Articles + Publications | October 4, 2021

WTF?! – Recurring Issues in Wire Transfer Fraud Coverage Disputes

Privacy & Cybersecurity Newsletter

WRITTEN BY

Molly McGinnis Stine | Melina Kountouris | Matthew Murphy

Business email compromise threats trick unsuspecting targets into sending money to the perpetrators, often through use of fraudulent wire or ACH transfer instructions. Entities should take steps to protect themselves from such attacks. An increasing number seek relief in litigation. Victims are also turning to their insurance policies to try to recoup some or all of their losses.

The policies to which fraud victims seek coverage often include Computer Fraud and Funds Transfer Fraud Coverage, which may provide coverage for loss of and damage to money, securities and other property following and directly related to the use of any computer to fraudulently cause a transfer of that property. It should be noted that policyholders may also look to other policies that may afford coverage, either in the coverage form or by endorsement, for fraudulent instructions, forgery, or alteration. An insured's ability to recover under a policy hinges on the policy language, the nature of the fraud, and the controlling law applied by a court to resolve any coverage issues.

Certain issues often arise in disputes over wire transfer fraud claims. Courts have grappled with these topics in reaching coverage decisions.

Whether the Insured "Held" the Funds

In some cases, coverage turned on whether the funds involved were "held" by the insured in a way and to an extent required by the subject policy and thus were covered "property" of the insured. For example, the federal district court for the Northern District of Texas[1] considered whether the insured had authority to direct the transfer of funds in an account at its third-party vendor, who provided payment processing services to the insured. A threat actor used a phishing scheme to obtain the account credentials of an employee of the insured and used the credentials to access the vendor's "dashboard" to alter the insured's payment information. The court held that, because the funds were in the vendor's account, and not the insured's, the insured did not "hold" the funds that were transferred using the fraudulent instructions. This decision is on appeal to the federal 5th Circuit Court of Appeals. The federal 9th Circuit[2] reached a similar conclusion where the insured accounting firm used fraudulent instructions believed to have come from its client to initiate a wire transfer from the client's account. The court denied coverage, but noted that the outcome may have been different if the "hacker had entered into [the insured's] computer system and been able to withdraw funds such that [the insured's] accounts were immediately depleted."[3]

"Directly Related to the Use of a Computer"

Another issue courts may have to decide is whether the particular loss "result[ed] directly from" or was "directly related" or "directly caused" by the "use" of a computer. In the past few years, a notable amount of case law has developed concerning this causation issue. Two distinct views have emerged with various courts in each camp. There are differences among the decisions and are influenced by the particular policy language and facts of an incident. However, one group generally posits that fraudsters' use of computers to dupe unwitting targets is "directly related" to those targets' loss of funds, even if there were intervening and otherwise genuine actions taken by people taken in by the schemes and even if those actions occur over time. The other group broadly concludes that the use of a computer is or may be tangential and that the losses instead "directly result" from the impersonation of a known or trusted person or entity by the perpetrators causing authorized people to make legitimate payments, unfortunately, to accounts controlled by the thieves.

The federal 6th Circuit Court of Appeals provides an example of the first view which favors coverage. The insured received emails that appeared to be from one of its vendors, it authorized payments to a bank account it believed belonged to the vendor once it verified that certain production milestones had been met. The emails were fraudulent and the payments were received by the fraudsters rather than the insured's vendor. The insurer denied coverage for the loss. The lower court found for the insurer on the basis of "intervening events", holding that the loss of funds was not "'directly caused' by the use of any computer."[4] The Sixth Circuit, however, reversed the district court's ruling and reasoned that: "[the insured] received the fraudulent email at step one. [The insured's] employees then conducted a series of internal actions, all induced by the fraudulent email, which led to the transfer of the money to the impersonator at step two. This was 'the point of no return,' because the loss occurred once [the insured] transferred the money in response to the fraudulent emails. Thus, the computer fraud 'directly caused' [the insured's] 'direct loss.'"[5] Similar outcomes have been reached by cases in the federal 2nd and 11th Circuit Courts of Appeals and various federal district courts.[6]

The second view tends against coverage and is illustrated by a decision from the federal 5th Circuit Court of Appeals. That court[7] held there was no coverage for the lost funds for a wireless transfer, determining that: "The email was part of the scheme; but, the email was merely incidental to the occurrence of the authorized transfer of money. To interpret the computer-fraud provision as reaching any fraudulent scheme in which an email communication was part of the process would … convert the computer-fraud provisions to one for general fraud."[8] The 5th Circuit also observed that the insured "failed to investigate accurately the new, but fraudulent, information provided to it." The court noted that "viewing the multi-step process in its simplest form, the transfers were made not because of fraudulent information, but because [the insured] elected to pay legitimate invoices. Regrettably, it sent the payments to the wrong bank account. Restated, the invoices, not the email, were the reason for the funds transfers."[9] Other cases have ruled comparably to the 5th Circuit.[10]

