Filed 5/27/25

CERTIFIED FOR PUBLICATION

COURT OF APPEAL, FOURTH APPELLATE DISTRICT

DIVISION ONE

STATE OF CALIFORNIA

BRIAN THOMAS, Plaintiff and Respondent, v. CORBYN RESTAURANT DEVELOPMENT CORP et al., Defendants and Appellants.	D083655 (Super. Ct. No. 37-2021-00047188-CU-PO-NC)

APPEAL from a judgment of the Superior Court of San Diego County, Robert P. Dahlquist, Judge. Affirmed.

Tyson & Mendes, Molly A. Gilardi, Mitchell B. Malachowski and Daniel P. Fallon for Defendants and Appellants.

O'Hagan Meyer, Angeli Aragon and Matthew E. Szwajkowski for Plaintiff and Respondent.

INTRODUCTION

This case presents an issue of first impression in California: Which party bears the risk of loss when an imposter causes one party to a settlement to wire settlement proceeds to the imposter instead of the other settling party? After plaintiff and defendants settled a personal injury lawsuit for $475,000, an unknown third party purporting to be plaintiff's

counsel sent "spoofed" emails[1] to defendants' counsel providing fraudulent wire instructions for the settlement proceeds. Defendants' counsel wired the settlement proceeds to the fraudulent account and the third party absconded with the funds. Once the fraud was discovered, plaintiff asked for the settlement money, but defendants refused to pay. Plaintiff then applied ex parte to enforce the settlement agreement.

Noting the lack of California authority discussing this topic, the trial court applied persuasive federal case law that uniformly shifts the risk of loss to the party in the best position to prevent the fraud. (See, e.g., *Beau Townsend Ford Lincoln, Inc. v. Don Hinds Ford, Inc*. (6th Cir. 2018) 759 Fed.Appx. 348, 359 (*Beau Townsend Ford*); *Ostrich Int'l Co., LTD v. Michael A. Edwards Grp. Int'l Inc*. (C.D. Cal., May 18, 2023, No. 2:21-cv-00639-JVS(ASx)) 2023 U.S. Dist. LEXIS 105828, p. *10 (*Ostrich*).) After "[l]ooking at the totality of the circumstances," the trial court found "defendants were in the best position to prevent the fraud" and that plaintiff bore no "comparative fault." The court granted plaintiff's application to enforce the settlement and entered judgment in his favor for $475,000.

On appeal, defendants maintain the trial court chose the correct law to apply but applied it incorrectly by mischaracterizing the evidence that supported shifting the blame to defendants, and by failing to consider the evidence that supported shifting the blame to plaintiff. Defendants assert that by doing so, the trial court undertook an overly simplistic analysis that presumed "the payor is . . . in the best position to avoid . . . fraud." We agree that the authority on which the trial court relied is persuasive but we disagree that the court misapplied it. The record shows that the trial court assessed each party's role in preventing the fraud. Substantial evidence supports the court's findings that several red flags should have alerted defendants to the fraud, and that there were none that should have alerted plaintiff.

Accordingly, we affirm the judgment.

FACTUAL AND PROCEDURAL BACKGROUND

The Lawsuit and Settlement

Plaintiff Brian Thomas (Plaintiff) sued defendants Corbyn Restaurant Development Corp. dba Cowshed Bar & Grill, Nicole Nocentino, and Jaime Lee Masters (together, Defendants) for personal injuries Plaintiff allegedly sustained during an altercation with Nocentino and Masters, employees of the corporate defendant's

---

[1] According to the Federal Bureau of Investigation (FBI), "[s]poofing is when someone disguises an email address, sender name, phone number, or website [address] — often just by changing one letter, symbol, or number — to convince you that you are interacting with a trusted source." (FBI: Spoofing and Phishing <https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/spoofing-and-phishing> [as of May 13, 2025], archived at: <https://perma.cc/R75B-2VED>.)

establishment. The Law Offices of Chambers & Noronha represented Plaintiff. Daniel Fallon of Tyson & Mendes, LLP, represented Defendants.

After a mediation, the parties settled their dispute for $475,000. Their understanding was memorialized in a formal Settlement Agreement and Release (Settlement Agreement) that included these key provisions:

> "3. In consideration of the promises, conditions and Release set forth herein, Defendants shall cause payment to be made to Plaintiff in the sum total of Four Hundred Seventy-Five Thousand Dollars and Zero Cents ($475,000.00) (the 'Settlement Payment'). Issuance of the Settlement Payment is conditioned on receipt of this fully executed Release.
>
> "4. Upon receipt of this fully executed Release the Settlement Payment shall become due and payable within thirty days. The Settlement Payment is to be issued to: 'Chambers and Noronha Client Trust Account for the benefit ('FBO') Brian Thomas.' "

Communications Regarding the Settlement Payment

Plaintiff's counsel sent the signed Settlement Agreement to Defendants' counsel via email on August 28, 2023. The email came from the law firm's office administrator, Janette Mattson, specifying: "Please make the check payable to our client and the Chambers & Noronha Client Trust Account." Mattson also requested a "possible ETA for the check." Mattson's email address was "jcmattson@cnlegalgroup.com." Her email signature included her correct email address, the firm's correct physical and website addresses, and the office phone number "(714) 558-1400."

Defendants' attorney, Fallon, replied the same day by email stating he would "advise once [he] ha[s] a better sense of timing on [the] settlement funding." Fallon's email address used the domain "@tysonmendes.com."

About one week later, on September 6, an email purporting to be from Mattson to Fallon asked, "[C]an we have the settlement funds sent electronically into my firm's IOLTA rather than sending a check?" However, this email came from "jmattson@cnlegalrgroup.com." The "spoofed" address differed from Mattson's authentic email address in two ways: it omitted the letter "c" from Mattson's username and added the letter "r" between "cnlegal" and "group" in the domain.[2] The signature in the fake Mattson email showed Mattson's correct email address and the firm's correct physical and website addresses but incorrect phone and fax numbers, respectively, "(714) 554-1500" and "(714) 558-0895." An identical email was sent eight minutes after the original. Both emails used the recipients' correct "@tysonmendes.com" domain.

---

[2] To demonstrate, "jcmattson@cnlegalgroup.com" became "jmattson@cnlegalrgroup.com."

That same day, September 6, Fallon replied to the spoofed Mattson email as follows: "I will look into your request so we can discuss. Possible the check has already gone out. Also, if we move towar[d] electronic transfer, I would like to discuss over the phone to ensure we are on the same page."

The next morning, on September 7, someone using the fake Mattson email account responded, "If the check has already gone out please disregard the electronic transfer request." This email was addressed to Fallon's correct "@TysonMendes.com" domain and to additional recipients at the spoofed "@cnlegalrgroup.com" domain.

The next day, on September 8 (a Friday), Fallon replied via email: "We are able to transfer the settlement funds electronically. I tried to call the number listed below but get an indication it is inoperable. [¶] Please provide the wire transfer instructions and a number to call to discuss."

Later that evening, a fraudster using the spoofed Mattson email account replied to Fallon as follows: "Sorry for the late response. We will send you the requested instructions accordingly, our firm policy states the finance department handles such information. Mark Anderson our head of finance also cc'd in this email will follow up with you on call [*sic*] and provide the wire instructions." In a separate paragraph, the email stated: "Mark – See below from opposing counsel, please follow up accordingly."

On the morning of the next business day (Monday, September 11), "Mark Anderson" replied by email to Fallon as follows: "Attached is [*sic*] the wire instructions. I can be reached directly on my line below (714) 395-5780 or you give me your number. I will give you a call so we can discuss. Either way is fine with me." The email signature identified "Anderson" as "Head of Finance," included the same phone number he provided in the body of his email message and contained apparently spoofed email and website addresses with the "@cnlegalrgroup.com" domain. Attached to the email were wire instructions to an account named "Chambers & Noronha APC" at "Citi Bank" in Los Angeles.

Accounting personnel from Fallon's firm called and spoke to Anderson at the phone number provided in the fraudulent email. Defense counsel then transferred the settlement proceeds to the account identified in the wire instructions contained in the email.

Then came what appears to be an effort aimed at delaying the Chambers & Noronha firm from suspecting a scam occurred. The same afternoon the funds were conveyed to the imposter's account, a fraudulent email masquerading as one sent from Fallon, but with the spoofed domain "@tysonmenrdes.com" (i.e., with an errant "r"),[3] went to Chambers & Noronha's office administrator, Mattson. The scam email stated: "I wanted to let you know that the settlement check is scheduled to go out this week. I will keep you posted and let you know once it's sent."

---

3 To make clear, the authentic domain is "@tysonmendes.com" while the fraudulent email domain is "@tysonmenrdes.com."

Over the next several weeks, the spoofed Fallon email account and Mattson's authentic email account communicated several times regarding the status of the settlement check. Then communication from the fake Fallon email account stopped. After several weeks of inactivity, Plaintiff's counsel contacted Defendants' counsel telephonically regarding the settlement payment. On October 10, 2023, the parties discovered they had been the victims of a cyber scam and that the settlement proceeds were wired to a fraudulent account.

Ex Parte Application to Enforce the Settlement

About a month after the parties discovered the fraud, Plaintiff still had not received the settlement proceeds, so he applied ex parte for an order enforcing the Settlement Agreement. (See Code Civ. Proc.,[4] § 664.6, subd. (a) ["If the parties to pending litigation stipulate . . . in a writing signed by the parties . . . for settlement of the case, . . . the court, upon motion, may enter judgment pursuant to the terms of the settlement."].) His application recounted the facts summarized above and attached printouts of the relevant email messages. Plaintiff noted that "California has no published authority on fraudulent wire transfers of settlement funds," but noted that federal courts have applied the "Imposter Rule" found in the Uniform Commercial Code (UCC) to shift the burden of loss to the party who had "more opportunity and was in the better position to discover the fraudulent behavior." (*Arrow Truck Sales, Inc. v. Top Quality Truck & Equip., Inc*. (M.D. Fla., Aug. 18, 2015, No. 8:14-cv-2052-T-30TGW) 2015 U.S. Dist. LEXIS 108823, p. *11 (*Arrow Truck Sales*).)

Applying this standard, Plaintiff argued that several red flags put Defendants and their counsel "in a better position to discover the fraudulent behavior." Among those warnings were: (1) the Settlement Agreement specified that payment be made to "Chambers and Noronha Client Trust Account for the benefit ('FBO') Brian Thomas," but the fraudulent wire instructions identified a different payee ("Chambers & Noronha APC"), omitted Plaintiff's name, and specified a bank in Los Angeles even though Plaintiff's counsel are located only in Orange County; (2) the parties had agreed by email that Defendants would deliver the settlement payment by check, but the imposter's email requested payment by wire transfer; (3) the signature in the spoofed emails to Defendants' counsel listed a different phone number than was listed in the signature of prior authentic emails, in written correspondence, and in court filings; (4) when defense counsel attempted to call the imposter, the phone number was inoperable and the imposter again changed the phone number in the spoofed email signature; and (5) the imposter communicated via spoofed email accounts with Defendant's counsel *before* the wire transfer, but the imposter did not begin communicating with Plaintiff's counsel until *after* the wire transfer.

---

4 Undesignated statutory references are to the Code of Civil Procedure.

Defendants filed a preliminary opposition. In a supporting declaration, Fallon explained his firm already notified its "cyber insurance carrier," contacted the bank to which the funds were wired, and "conducted an internal computer forensic analysis on [the firm's] computer systems" that found "no breach." Fallon stated Plaintiff's counsel had "not advised [Fallon's] office of any IT investigation on their end, let alone any results." Defendants requested additional time for further investigation.

The trial court set the matter for hearing one month later to allow for further investigation and briefing, if desired.

Defendants filed a further opposition. Noting the lack of California precedent, Defendants relied on *Beau Townsend Ford*, *supra*, 759 Fed.Appx. 348, in which the Sixth Circuit reversed a summary judgment ruling in a fraudulent wire transfer dispute because the "district court erred by taking an overly simplistic view of th[e] case" that focused strictly on contractual performance (i.e., whether the payor ever paid the actual payee). (*Id*. at p. 357.) Finding that neither side " 'was negligent in the manner that they maintained their e-mail accounts' " (*id*. at p. 355) and that " '[t]hey were both victims of a sophisticated third-party fraudster,' " (*ibid*.) the appellate court reasoned the district court should instead have "determine[d] which party 'was in the best position to prevent the fraud,' " an issue of fact not suitable for resolution on summary judgment. (*Id*. at p. 359.) The court stated that on remand the factfinder "would have to determine whether either [party's] failure to exercise ordinary care contributed to the hacker's success, and would then have to apportion the loss according to their comparative fault." (*Id*. at p. 357.)

Under this analysis, Defendants argued their counsel acted reasonably in preventing the fraud by: (1) attempting to call Plaintiff's counsel to confirm the wire instructions; (2) upon finding the phone number to be inoperable, having accounting personnel call a different number and speak to the purported Head of Finance for Plaintiff's counsel's firm; (3) contacting the bank that received the wire; (4) notifying the firm's cyber insurance carrier; (5) filing a report with the FBI; and (6) having the firm's IT personnel conduct an investigation that ruled out access to defense counsel's systems.[5] Because defense counsel's firm concluded its computer system had not been compromised, Defendants reasoned the fraudulent scheme must have been accomplished by breaking into Plaintiff's counsel's computer system.

Plaintiff filed a reply brief. Citing the recent decision in *Ostrich*, *supra*, 2023 U.S. Dist. LEXIS 105828, which held that "courts may allocate the risk of loss to the party 'best able to avoid it' when 'it is reasonable in the circumstances to do so' " (*id*. at p. *10), Plaintiff reiterated his view that Defendants were the party best able to prevent

---

5 In a supporting declaration, Fallon described the investigation: "My office conducted an internal computer forensic analysis on our computer systems immediately upon notification of the fraud and found no breaches. Specifically, my firm's IT professionals were able to rule out access to my firm's system based upon its verbose access logging and email header tracking from Microsoft."

the loss here. Specifically, Plaintiff cited the following red flags: (1) "The payment instructions changed in four . . . different ways: i) the form of payment; ii) change in the name of the payee; iii) removal of the client's name; and iv) location of [b]ank"; (2) the imposter used spoofed email accounts, "which would have revealed the fraud"; (3) the imposter communicated with Defendants' counsel before the fraudulent wire transfer and did not communicate with Plaintiff's counsel until after the transfer; (4) the imposter sent two identical emails within eight minutes of each other requesting that the settlement funds be wired; (5) Defendants' counsel reached an "inoperable" phone number when he called to confirm the wire transfer; and (6) the imposter changed Plaintiff's counsel's phone number twice during the course of the scheme — first from the correct number to the inoperable one, and then to the one for "Mark Anderson."

Plaintiff also disputed Defendants' "quasi-res ipsa loquitor theory that since their IT department allegedly found no breach, that the only conclusion is the Plaintiff['s] counsel's office was breached." Plaintiff reasoned a breach was unnecessary because the imposter used spoofed email addresses rather than authentic emails sent from Plaintiff's counsel's computer system. In addition, Plaintiff represented that his "counsel's office performed an internal investigation and research on [its] computer system and did not find any breach in [its] system nor [its] email accounts."[6]

Mattson also submitted a declaration asserting that, "[o]n information and belief, upon research and investigation, no breach in our system nor our email accounts was found." She also stated that her firm "has had the same phone number (714) 558-1400 since 1989."

The Trial Court's Ruling

The trial court issued a tentative ruling anticipating it "must decide whether the loss resulting from the cyber-scam here should be allocated based on comparative fault (as indicated in the Sixth Circuit case of [*Beau Townsend Ford*], cited in Defendant's brief) or assigned to the party best able to have avoided the loss (as indicated in the Central District of California case of *Ostrich*, cited in Plaintiff's reply brief)." The court

---

6 One of Plaintiff's attorneys substantiated this claim in a declaration: "I am one of the attorneys responsible for the handling of this matter, and as such, I have personal knowledge of the facts set forth herein, and if called upon, could and would testify to the following: [¶] . . . [¶] After the phone call [from Defendants' counsel disclosing the fraud], [I] directed our office to do an internal investigation and research to determine whether a breach had occurred. On information and belief, there was no breach in our system or email accounts. [¶] . . . [¶] On information and belief, there has never been a breach in our system or email accounts. [¶] . . . [¶] [I] and [my] office . . . have never known, or had any reason to suspect, that any alleged breach occurred during the finalization of the settlement in this matter." The declarant offered no details about how the firm conducted its "internal investigation," who did it, or that person's qualifications.

stated it was "tentatively inclined to conclude that the approach from [*Beau Townsend Ford*] should be followed in this instance."

The court heard Plaintiff's application on December 22, 2023, and issued its ruling in a minute order one month later, on January 22, 2024. The hearing was not reported. The court confirmed in its ruling that "both sides agreed" the "matter would be submitted for decision on the evidentiary record created for th[e] motion," without "further investigations into the scam" and without an evidentiary hearing. The parties did not raise, and the court did not address, any evidentiary objections.

Turning to the merits, the court granted Plaintiff's application. The court noted that one alternative was to resolve the case on "its simplest terms": "[D]efendants agreed to pay plaintiff $475,000 to settle the case. Plaintiff has not been paid the agreed-upon settlement," and therefore "plaintiff should be entitled to a judgment in his favor for the agreed-upon amount of $475,000."

But the court instead conducted the "more nuanced analytical approach" presented in the federal cases the parties cited in their briefing. The trial court explained:

> "The Sixth Circuit, in the [*Beau Townsend Ford*] case, reversed a decision by the district court, indicating that there were triable issues of fact as to 'whether either [party's] failure to exercise ordinary care contributed to the hacker's success.' [Citation.] Once those facts were adjudicated, then the district [court] was required to 'apportion the loss according to [the parties'] comparative fault.' [Citation.] As part of this determination, the district court was required to 'determine which party was in the best position to prevent the fraud.' [Citation.]
>
> "The district court in the [*Ostrich*] case similarly undertook a factual analysis to determine 'who was in the better position to prevent the fraud.' [Citation.]
>
> "Turning to the facts of this case, it is unknown how the fraudster learned of the settlement. But the fraudulent wiring instructions conflicted with the payment procedure established by the parties' written Settlement Agreement and Release. Also, the email containing the wiring instructions contained a telephone number for the purported 'head of finance' of plaintiff's counsel'[s] law firm. A representative from defendants' law firm called that phone number and found that it was inoperable.
>
> "Looking at the totality of the circumstances of this case, the court concludes that defendants were in the best position to prevent the fraud. Also, on this evidentiary record, the court concludes that it is unable to find any comparative fault on the part of plaintiff, so that if

the loss is apportioned according to the parties' comparative fault, defendants are responsible for 100% of the loss.

