FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

ERNST AND HAAS MANAGEMENT COMPANY, INC., *Plaintiff-Appellant*, v. HISCOX, INC., Erroneously Sued As Hiscox Insurance Company Inc., *Defendant-Appellee*, and DOES, 1 through 10, *Defendants.*	No. 20-56212 D.C. No. 2:20-cv-04062-AB-PVC OPINION

Appeal from the United States District Court
for the Central District of California
Andre Birotte, Jr., District Judge, Presiding

Argued and Submitted October 19, 2021
Pasadena, California

Filed January 26, 2022

Before: Ryan D. Nelson and Lawrence VanDyke, Circuit Judges, and Karen E. Schreier,* District Judge.

Opinion by Judge VanDyke

SUMMARY**

Insurance Law

The panel reversed the district court's order dismissing Ernst and Haas Management Company, Inc.'s diversity insurance coverage action, and remanded for further proceedings.

Hiscox, Inc. sold Ernst a commercial crime insurance policy in 2012. In 2019, an Ernst accounts payable clerk, in response to a fraudulent email, wired payments to a fraudulent actor she believed to be the founder and managing broker of Ernst. In 2019, Ernst submitted a $200,000 claim under the policy. Hiscox denied Ernst's claim because purportedly the funds transfer fraud portion of Ernst's policy did not cover the fraud here because an employee had taken action to initiate the wire transfer.

Two provisions of the parties' 2012 insurance policy were disputed: the "Computer Fraud" provision, and the "Funds Transfer Fraud" provision.

* The Honorable Karen E. Schreier, United States District Judge for the District of South Dakota, sitting by designation.

** This summary constitutes no part of the opinion of the court. It has been prepared by court staff for the convenience of the reader.

The panel held that the district court erred when it held that neither disputed provision in the 2012 crime insurance policy covered Ernst's $200,000 loss.

First, the district court incorrectly interpreted the 2012 Computer Fraud provision for two reasons: (1) the district court wrongly relied on facts analyzed in *Pestmaster Servs., Inc. v. Travelers Cas. & Sur. Co. of Am.,* 656 Fed. App'x 332 (9th Cir. 2016), which were dispositively different than the facts here; and (2) improper reliance on *Pestmaster*'s embezzlement-based analysis led to a flawed interpretation of the computer fraud provision and how it applied to the pleaded facts of this case. Here, Ernst immediately lost its funds when the funds were transferred as directed by the fraudulent email, and there was no intervening event. The panel held that, taking the pleaded facts as true, Ernst suffered a loss resulting "directly" from the fraud, arguably entitling Ernst to coverage under the policy. The panel remanded with instructions to reconsider the case with the recognition that Ernst's loss fell within the Computer Fraud provision of the 2012 policy.

The panel held that the Funds Transfer provision also covered Ernst's loss resulting directly from the fraudulent email instruction. The district court erred when it reasoned that Ernst's alleged loss did not result directly from fraudulent instructions. Here, the fraudulent email directed the Ernst employee to transfer funds, provided wire details, and provided fraudulent authorization. The Ernst employee initiated a wire pursuant to the fraudulent authorization, resulting in Ernst's loss. The panel remanded with instructions to reconsider the case with recognition that, under the facts as alleged by Ernst, Ernst's loss fell within the Funds Transfer fraud provision in the 2012 policy.

COUNSEL

Robert L. Bastian Jr. (argued), and Marina R. Dini, Law Offices of Bastian & Dini, Beverly Hills, California, for Plaintiff-Appellant.

Albert K. Alikin (argued), Joseph A. Oliva (argued), and Kent V. Grover, Goldberg Segalla LLP, Los Angeles, California, for Defendant-Appellee.