Forgery or Alteration

Courts have also considered whether there is coverage for fraudulent wire transfer schemes under forgery or alteration provisions. For example, in[11] the federal district court for the Eastern District of Pennsylvania assessed a policy that included insurance against forgery or alteration which limited coverage to losses from a "financial instrument" defined as "forged or altered checks, drafts, promissory notes, and similar documents directing payment of a sum." Hackers accessed the insured's email system, cut and pasted the insured's officers' signatures onto wire transfer forms; and sent forms to bank. The court denied coverage, holding that the "fraudulent email" is not a "financial instrument".[12]

Exclusions May Bar Coverage

It must be noted that exclusions may operate to preclude coverage regardless of the coverage issues that may arise as noted above. Exclusions vary by policy and so should be carefully reviewed. One example is a "deception fraud" exclusion. The federal district court for the Southern District of New York[13] concluded there was no coverage for the loss of funds occasioned by emails purportedly coming from one of the insured's lawyer's office. The policy's Computer Fraud or Funds Transfer Fraud provisions were subject to an exclusion for "deception fraud", which was defined as "the intentional misleading of a person to induce the Insured to part with Money …" by someone pretending to be, among others, a "vendor", which the court concluding the insured's lawyer is a "vendor".

Another example is an "authorized personnel" exclusion. The federal 9th Circuit Court of Appeals[14] enforced an exclusion that provided that the policy "will not apply to loss or damages resulting directly or indirectly from the input of Electronic Data by a natural person having the authority to enter the Insured's Computer System…." The court held that the exclusion applied to bar coverage where the insured's "losses resulted from employees authorized to enter its computer system changing wiring information and sending four payments to a fraudster's account."

We also highlight that in at least one case,[15] coverage was denied because the subject policy included a coverage territory of the United States, Puerto Rico and Canada. The federal district court for the Eastern District of Virginia determined that the "occurrence" was the threat actor sending the emails containing wiring instructions, and therefore denied summary judgment because there was a genuine issue of fact as to the identity of the threat actor sent the emails and the location from which the emails were sent.[16]

Number of Occurrences

Another issue that may arise in the context of addressing BEC threats is the determination of the number of occurrences. Unfortunately, the discovery of a BEC threat and wire transfer fraud may go undetected for some time, allowing the threat actors to dupe unsuspecting victims into a number of fraudulent transfers. There may therefore be an argument that each wire transfer is a separate occurrence. In a matter[17] in which the insured had received a number of emails, the federal district court for the Eastern District of Virginia observed that:

[I]f a finder of fact found that the same person sent the emails, such that they constitute the same Occurrence under the Policy, then [the insured's] damages would be capped at $1,000,000. However, if the finder of fact found that different people sent the emails, such that more than one Occurrence exists, then [the insured] would be entitled to recover the full amount of its damages, less the amount it recovered … .[18]

Takeaways

In previous articles, we have discussed some measures that entities can take to address the risks of fraudulent wire transfer schemes. We have also discussed other avenues for recourse against entities, such as vendors, who may have experienced an email compromise and who may have been in a better position to take steps to avoid a fraudulent wire transfer. As courts continue to wrestle with coverage issues surrounding fraudulent wire transfer claims, it is clear that uncertainty abounds as to whether policyholders can recover for loss of funds due to

fraudulent wire transfers. Given this uncertainty, policyholders should therefore be aware that constant vigilance to *prevent* fraudulent wire transfer loss in the first instance is a wise investment. When loss is discovered, a policyholders should discuss with its insurance broker timely notice to carriers that issued all potentially implicated policies. Legal actions have been brought against other entities that may have some unintentional connection to a fraudulent wire transfer, such as a vendor whose compromised email account has been used to send fraudulent wire instructions to a customer. The decisions in cases against other entities, and the coverage cases discussed above, suggest that when an entity considers what action to take in response to a fraudulent wire transfer loss, policy language, the particular facts of a case, and the controlling case law all affect whether there may be coverage for a claim.

