly" caused the loss of funds.

The 9th Circuit also rejected the conclusion that there was no coverage for Ernst's loss under the policy's coverage for funds transfer fraud. The district court had based its ruling on the fact that the fraudulent instructions did not direct Ernst's bank to transfer the funds but instead directed the account payable clerk to direct the company's bank to transfer those funds. The 9th Circuit pointed to language in the policy stating that funds transfer fraud includes not only fraudulent instructions sent directly to a bank but also fraudulent instructions initially received by an insured's employee. The appellate court cited *Principle Solutions Group, LLC v. Ironshore Indemnity*, 944 F.3d 886 (11th Cir. 2019), which held that an email directing an employee recipient to initiate a wire transfer through a bank satisfied the requirement that a fraudulent instruction "direct a financial institution" to transfer funds.

With the *Ernst and Haas* decision, the 9th Circuit appears to be joining with the decisions of other jurisdictions which have expanded the concept of "use of any computer" (as that language is used in computer-fraud policies) to include not only the unauthorized intrusion into, and manipulation of, an insured's computer by a third-party hacker, but also instances where an insured's employee authorizes the transmission of funds based on a fraudulent instruction.

Peter Selvin *is chair of the Insurance Coverage and Recovery Department at Ervin Cohen & Jessup LLP.*