OPINION

VANDYKE, Circuit Judge:

Ernst and Haas Management Company, Inc. (Ernst) appeals the district court's order dismissing this action pursuant to Fed. R. Civ. P. 12(b)(6). On appeal, we must decide whether the district court incorrectly interpreted the "Computer Fraud" and "Funds Transfer Fraud" provisions in a 2012 commercial crime insurance policy issued to Ernst by Hiscox, Inc. The parties dispute whether these provisions cover funds lost by an Ernst employee who was directed by fraudulent email requests and payment invoices to transfer the funds to a swindling third party. The district court, relying on a distinguishable unpublished case, found that neither provision covered Ernst because Ernst's alleged loss resulted from an employee initiating a wire, not from the fraudulent email directing her to do so. But the insurance policy itself is not so limited. We reverse the district court's decision because both disputed provisions could cover Ernst's alleged loss.

BACKGROUND

I. Ernst Loses $200,000 After Receiving Fraudulent Emails Directing an Employee to Transfer Funds.

Ernst is a property management company located in California. Hiscox is an insurance company, who sold Ernst a Commercial Crime Insurance Policy in 2012. In 2019, Ernst suffered a loss and submitted a claim under the policy.

At the time, Krystale Allen was an Accounts Payable Clerk for Ernst. On March 12, 2019, Allen received an email purporting to be from her superior, David Haas, directing her to make a payment. As the accounts payable clerk, Allen regularly disbursed payments according to Ernst's protocols. But this email was different. Unbeknown to Allen, the email was sent by a fraudulent actor (Fake David). And unfortunately for Allen, she believed the email was authentic and from the founder and managing broker of Ernst, David Haas (Real David). The email included an invoice for $50,000, which Allen was directed to pay to Zang Investments, LLC (Zang) by wire transfer. Believing the email instruction was from Real David, Allen processed the payment by wire transfer to Zang.

After the first transfer, Allen received two more email instructions from Fake David, for payments of $150,000 and $470,000. Allen completed the same steps for the $150,000 payment and wired the money to Zang. But before authorizing the $470,000 payment, Allen's suspicions were raised, and she emailed Real David to confirm the authenticity of the invoice. Upon receiving Allen's email, Real David informed her that he had not requested the prior transfers. Allen attempted to stop the previous wire payments from the bank, but because the $50,000 and

$150,000 wire transfers had already been completed, Ernst could not recover the funds.

II. Hiscox Denies Ernst's $200,000 Claim for Computer Fraud and Funds Transfer Fraud.

As mentioned above, Ernst had contracted with Hiscox for a Crime Insurance Policy in 2012. The insurance policy included coverage for computer fraud and funds transfer fraud. After realizing it could not recover the funds it lost in March 2019 from the bank, Ernst filed a claim under the policy. Hiscox denied Ernst's claim on June 10, 2019. Hiscox stated that the funds transfer fraud portion of Ernst's policy did not cover the fraud here because an employee had taken action to initiate the wire transfer. Ernst challenged the denial, but Hiscox replied that Ernst should have purchased more comprehensive coverage. At this point, Ernst realized that Hiscox was relying on language from an updated policy that (in Ernst's view) reduced coverage (the 2019 policy). Ernst believes it was not given the notice required by California law of any change, and thus as a matter of California law the 2012 policy governs the dispute, and that the 2012 policy covers its loss.[1]

III. The Disputed 2012 Crime Insurance Policy

While the parties disagree whether the 2012 policy or the updated 2019 policy governs the instant dispute, the district court avoided addressing that disagreement by assuming Ernst was correct that the 2012 policy applies, and interpreting only that policy in its dismissal order. As noted

[1] Because the district court limited its review to the 2012 policy, this opinion does not consider the 2019 policy. If necessary, the district court can address that policy in the first instance on remand.

above, two provisions in the 2012 policy are disputed, the "Computer Fraud" provision and the "Funds Transfer Fraud" provision.[2] The provisions state:

Insuring Agreements

> Coverage is provided under the following Insuring Agreements for which a Limit of Insurance is shown in the Declarations and applies to loss that You sustain resulting directly from an Occurrence taking place at any time which is Discovered by You or an Executive Employee during the Policy Period shown in the Declarations or during the period of time provided in the Extended Period To Discover Loss Condition:
>
> * * *
>
> **Coverage D: Computer and Funds Transfer Fraud**
>
> (1) Computer Fraud
>
> > [The insurance company] will pay for loss of or damage to [currency, coins, bank notes, bullion, checks, money orders], [negotiable or nonnegotiable instruments or contracts representing either currency, [etc.], or property], and/or [any other tangible property] resulting directly from the use of any computer to fraudulently cause a transfer