---

[1] *RealPage Inc. v. Nat'l Union Fire Ins. Co. of Pittsburgh, PA*, No. 3:19-CV-1350-B, 2021 WL 718366, at *8 (N.D. Tex. Feb. 24, 2021), appeal docketed, No. 21- 10299 (5th Cir. Mar 26, 2021) .
[2] *Taylor & Lieberman v. Fed. Ins. Co.*, No. CV 14-3608, 2015 WL 3824130, at *4 (C.D. Cal. June 18, 2015), *aff'd*, 681 F. App'x 627 (9th Cir. 2017).
[3] *Id*.
[4] *Id*. at *2.
[5] *See Am. Tooling Ctr., Inc. v. Travelers Cas. & Sur. Co. of Am*., 895 F.3d 455, (6th Cir. 2018).
[6] *See Medidata Sols., Inc. v. Fed. Ins. Co*., 268 F. Supp. 3d 471, 479 (S.D.N.Y. 2017), aff'd, 729 F. App'x 117 (2d Cir. 2018) ("The Court finds that Medidata's employees only initiated the transfer as a direct cause of the thief sending spoof emails posing as Medidata's president."); *Principle Sols. Grp., LLC v. Ironshore Indem., Inc.*, 944 F.3d 886, 889 (11th Cir. 2019); *Cincinnati Ins. Co. v. Norfolk Truck Ctr., Inc*., 430 F. Supp. 3d 116, 118 (E.D. Va. 2019) (Where the insured received an email containing fraudulent wire instructions that appeared to come from its vendor, the court looked to decision in *American Tooling* to find that the fraud was directly caused by a computer.)
[7] *Apache Corp. v. Great Am. Ins. Co*., 662 F. App'x 252 (5th Cir. 2016).
[8] *Id*. at 258.
[9] *Id*. at 259.
[10] *See InComm Holdings, Inc. v. Great Am. Ins. Co*., No. 1:15-CV-2671-WSD, 2017 WL 1021749 (N.D. Ga., Mar. 16, 2017), aff'd sub nom., 731 F. App'x. 929 (The district court held that the insured's loss did not result "directly" from the fraudulent redemptions of "chits" (prepaid funds loaded onto debit cards) because the losses occurred after the insured wired money to the issuer of the card, after the cardholder used his/her card to pay for a transaction and after the issuer of the card paid the merchant for the cardholder's transaction . The Eleventh Circuit agreed that the loss did not result directly from the initial computer fraud .); *Ernst & Haas Mgmt. Co., Inc. v. Hiscox, Inc*. , No. CV2004062ABPVCX, 2020 WL 6789095, at *3 (C.D. Cal. Nov. 5, 2020), *appeal docketed*, No. 20-56212 (9th Cir. Nov. 18, 2020) (The court determined that, although the imposter's fraudulent email was likely sent through a computer, the insured's claimed losses did not "flow immediately" and "directly" from imposter's use of a computer as the insured "authorized its bank to initiate the wire transfers from its account, albeit through an unwitting employee".); *Mississippi Silicon Holdings, LLC v. AXIS Ins. Co*., 440 F. Supp. 3d 575, 582 (N.D. Miss. 2020), *aff'd sub nom*., 843 F. App'x 581 (5th Cir. 2021) (no coverage under Computer Fraud or Funds Transfer Fraud provisions where insured's employees, not the fraudulent emails themselves, actually initiated the transfer); *Sanderina, LLC v. Great Am. Ins. Co*., No. 218CV00772JADDJA, 2019 WL 4307854, at *3 (D. Nev. Sept. 11, 2019) (where computer fraud provision covered losses "resulting directly from the use of any computer to impersonate you, or your authorized officer or employee, to gain direct access to your computer system, or to the computer system of your financial institution, and thereby fraudulently cause the transfer of money….", a threat actor's email to the insured's controller was not computer fraud).

[11] *Ryeco, LLC v. Selective Ins. Co*., No. CV 20-3182, 2021 WL 1923028, at *1 (E.D. Pa. May 13, 2021).
[12] *See also Midlothian Enterprises, Inc. v. Owners Ins. Co*., 439 F. Supp. 3d 737, 743 (E.D. Va. 2020) (a "covered instrument" under a forgery or alteration provision does not include a fraudulent email).
[13] *Children's Apparel Network Ltd. v. Twin City Fire Ins. Co*., No. 18 CIV. 10322, 2019 WL 3162199, at *3 (S.D.N.Y. June 26, 2019).
[14] *Aqua Star (USA) Corp. v. Travelers Cas. & Sur. Co. of Am*., 719 F. App'x 701, 702 (9th Cir. 2018).
[15] *Quality Plus Servs., Inc. v. Nat'l Union Fire Ins. Co. of Pittsburgh, PA*., No. 3:18CV454, 2020 WL 239598, at *9 (E.D. Va. Jan. 15, 2020).
[16] *Id*. at *9.
[17] *Id*. at *2.
[18] *Id*. at *9. *See also Ad Advert. Design, Inc*., 344 F. Supp. 3d at 1184 ("The unresolved question the parties are directed to address is whether [the] loss is a single occurrence … or if the loss is comprised of four separate occurrences …."); *AIMS Ins. Program Managers Inc. v. Nat'l Fire Ins. Co. of Hartford*, No. 1 CA-CV 20-0032, 2021 WL 408874, at *3 (Ariz. Ct. App. Feb. 4, 2021) (not published) ("Each email package represented a separate fraudulent payment demand, and each resulted in a separate wire transfer by AIMS, the victim of the fraud. In the language of the computer fraud endorsement, each of the three wire transfers "result[ed] directly from" a separate and distinct fraudulent payment demand by the thieves.").

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber