LOS ANGELES & SAN FRANCISCO

Daily Journal

www.dailyjournal.com

WEDNESDAY MARCH 22, 2023

PERSPECTIVE

Companies that pay hackers may be able to recoup their losses

Peter S. Selvin

Shutterstock

Where companies are victimized by ransom ware or email scams, their losses arise from payments made by an officer or employee of the company.

In the case of ransomware, a company's files are held hostage pending payment by the company to release them. In the case of email scams, typically a company's employee is tricked into sending funds to a third party account which the employee believes is legitimate.

In both cases, the loss is occasioned *through some action by the company* either in the form of payment to the cyber thief or to the fraudster's account.

Insurers resisting payment on account of such claims typically argue that insured losses in these scenarios only occur where a hacker penetrates the insured's computer system and directly steals funds without the insured's knowledge or involvement. In making this argument, insurers point to two provisions that are typically found in crime policies.

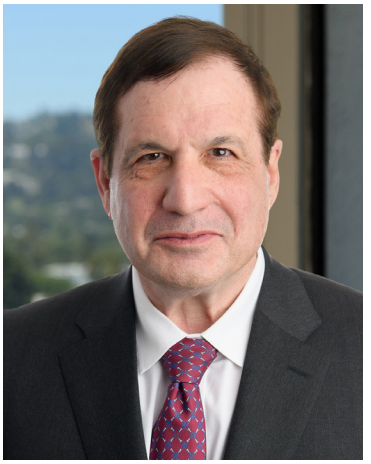
Many crime policies define computer fraud coverage in terms of the "**direct** loss of Money, Securities or Property sustained by an Insured resulting from Computer Fraud..." (emphasis added). Further, these policies often have an exclusion that bars coverage where "any transfer, payment of or delivery of Money, Securities or Property [is] **approved** by an Employee..."

Insurers resisting reimbursement for these kinds of losses will therefore argue that an insured's loss was not the "direct" result of the underlying fraud because of the intervening action of the company in actually making the pertinent payment. Similarly, insurers will also argue that coverage is barred because the company's payment to the ransomware thief or to the fraudulent account was "approved" or "authorized" by the company or its managers.

Although there have been a couple of cases supporting this position (*Taylor & Lieberman v. Federal Insurance Co.*, 2015 WL38-24130 (C. D. Cal. 2015), aff'd, 681 Fed. Appx. 627 (9th Cir. 2017); *Pestmaster Services, Inc. v. Travelers Casualty and Surety Company of America*, 2014 WL 3844627, aff'd in part, vacated in part, 65 Fed. Appx. 332 (9th Cir. 2016)), more recent cases take a different, more policyholder-friendly view.

In *Ernst and Haas Mgmt. Co., Inc. v. Hiscox, Inc.*, 23 F. 4th 1195, 1199-1120 (9th Cir. 2022) the policy at issue stated that the carrier would cover a loss "resulting **directly** from the use of any computer to fraudulently cause a transfer" of the insured's property to a third person. (emphasis added). In that case, 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 im-

Peter Selvin *is a partner at Ervin Cohen & Jessup LLP and chair of the firm's Insurance Coverage and Recovery Department.*



personating her superior. Believing the emails to be genuine, the clerk approved and processed the payments to Zang by wire transfer.

The company's carrier denied responsibility for the loss, stating that the fraud was not covered because the company's employee (i.e., its accounts payable clerk) had taken action to initiate the wire transfer - hence the loss was not the "direct" result of the use of a computer. In the ensuing coverage litigation, the District Court agreed with the carrier's position, but the Ninth Circuit reversed.

The Ninth Circuit held that Ernst immediately lost its funds when those funds were transferred to Zang as directed by the fraudulent email. There was no intervening event - [the accounts payable clerk] acting pursuant to the fraudulent instruction directly caused the loss of the funds. Thus, ... Ernst suffered a loss 'directly' from the fraud, arguably entitling Ernst to coverage under the policy."

An even more recent case, *Yoshida Foods Int'l, LLC v. Fed. Ins. Co.*, 2022 WL 17480070 (Dec. 6, 2022 D. Oregon) is to the same effect. In that case, the Yoshida company was the victim of a ransomware attack in which the thief demanded a ransom payment in exchange for a decrypting program. In order to have its files released, the company paid $100,000 for the ransom payment and another $7,000 in IT expenses. As for the ransom payment, it was advanced by the company's CEO as the company did not have sufficient cash on hand to make that payment. The company subsequently reimbursed its CEO for this advance.

Although Yoshida sought reimbursement under its crime policy, the carrier declined coverage. In so doing, the carrier stated that because the ransom payment was made by the company, "there was no permanent loss of Money...that **directly** resulted from a Computer Violation." (emphasis added). The carrier also declined coverage on the basis of the Fraudulent Instructions Exclusion, presumably arguing that the ransomware payment had been "approved" by a company employee.

In granting Yoshida's motion for summary judgment on its breach of contract claim, the District Court rejected both of these arguments. The Court rejected the carrier's argument that the company's loss was not "directly resulting" from a computer violation: "Both the ransom payment made by Mr. Yoshida and the reimbursement of that amount by Plaintiff were proximately caused by the hacker's computer violation directed against Plaintiff's computer system. There was no intervening occurrence between the ransomware attack, the ransom payment and the reimbursement to Mr. Yoshida, which were all part of an unbroken sequence of events." See also *G&G Oil Co. of Indiana v. Cont'l W. Ins. Co.*, 165 N.E.3d 82 (Ind. 2021).

The Court also rejected the application of the carrier's argument that Fraudulent Instructions Exclusion barred coverage because the ransomware payment had been "approved" by a company employee. See *Aqua Star (USA) Corp. v. Travelers Cas. & Sur. Co. of Am.*, 2016 WL 3655265 (W.D. Wash. 2016) (finding a coverage exclusion applied when employees were induced by fraudulent emails to initiate fraudulent transfers to third parties). Instead, the Court found that because the ransomware payment had been coerced, Mr. Yoshida did not "approve" the ransom payment needed for the company to regain access to its computer system.