[2] Relevant portions of the policy quoted herein are reformatted to include referenced definitions in brackets for improved readability.

of that property from inside the [interior of any building Ernst or a subsidiary occupies in conducting Ernst's business] or [the interior of that portion of any building containing a financial institution or similar safe depository]:

i) To a person (other than [Ernst, a Partner, a Member, or an Employee]) outside [the interior of any building Ernst or a subsidiary occupies in conducting Ernst's business] or [the interior of that portion of any building containing a financial institution or similar safe depository]; or

ii) To a place outside [the interior of any building Ernst or a subsidiary occupies in conducting Ernst's business] or [the interior of that portion of any building containing a financial institution or similar safe depository].

(2) Funds Transfer Fraud

[The insurance company] will pay for loss of [currency, coins, bank notes, bullion, checks, money orders] and [negotiable or nonnegotiable instruments or contracts representing either currency, [etc.], or property] resulting directly from a [Fraudulent Instruction] directing a financial institution to transfer, pay or deliver

[currency, coins, bank notes, bullion, checks, money orders] and [negotiable or nonnegotiable instruments or contracts representing either currency, [etc.], or property] from [an account maintained by Ernst at a financial institution from which Ernst can initiate the transfer, payment, or delivery of [currency, coins, bank notes, bullion, checks, money orders] or [negotiable or nonnegotiable instruments or contracts representing either currency, [etc.], or property]].

* * *

Fraudulent Instruction means:

(i) an electronic, telegraphic, cable, teletype, telefacsimile or telephone instruction which purports to have been transmitted by You, but which was in fact fraudulently transmitted by someone else without Your knowledge or consent;

(ii) a written instruction (other than those described in Coverage B) issued by You, which was forged or altered by someone other than You without Your knowledge or consent, or which purports to have been issued by You, but was

> in fact fraudulently issued without Your knowledge or consent; or
>
> (iii) an electronic, telegraphic, cable, teletype, telefacsimile, telephone or written instruction initially received by You which purports to have been transmitted by an Employee but which was in fact fraudulently transmitted by someone else without Your or the Employee's knowledge or consent.

Ernst contends that the above provisions entitle it to coverage for its loss of $200,000, while Hiscox maintains that the provisions do not entitle Ernst to any coverage for its loss.

IV. Procedural History

On May 1, 2020, Ernst filed a lawsuit against Hiscox asserting claims for breach of contract, breach of the implied covenant of good faith and fair dealing, tortious breach of the implied covenant of good faith and fair dealing, bad faith, and unfair trade practices. Hiscox moved to dismiss the Complaint on June 30, 2020. On November 5, the Court granted Hiscox's motion and dismissed the Complaint in its entirety. Ernst appealed and on December 3, 2020, the court entered a final judgment and dismissed the case, priming it for appellate review.

JURISDICTION AND STANDARD OF REVIEW

This court has jurisdiction under 28 U.S.C. § 1291. "We review de novo an order granting a motion to dismiss under

Federal Rule of Civil Procedure 12(b)(6) for failure to state a claim, accepting as true all well-pleaded allegations of material fact and construing those facts in the light most favorable to the non-moving party." *Judd v. Weinstein*, 967 F.3d 952, 955 (9th Cir. 2020). "[D]ismissal is affirmed only if it appears beyond doubt that [the] plaintiff can prove no set of facts in support of its claims which would entitle it to relief." *City of Almaty v. Khrapunov*, 956 F.3d 1129, 1131 (9th Cir. 2020) (citation, internal alternations and quotation marks omitted). "It is axiomatic that the motion to dismiss . . . is viewed with disfavor and is rarely granted." *McDougal v. Cnty. of Imperial*, 942 F.2d 668, 676 n.7 (9th Cir. 1991) (citation, internal alterations and quotation marks omitted).

