Articles + Publications | May 16, 2022

# WTF?! – Wire Transfer Fraud Coverage Disputes Continue

Privacy & Cybersecurity Newsletter

**WRITTEN BY**

Molly McGinnis Stine | Melina Kountouris | Matthew Murphy

Business email compromises (BECs) remain big business. According to a recent FBI report, "[i]n 2021, BEC schemes resulted in 19,954 complaints with an adjusted loss of nearly $2.4 billion." This is an increase from just over $1.8 billion in 2020. With the amount of money at stake, it is not surprising that courts continue to have opportunities to consider potential coverage under victims' insurance policies.

As we have previously discussed, prior court decisions in several jurisdictions address potential insurance coverage for BECs under commercial crime policies, wrestling with some common issues and reaching different results. We examine the newest opinions here which concern two recurring topics in these types of coverage disputes: (1) whether an insured "held" the funds sent to a fraudster, and (2) whether a loss was "directly related to the use of a computer." Courts continue to disagree.

In addition, BEC losses are the subject of claims under other types of insurance policies including policies loosely referred to as "cyber policies". We discuss below a recent decision under such a policy.

**Coverage Under Commercial Crime Policies**

The Fifth Circuit recently favored insurers in a matter in which an employee clicked a phishing link and provided login information for the employer's account with its third party payment vendor.[1] The threat actor used the stolen credentials to divert property rental payments intended for the employer insured's clients. The insured reimbursed its clients and filed claims under its commercial crime insurance policies. In the ensuing coverage action, the federal district court for the Northern District of Texas found there was no coverage because the funds were in the vendor's account, and not the insured's, the insured did not, as required by the policy, "hold" the funds that were transferred. The Fifth Circuit, in affirming the trial court's decision, observed that "[u]nder any definition of 'hold' that entails 'keep[ing] in custody' or 'possession,'" the insured could not claim a loss under the subject policies because it never "held" the funds intended for its property manager clients.[2]

In contrast, the Ninth Circuit in January 2022 reversed a lower court that found no coverage under a commercial crime policy for a property management company's losses following fraudulent emails requesting that the insured transfer $200,000.[3] The trial court determined that the alleged loss did not result directly from fraudulent emails instructing one of the insured's employees to transfer funds to a deceptive third party.[4] In holding the insured had coverage for its losses, the Ninth Circuit concluded that the trial court erred for three reasons: (1) by analyzing the case "as if it involved theft of funds authorized for payment;" (2) by narrowly interpreting the computer fraud provision "to mean a direct loss [ ] limited to unauthorized computer use, like hacking;" and (3) by limiting "funds

transfer fraud to exclude fraudulent instructions to [the insured's] employee", where "the language of the policy was not so limited."[5] The Ninth Circuit declined to reconsider the reversal.[6]

A federal court in Alaska in March 2022 looked to that Ninth Circuit decision to examine coverage under a commercial crime policy following an Alaskan city's payments using fraudulent instructions purportedly sent by one of the city's regular vendors. The court, concluding the insured was entitled to coverage, found that "the City experienced a loss of money resulting directly from the fraudster's use of a computer," and 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."[7] The court also found that the plain language of the computer fraud insuring agreement did not require "more than proximate causation for coverage."[8]

These recent decisions highlight that the common issues found in earlier court opinions persist and that different outcomes continue. Does an insured "hold" the property (i.e., the money)? Does the policy require an insured to "hold" the funds? What does "hold" mean? Does the loss "result directly" from the use of a computer? What does "directly" encompass and, importantly, not include? Are there parameters or limits to the extent or nature of the "use" of a computer? All of these questions are fact-intensive and affected by the standards in the applicable law.

**Cyber Policy Coverage**

A federal court in Florida determined that there was no coverage under a cyber policy for a loss that occurred after a fraudster induced the insured's employee to wire funds to an incorrect account.[9] The insured was a title company who had been hired to act as the settlement agent for the sale of a home. The insured's employee requested payoff information from the seller's lender and lienholder. She received a payoff statement via email and facsimile that was purportedly from the seller's lender and lienholder, but did not verify the authenticity of the wire information. The wire instructions the insured's employee received were fraudulent. The court determined that there was no coverage because "the fraudster did not 'purport to be an employee, customer, client or vendor'; and (2) 'the authenticity of [the] transfer request [was not] verified in accordance with [the insured's] internal procedures'", both of which were requirements for coverage under the policy. The insured's appeal is pending before the Eleventh Circuit.

**Conclusion**

The onslaught of BEC activity over the last few years has led to a spate of litigation (by victims against those they allege caused the loss and between insureds and their insurers), and the litigation life cycle continues apace.[10] Litigation is expensive and uncertain. Avoiding losses from a BEC in the first instance is preferable to pursuing a suit against some other party or making a claim under an insurance policy. As we advised in a previous article, there are steps entities can take now, including technical safeguards, and not to be understated, employee training, that can help entities guard against the threat of BECs. But if an insurance claim is made and if an insured and its insurer disagree about coverage for the claim, all should be aware that the particular policy language at issue, the specific facts involved, and the substance of the law of the potential applicable jurisdictions will play a significant role in the outcome.

***

[1] *RealPage, Inc. v. Nat'l Union Fire Ins. Co. of Pittsburgh, PA*, 21 F.4th 294 (5th Cir. 2021).

[2] *Id*. at 298.

[3] *Ernst & Haas Mgmt. Co., Inc. v. Hiscox, Inc*., 23 F.4th 1195, 1196–97 (9th Cir. 2022).

[4] *Id*. at 1199.

[5] *Id*. at 1199–200.

[6] Notably, during the trial court litigation, the insured and its insurers disagreed whether the language in a 2012 policy form applied, or whether the more restrictive language in a 2019 policy language applied. The trial court assumed the 2012 language applied, rather than the more restrictive language of the 2019 policy. Accordingly, the Ninth Circuit did not address the 2019 policy language, but indicated that the trial court could address it in the first instance on remand. *Id*. 1197 n.1.

[7] *City of Unalaska v. Nat'l Union Fire Ins. Co*., No. 3:21-CV-00096-SLG, 2022 WL 826501, at *8 (D. Alaska Mar. 18, 2022).

[8] *Id*. at *8. ("The Court finds the reasoning of the Eleventh Circuit in Principle Solutions persuasive on this point—though the word 'directly' may connote immediacy when read in isolation, a reasonable insured would consider the phrase 'resulting directly from' to convey the concept of proximate cause.").

[9] *Star Title Partners of Palm Harbor, LLC v. Illinois Union Ins. Co*., (M.D. Fla., Sept. 1, 2021, No. 8:20-CV-2155-JSM-AAS) 2021 WL 4509211, appeal docketed, No. 21-13343, 11 Circuit.

[10] *See., e.g., Downwind Trading Company c. Federal Insurance Company*, No. 2022CP2600971 (S.C. Com. P. filed Mar. 17, 2022) (Complaint filed against insurer seeking coverage under crime policy, following alleged breach of email address of insured's president); *SJ Computers, LLC v. Travelers Cas. & Sur. Co. of America*, No. 21-cv-02482 (D.C. Minn., filed January 7, 2022) (Insurer's Motion to Dismiss Insured's Complaint seeking coverage under commercial crime policy); *Fishbowl Sols., Inc. v. Hanover Ins. Co*., No. CV 21-794 (SRN/BRT), 2022 WL 1037083, at *1 (D. Minn. Apr. 6, 2022) (denial of plaintiff's motion to amend complaint to include bad faith claim against professional liability insurer who declined coverage because the coverage issue was "fairly debatable", where insured plaintiff sought coverage following loss incurred because of a "man in the middle" business email compromise).

## RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber