Cooley

Ninth Circuit's Fraudulent Payments Coverage Ruling Has Implications for Cyber Insurance Purchasers

February 2, 2022

In a decision with significant implications for policyholders seeking coverage for social engineering scams and cybercrime losses, the US Court of Appeals for the Ninth Circuit held in ***Ernst and Haas Management Company, Inc. v. Hiscox, Inc.*** that an insurance policy covering losses resulting directly from computer fraud included coverage for payments made based on a fraudulent invoice. The Ninth Circuit held that the loss was "directly" caused by the fraud, disagreeing with the insurer's argument that the unwitting employee who received the fraudulent invoice and sent the payment to the fraudster was an intervening actor.

Ernst and Haas Management Company was a victim of a common social engineering scam: A fraudster emailed an Ernst employee a fraudulent invoice, posing as that employee's superior. Believing the email to be legitimate, the employee directed Ernst's bank to wire $200,000 to a third-party account reflected in the fraudulent invoice. Afterward, the employee discovered that the superior did not actually send the fraudulent invoice. However, the $200,000 had already been transferred, and Ernst could not recover the funds.

Ernst's crime insurance policy contained two types of coverage common in many cyber and crime insurance policies: computer fraud coverage and funds transfer coverage. The computer fraud coverage insured loss "resulting directly from the use of any computer to fraudulently cause a transfer." The insurer denied coverage on the basis that the bank transfer did not result directly from computer fraud; rather, it resulted from the employee's subsequent instruction to the bank. The Ninth Circuit disagreed, following the US Court of Appeals for the Sixth Circuit's reasoning in *Am. Tooling Center, Inc., v. Travelers Cas. & Sur. Co. of Am.*, 895 F.3d 455, 457 (6th Cir. 2018), and held that Ernst's loss resulted directly from a computer fraud because the employee was acting pursuant to a fraudulent instruction received in an email.

Similarly, the funds transfer coverage insured loss "resulting directly from a Fraudulent Instruction directing a financial institution to transfer, pay or deliver Money." The insurer denied coverage, arguing that the fraudulent instructions were directed to the insured, and not to the financial institution. The Ninth Circuit again disagreed, reasoning that the sole purpose of the fraudster's instructions was to direct the employee to initiate a wire from Ernst's bank. Hence, this instruction was "direct" enough to trigger the policy's funds transfer coverage.

The Ninth Circuit's decision rejects a common defense often raised by insurers to avoid providing coverage for increasingly frequent social engineering scams. While the decision is a victory for policyholders, it also serves as a reminder **to be proactive about purchasing cyber coverage with more favorable terms** to avoid coverage disputes like this one. Ambiguities can lead to lost coverage for the costs of ransomware attacks, data breaches, privacy claims, government investigations and other cyber exposures. Coverage counsel can assist with minimizing these potential gaps and vulnerabilities as part of an organization's overall cyber risk management strategy.

If you have any questions about cyber insurance, please reach out to a member of the Cooley insurance team.