DISCUSSION

We must decide whether the district court erred when it held that neither disputed provision in the 2012 crime insurance policy covered Ernst's $200,000 loss. The district court found that Ernst's alleged loss did not result directly from fraudulent emails instructing an Ernst employee to transfer funds to a deceptive third party. And because the court reasoned that both the computer fraud and funds transfer fraud provisions required the loss to result directly from the fraudulent emails, it found neither provision applied to Ernst.

The district court erred for three reasons. First, the court analyzed this case as if it involved theft of funds authorized for payment, like the unpublished *Pestmaster* decision on which the court relied. *See Pestmaster Servs., Inc. v. Travelers Cas. & Sur. Co. of Am.*, 656 Fed. App'x. 332 (9th Cir. 2016); *see also Pestmaster Servs., Inc. v. Travelers Cas. & Sur. Co. of Am.*, No. CV 13-5039-JFW, 2014 WL 3844627, at *1 (C.D. Cal. July 17, 2014). But for the reasons

explained below, it doesn't. Second, the district court interpreted the computer fraud provision to mean a direct loss is limited to unauthorized computer use, like hacking. But that is an improperly narrow reading of the contractual language. And third, the district court incorrectly limited funds transfer fraud to exclude fraudulent instructions to an Ernst employee. But the language of the policy is not so limited. Because the district court erred in dismissing the case, we reverse and remand.

I. The District Court Incorrectly Interpreted the 2012 Computer Fraud Provision.

The district court's interpretation of the computer fraud provision was wrong for two reasons: (1) the district court wrongly relied on facts analyzed in *Pestmaster*, which are dispositively different than the facts here, and (2) improper reliance on *Pestmaster*'s embezzlement-based analysis led to a flawed interpretation of the computer fraud provision and how it applies to the pleaded facts in this case.

A. The District Court Erred by Relying on the Facts in *Pestmaster* Instead of Applying the Hiscox Policy's Terms to the Facts Pleaded in this Case.

As a threshold matter, the district court erred by solely relying on *Pestmaster* to interpret the Hiscox policy, because the embezzlement addressed in that unpublished decision was dispositively different than the third-party email fraud committed in this case.

In *Pestmaster*, a third-party contracted with Pestmaster to provide payroll tax services. *Pestmaster*, 2014 WL

3844627, at *1.[3] Every payroll period, the contractor was authorized to transfer a specific amount of money from Pestmaster's accounts to pay taxes. *Id.* At some point, though, the contractor began stealing some of the money it was authorized to pay, essentially embezzling money with which it had been entrusted. *Id.* at *2. Pestmaster filed a lawsuit after Travelers denied coverage for the loss under a crime insurance policy. *Id.* On appeal, our court held that the computer fraud provision in Pestmaster's policy did not cover the stolen funds because the funds were transferred by the contractor "pursuant to authorization from" the insured, and *then* stolen. *Pestmaster*, 656 Fed. App'x at 333.

The facts in this case are materially different. Ernst did not authorize Zang to pay its bills and Zang did not steal funds it was ever authorized to receive. Instead, Fake David sent an email *fraudulently authorizing* an Ernst employee (Allen) to pay Zang based on a fraudulent invoice. The district court held that because Allen requested a wire transfer to Zang, the transfer was "authorized" in the same way as the payments in *Pestmaster*. But initiating a wire transfer is not the same as authorizing a payment. Unlike in *Pestmaster*, neither Zang nor Allen was ever *properly* authorized to pay anyone the $200,000 that Ernst lost. To the contrary, the entire purpose of Fake David's email invoice was to provide *fraudulent* authorization.

If Ernst had authorized Allen to pay a third party $200,000 and Allen then stole some of that money, then this case might be analogous to *Pestmaster*. But no party alleged those facts, nor does Ernst allege Allen acted dishonestly or

[3] Because our court's *Pestmaster* decision was unpublished, these facts are drawn primarily from the district court order underlying our court's decision.

somehow embezzled the money.[4] Given that this case is about an email fraud scheme, the district court erred by relying on *Pestmaster* to interpret the policy as if the case were about embezzlement.

B. The 2012 Policy's Computer Fraud Provision Covers Ernst's Loss Resulting Directly from Fake David's Email Instruction.

Because *Pestmaster* is non-binding and the court's reasoning distinguishable, we must decide whether the district court's reliance on that case flawed its interpretation of the disputed policy provisions. It did.

The computer fraud provision states Hiscox will cover loss "resulting directly from the use of any computer to fraudulently cause a transfer of that property from" Ernst to a person or location outside of Ernst. The district court erred by limiting its interpretation of a loss "result[ing] directly from use of a computer to fraudulently cause transfer" to only a loss resulting directly from unauthorized use of Ernst's computers or hacking. The district court's interpretation that Ernst's alleged loss did not result "immediately" and "directly" from computer fraud because Ernst, through Allen, "authorized its bank to initiate the wire

[4] Similarly, *Vons Co., Inc. v. Fed. Ins. Co.*, 212 F.3d 489 (9th Cir. 2000), does not apply here because the policy in that case required any loss be caused by employee dishonesty (i.e., an embezzlement policy), rather than resulting from the use of a computer for fraud. *Vons* illustrates that where a company is seeking insurance coverage under an embezzlement policy, such claims should be strictly construed. We won't broadly construe employee misconduct as embezzlement in order to force coverage for a broad range of employee torts under a narrow embezzlement policy. Because this case does not involve an embezzlement policy, *Vons* is not particularly relevant.

transfers from its account, albeit through an unwitting employee," eliminates the possibility of coverage *whenever* an employee is defrauded into taking an action. By relying on *Pestmaster* to reach this conclusion, the district court endorsed a faulty circular premise—that Allen "authorized" a transfer of $200,000, curing any prior fraud, when she initiated a transfer of $200,000 *based on fraud*. That reasoning—that this fraud became "authorized" precisely when it succeeded—cannot be the correct reading of the contract.

On this point, we find the Sixth Circuit's *American Tooling* decision persuasive and much more on-point than any of the Ninth Circuit cases cited by Hiscox. In *Am. Tooling Center, Inc., v. Travelers Cas. & Sur. Co. of Am*., a company named "ATC received a series of emails, purportedly from its Chinese vendor, claiming that the vendor had changed its bank accounts and ATC should wire transfer its payments to these new accounts." 895 F.3d 455, 457 (6th Cir. 2018). ATC then went through a multi-step authorization process on three different occasions, ultimately transferring more than $800,000 in funds. *Id.* at 458. Upon learning that the emails from the vendor were actually fraudulent emails from an imposter, ATC sought coverage for the loss under a Traveler's insurance policy. *Id.* The computer fraud provision of ATC's policy stated:

> The Company will pay the Insured for the Insured's direct loss of, or direct loss from damage to, Money, Securities and Other Property directly caused by Computer Fraud.

Id. at 459. ATC and Travelers disagreed about whether the wire transfers to the imposter were considered a "direct loss" of ATC's money under the provision. *Id.* The court found

that ATC "immediately lost its money when it transferred the approximately $834,000 to the impersonator; there was no intervening event." *Id*. at 460. Therefore, ATC had suffered a direct loss.

Here, the computer fraud provision provides that Ernst's loss must "result directly" from the fraud. In other words, like ATC, Ernst must suffer a direct loss. And like ATC, Ernst immediately lost its funds when those funds were transferred to Zang as directed by the fraudulent email. There was no intervening event—Allen acting pursuant to the fraudulent instruction "directly" caused the loss of the funds. Thus, taking the pleaded facts as true, Ernst suffered a loss resulting "directly" from the fraud, arguably entitling Ernst to coverage under the policy.[5] So here, as in *American Tooling*, we cannot conclude that Ernst's alleged immediate loss of funds based on the fraudulent email was not "direct." *Id.* at 461. Accordingly, we reverse the district court and remand with instructions to reconsider the case with the recognition that, under the facts as alleged by Ernst, Ernst's loss falls within the computer fraud provision of the 2012 policy.

[5] The alleged loss here was arguably *more* direct than the loss in *American Tooling* because the requested payments in that case were identical to amounts ATC owed an innocent third party and ATC had authorized payment in those amounts. Here, Ernst had not contracted with another party for the exact amounts requested in the emails and Allen acted solely and directly as a result of the fraudulent payment authorization.

II. The Funds Transfer Fraud Clause Also Covers Ernst's Loss Resulting Directly from Fake David's Email Instruction.

Even if Ernst's injury was not covered under the computer fraud provision of the 2012 policy, it is likely covered under the same policy's funds transfer fraud provision. The district court erred when it reasoned that Ernst's alleged loss did not result directly from fraudulent instructions because Fake David's "communications did not direct [Ernst's] bank to transfer the $200,000 [Ernst] now seeks to recover," but instead directed Allen to direct Ernst's bank to transfer the money. The district court's interpretation overlooks the express language of the policy, which states that funds transfer fraud includes not only fraudulent instructions sent directly to a bank, but also fraudulent instructions initially received by an employee. Either type of fraudulent instruction that results in "directing" a financial institution to transfer funds is covered by the policy.

Funds transfer fraud covers "loss of Money and Securities resulting from a Fraudulent Instruction directing a financial institution to transfer, pay or deliver Money and Securities from Your Transfer Account." Importantly, the definition of fraudulent instruction includes three different definitions. The third definition states that a fraudulent instruction includes "an electronic . . . instruction *initially received by You* which purports to have been transmitted by an Employee but which was in fact fraudulently transmitted by someone else without Your or the Employee's knowledge or consent."

This language is nearly identical to the fraudulent instruction definition considered by the Eleventh Circuit in *Principle Solutions Group, LLC v. Ironshore Indemnity*,

944 F.3d 886 (11th Cir. 2019).[6] Relying on *Principle Solutions*, Ernst argues that the fraudulent email here was a "fraudulent instruction" that "directed a financial institution" to transfer funds and should be covered by the policy because "[e]very action [Allen] took to facilitate the transfer of funds was the direct result of having been duped by the fraudster's email." Hiscox disagrees and argues that because the fraudulent emails here were sent to the insured rather than directly to a financial institution without Ernst's knowledge, Ernst is not covered under the policy.

We find *Principle Solutions* persuasive. In *Principle Solutions*, the Eleventh Circuit resolved a similar disagreement and 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. 944 F.3d at 890. The email directed Principle's financial controller to transfer money from Principle's account, provided payment details, and provided fraudulent authorization to transfer the funds. *Id.* at 890–91. The court reasoned that such an email, which instructed a Principle employee to initiate a wire, could not be construed as doing anything but "directing a financial institution" to transfer funds. *Id.*

Here, Fake David directed Allen to transfer funds to Zang, provided wire details, and provided fraudulent authorization. Allen initiated a wire pursuant to the fraudulent authorization, resulting in Ernst's loss. The sole

[6] In *Principle Solutions*, the court reviewed the following definition of fraudulent instruction: "[an] electronic or written instruction initially received by [insured], which instruction purports to have been issued by an employee, but which in fact was fraudulently issued by someone else without [insured's] or the employee's knowledge or consent." 944 F.3d at 890.

purpose of Fake David's email was to instruct Allen to initiate a wire. As in *Principle Solutions*, we would be "hard pressed to construe the email as doing anything but directing a financial institution to debit [Ernst's] transfer account and transfer . . . money . . . from that account." 944 F.3d at 890. Otherwise, the relevant portion of the 2012 policy's fraudulent instruction definition—which anticipates an instruction sent to the insured *before* the bank—is superfluous. On this point too, we reverse the district court and remand with instructions to reconsider the case with the recognition that, under the facts as alleged by Ernst, Ernst's loss falls within the funds transfer fraud provision of the 2012 policy.

CONCLUSION

The judgment of the district court granting Hiscox's motion to dismiss and dismissing Ernst's complaint with prejudice is **REVERSED AND REMANDED** for further proceedings consistent with this opinion.[7]

[7] Because appellee argues changes to the 2019 policy preclude coverage, on remand the district court should consider in the first instance whether Ernst received adequate notice of the 2019 policy changes under California law, and if not, the consequence of the inadequate notice. This panel does not reach and takes no position on those questions.