"Similar to the court in the [*Ostrich*] case, the court here is not finding that any party or lawyer in this case was negligent. The parties and lawyers in this case are victims of a sophisticated scam.

"Therefore, the court will enter a judgment in favor of plaintiff for the agreed-upon settlement amount of $475,000. The court invites plaintiff's counsel to submit a proposed judgment."

Proceedings on the Judgment

Before Plaintiff submitted a proposed judgment, Defendants purported to appeal from the minute order. Defendants also moved ex parte to stay enforcement of the judgment pending perfection of the appeal. The application largely repeated Defendants' earlier arguments.

Plaintiff opposed Defendants' application. Beyond the merits of the statutory stay procedure, Plaintiff argued Defendants had "unclean hands" arising from "unconscionable conduct" following the court's ruling. In a declaration with corroborating emails attached, Plaintiff's counsel explained that Defendants' counsel wrote that he was "working on the settlement draft for the $475,000 so we can wrap things up and avoid the judgment," that Plaintiff's counsel received this payment via check and deposited it in his client trust account, and he was notified the check did not clear because a stop payment order had been placed. Based on this conduct, Plaintiff submitted a proposed judgment awarding him $475,000 plus 10 percent prejudgment interest from the date of the court's minute order (January 22, 2024).

On February 26, 2024, the trial court entered judgment for Plaintiff in the amount of $475,000. The judgment further states that "[a]ny request for prejudgment interest shall be made by noticed motion."

Defendants appealed from the judgment.[7]

DISCUSSION

Standard of Review

Defendants acknowledge the general rule that a "trial court's factual findings on a motion to enforce a settlement under section 664.6 'are subject to limited appellate review and will not be disturbed if supported by substantial evidence.' " (*Critzer*, *supra*, 187 Cal.App.4th at p. 1253.) They argue, however, that we should review the trial court's order de novo because the " 'facts of this case' cited in the court's minute order" show that the court failed to apply the correct law inasmuch as "the court did not consider both party's [*sic*] ordinary care." We disagree. In our view, the trial court chose the correct governing law, which requires a fact-intensive analysis, and correctly applied it to the evidence regarding each party's exercise of ordinary care. Accordingly, we will review the court's ruling for substantial evidence. (See *Beau Townsend Ford*, *supra*, 759 Fed.Appx. at p. 359 ["the factfinder must determine which party 'was in the best position to prevent the fraud' "].)

The Authority on Which the Trial Court Relied is Persuasive

Like the trial court and the parties, we are unaware of any published California authority addressing who bears the risk of loss when a third party fraudulently induces

---

[7] We directed the parties to brief the appealability of the judgment. We have read and considered their briefing and are satisfied the judgment is appealable. First, "a judgment on an order granting a motion to enforce settlement under section 664.6 is appealable." (*Critzer v. Enos* (2010) 187 Cal.App.4th 1242, 1251 (*Critzer*).) Second, even if the judgment were deemed a consent judgment, which ordinarily is not appealable (*Machado v. Myers* (2019) 39 Cal.App.5th 779, 789), it is appealable here because Defendants contend the judgment does not reflect the terms of the parties' settlement with respect to the total settlement consideration owed (i.e., by shifting the risk of loss to Defendants, they contend the judgment requires them to pay twice the amount they agreed to pay) and contemplates an award of prejudgment interest about which the settlement agreement is silent (see *Steinman v. Malamed* (2010) 185 Cal.App.4th 1550, 1555 (*Steinman*) ["While a settlement stipulation results in the waiver of any right to appeal from the judgment entered under the stipulation, it does 'not preclude an appeal to determine whether or not the judgment was authorized by the stipulation.' "]). We discuss the merits of Defendants' contentions in part III.D., *post*. Finally, even if the judgment were not appealable, we would exercise our discretion to address the merits of the fully briefed issue of first impression by treating the opening brief as a writ petition. (See *H.D. Arnaiz, Ltd. v. County of San Joaquin* (2002) 96 Cal.App.4th 1357, 1366–1367; cf. *People v. Djekich* (1991) 229 Cal.App.3d 1213, 1219 ["we elect to treat this matter as a writ of habeas corpus as a matter of judicial economy and efficiency"].)

one party in a transaction to divert to the third party funds that were intended for the other party to the transaction. Several federal courts, however, have considered the issue and uniformly shifted the risk of loss caused by an imposter's fraud to the party in the best position to prevent the fraud. (See *Beau Townsend Ford*, *supra*, 759 Fed.Appx. at p. 359; *Erie Ins. Co. v. WAWGD, Inc.* (D. Md., Apr. 29, 2024, No. EA-22-1783) 2024 U.S. Dist. LEXIS 77140, p. *14 (*Erie Ins*.); *Ostrich*, *supra*, 2023 U.S. Dist. LEXIS 105828, at p. *10; *Jetcrete North America LP v. Austin Truck & Equipment, Ltd*. (D. Nev. 2020) 484 F.Supp.3d 915, 919 (*Jetcrete*); *Bile v. RREMC, LLC* (E.D. Va., Aug. 24, 2016, No. 3:15cv051) 2016 U.S. Dist. LEXIS 113874, p. *33 (*Bile*); *Arrow Truck Sales*, *supra*, 2015 U.S. Dist. LEXIS 108823, p. *15.)

In reaching this conclusion, the majority of these courts relied on UCC section 3-404(d)'s "imposter rule," which provides that a "person bearing the loss may recover from the person failing to exercise ordinary care to the extent the failure to exercise ordinary care contributed to the loss."[8] (See *Jetcrete*, *supra*, 484 F.Supp.3d at p. 919, citing *Beau Townsend Ford*, *supra*, 759 Fed.Appx. at p. 357; *Bile*, *supra*, 2016 U.S. Dist. LEXIS 113874, at pp. *25–26; *Arrow Truck Sales*, *supra*, 2015 U.S. Dist. LEXIS 108823, at p. *15; see also *Erie Ins*., *supra*, 2024 U.S. Dist. LEXIS 77140 at p. *14 [finding it persuasive that *Beau Townsend Ford* and *Bile* "looked to" UCC § 3-404(d) when "examin[ing] the enforceability of settlement agreements and other contracts after a third-party fraudulently diverted payment"].) Although the imposter rule "by its terms governs only negotiable instruments, not contract disputes or wire transfers" (*Bile*, at p. *25), "courts have cited to [it] when wired funds have been fraudulently diverted by a hacker." (*Jetcrete*, at p. 919; see *Bile*, at p. *25 [UCC "Article 3 is persuasive in areas of law which it does not directly govern"]; *Arrow Truck Sales*, at p. *15 ["cases in the banking context dealing with third party 'imposters' and forged checks . . . are helpful to

---

8 California has adopted the UCC and its imposter rule. (Cal. U. Com. Code, § 3404, subd. (d) ["the person bearing the loss may recover from the person failing to exercise ordinary care to the extent the failure to exercise ordinary care contributed to the loss"]; see *Unlimited Adjusting Group, Inc. v. Wells Fargo Bank, N.A*. (2009) 174 Cal.App.4th 883, 890 [Cal. U. Com. Code, § 3404 "allocates to the drawer losses in certain circumstances in which it is presumed the drawer failed to exercise due care to avoid the loss"].) "[B]ecause California's Uniform Commercial Code was adopted verbatim from the national Uniform Commercial Code, we may look to . . . how other courts have interpreted the Uniform Commercial Code . . . for guidance." (*Kirzhner v. Mercedes-Benz USA, LLC* (2020) 9 Cal.5th 966, 978.)

resolve this issue" in cases involving wire fraud]; *Erie Ins*., at p. *14; *Beau Townsend Ford*, at p. 357.)[9]

In determining which party was best positioned to prevent the fraud, courts have considered a variety of "red flags," including: the extent to which each party secured its computer system or whether the system had been breached before; whether a party was aware that its transaction was being targeted, and, if so, whether that party disclosed the targeting to the other party in the transaction, or to the court; whether either party failed to scrutinize spoofed email addresses or overlooked typographical errors or duplicative information; and whether the payor called to confirm wire instructions, particularly when they conflicted with prior payment arrangements or new payment instructions changed material information like names and addresses. (See *Erie Ins*., *supra*, 2024 U.S. Dist. LEXIS 77140, at p. *16 [reviewing cases]; *Ostrich*, *supra*, 2023 U.S. Dist. LEXIS 105828, at p. *13.)

We are persuaded by the federal decisions cited above that we should also anchor our analysis to the imposter rule when considering who should bear the risk of loss from a fraudulently induced wire transfer. Accordingly, we hold that the risk of loss from an imposter's fraudulent diversion of a wire transfer shall be borne by the party in the best position to prevent the fraud. In making this factual determination, trial courts must consider the extent to which each party exercised ordinary care with respect to preventing the fraud and may apportion the loss accordingly. (See *Beau Townsend Ford*, *supra*, 759

---

9 Courts have posited that applying other legal theories would lead to the same result as applying the UCC's imposter rule. For example, the *Ostrich* court reached the same conclusion by applying mistake principles under California law (Civ. Code, § 1577) and the Restatement (Second) of Contracts § 154(c), which provides that "courts may allocate the risk of loss to the party 'best able to avoid it' when 'it is reasonable in the circumstances to do so.' " (*Ostrich*, *supra*, 2023 U.S. Dist. LEXIS 105828, at p. *10, quoting Restatement (Second) of Contracts § 154(c).) In applying this standard, the *Ostrich* court followed *Beau Townsend Ford*, *Arrow Truck Sales*, and *Bile*. (*Ostrich*, at pp. *10–*12.)

Similarly, the *Beau Townsend Ford* court theorized that the same conclusion could also be reached under the principle of " 'agency by estoppel,' " which shifts the risk of loss to a party who " 'carelessly caused [the] belief' that 'an actor has authority as an agent.' " (*Beau Townsend Ford*, *supra*, 759 Fed.Appx. at p. 357, quoting Restatement (Third) of Agency, § 2.05.) Thus, for example, "if [a seller] had failed to exercise ordinary care in maintaining its email server, thus allowing [a] hacker to pose as [the seller's employee], then [the seller] could be liable for [the buyer]'s reasonable reliance on the hacker's emails [containing fraudulent wire instructions]. In addition, any potential liability would be reduced if [the buyer] also failed to exercise reasonable care." (*Id*. at p. 358.)

Fed.Appx. at p. 359.) In doing so, courts must consider the totality of the circumstances, which may include the nonexhaustive list of factors described above.

We note that although a party's negligence may contribute to a finding that that party was in the best position to prevent the fraud, a finding of negligence is neither necessary to, nor dispositive of, the ultimate question of which party was best positioned to prevent the fraud. Indeed, courts — including the trial court here — have found one party was best positioned to prevent the fraud even when neither party acted negligently. (See, e.g., *Arrow Truck Sales*, *supra*, 2015 U.S. Dist. LEXIS 108823, at p. *10 ["The Court makes a finding of fact that neither [party] was negligent in the manner that they maintained their e-mail accounts."]; *Ostrich*, *supra*, 2023 U.S. Dist. LEXIS 105828, at p. *14 ["To be sure, the Court is not concluding that [the payor's counsel] was negligent. The question is, based on the facts before this Court, who was in the *better* position to prevent the fraud in an unfortunate case such as this."].) We turn now to that question.

Substantial Evidence Supports the Trial Court's Allocation of the Risk of Loss

Viewing the evidence in the light most favorable to the judgment (*Steinman*, *supra*, 185 Cal.App.4th at p. 1556), we conclude substantial evidence supports the trial court's factual findings that "defendants were in the best position to prevent the fraud."

Contrary to Defendants' assertion, there were red flags that should have alerted their counsel to the fraudulent scheme. First, as the trial court observed, the imposter's "wiring instructions conflicted with the payment procedure established by the parties' written Settlement Agreement and Release." While the Settlement Agreement specified that the settlement payment "is to be issued to: 'Chambers and Noronha Client Trust Account for the benefit ("FBO") Brian Thomas,' " the wire instructions changed the payee to "Chambers & Noronha APC." This change was material in at least two ways: it omitted the "client trust account" aspect of the payee and omitted Plaintiff's correct name. Both changes reduced safeguards that benefited and protected both Plaintiff and his attorneys.

The wire instructions raised additional warnings that, while not in direct conflict with the Settlement Agreement, should still have given Defendants' counsel reason to question the validity of the transfer instructions. For example, the imposter's request to wire the settlement proceeds conflicted with counsels' informal agreement that the settlement payment would be made by check.

Together, these anomalies surrounding the wire instructions support the trial court's finding that Defendants were better positioned to prevent the fraud. (See *Arrow Truck Sales*, *supra*, 2015 U.S. Dist. LEXIS 108823, at p. *11 [finding the payor "had more opportunity and was in the better position to discover the fraudulent behavior" where "the fraudulent wiring instructions involved a different beneficiary, different bank, different location, and different account information from all of the previous wiring instructions"]; *Erie Ins.*, *supra*, 2024 U.S. Dist. LEXIS 77140, at p. *15 [citing as a red flag the fact that "the communications regarding payment conflicted with the original instructions provided by [the payee's] counsel, altering the name and address of the

recipient, and attempting to alter the method of payment from a check to a wire transfer"]; cf. *Bile*, *supra*, 2016 U.S. Dist. LEXIS 113874, at pp. *16–*17 [shifting the risk of loss to the payee where, among other things, "the recipient name on the wire transfer order was" the plaintiff's name and "per banking industry standard practices, the receiving bank confirmed that the recipient name on the wire transfer order corresponded to the name of the holder of the recipient account"].)

Second, substantial evidence supports the trial court's finding that if a law firm's primary phone number was "inoperable," that was another warning sign to Defendants' counsel.[10] Several of the courts that shifted the risk of loss to the payor did so because the payor failed to call the payee to confirm wire instructions unknowingly received from an imposter. (See *Jetcrete*, *supra*, 484 F.Supp.3d at p. 920; *Ostrich*, *supra*, 2023 U.S. Dist. LEXIS 105828, at p. *14; *Arrow Truck Sales*, *supra*, 2015 U.S. Dist. LEXIS 108823, at p. *11; see also *Erie Ins.*, *supra*, 2024 U.S. Dist. LEXIS 77140, at p. *16 ["no earnest effort was made to verify the payment instructions before issuing the settlement draft"].) Although Defendants' counsel took that preliminary step here, the fact the phone number was inoperable should have signaled counsel to exercise greater vigilance. That would have revealed that the phone number Defendants' counsel got from the imposter's first spoofed email message signature block differed from the number that appeared in the email signature of Plaintiff's counsel's authentic email messages and the caption on the firm's pleadings filed in this case. Indeed, Plaintiff's counsel's phone number has been the same since 1989. Yet, rather than determine the correct phone number via a source extrinsic to the spoofed email thread (e.g., look at the state bar's website), Defendants' counsel relied on further information provided by the imposter's suspicious communications — yet another phone number that differed from the one in counsel's authentic email signature and on their court filings. Further, despite these anomalies, Defendants' counsel delegated the chore of confirming the accuracy of the wire instructions. Instead of following up himself, he delegated the follow-up call regarding the wire instructions to his firm's accounting personnel.

Third, the imposter's use of a spoofed email address for Mattson, which differed in both her name (it omitted the letter "c") and the domain name (it added the letter "r"), was yet another red flag to Defendants' counsel. Several courts have shifted the risk of loss to the party that failed to scrutinize spoofed email addresses. (See *Erie Ins.*, *supra*, 2024 U.S. Dist. LEXIS 77140, at p. *15 ["A review of the emails . . . reveals that the imposter's email address was not the same as that of [payee]'s counsel."]; *Ostrich*, *supra*, 2023 U.S. Dist. LEXIS 105828, at p. *14 ["had counsel carefully evaluated the email address of the [spoofed] emails . . . , this would have . . . revealed the fraud because the email addresses did not match"].)

Fourth, the fact the imposter carelessly sent two identical requests for wire instructions within a matter of minutes is akin to typographical errors that courts have

---

10 We observe that the court's minute order misstates this phone number as belonging to "the purported 'head of finance' " Mark Anderson.

deemed significant in shifting the risk of loss. (See *Erie Ins.*, *supra*, 2024 U.S. Dist. LEXIS 77140, at p. *15 [red flags included that the imposter's emails "contained typographical errors and did not reflect a sophisticated understanding of how settlement payments are executed"]; *Ostrich*, *supra*, 2023 U.S. Dist. LEXIS 105828, at p. *4 ["some grammatical and punctuation errors, and a duplicated signature block" were suspicious].)

These numerous red flags, backed by substantial evidence in the record, support the trial court's factual finding that Defendants were in the best position to prevent the fraud.

Defendants argue the trial court erred by failing to also consider Plaintiff's counsel's contribution to the fraudulent scheme's success. We disagree. In finding no "comparative fault on the part of plaintiff," the trial court stated it had "[l]ook[ed] at the totality of the circumstances of this case." We presume the court did so. (See *Laabs v. City of Victorville* (2008) 163 Cal.App.4th 1242, 1271–1272 ["courts have developed the doctrine of implied findings by which the appellate court is required to infer that the trial court made all factual findings necessary to support the order or judgment"].) And although the trial court did not identify the specific evidence that supports the court's finding, we conclude substantial evidence supports it.

Defendants' primary theory for shifting the blame to Plaintiff's counsel relies largely on a series of logical leaps: (1) "[t]he fraudster could not have succeeded but for breaching one of the party's computer systems undetected"; (2) Defendants' counsel explained why his firm could not have been responsible for the breach; therefore, (3) Plaintiff's counsel must have been responsible for the breach. This syllogism fails.

First, the fact the fraudulent scheme was perpetrated using only spoofed email addresses suggests it *could have* been accomplished without compromising either side's computer system. Theoretically, to perpetrate the fraud the imposter needed to know only the fact of the settlement and the identities of the players involved. This information could have been obtained in many ways other than breaching either party's computer system — for example, by overhearing a conversation in a public place or by reading documents carelessly left about. The record simply does not support Defendants' assertion that the fraud *must* have been perpetrated by means of breaching either side's computer system. We agree with the trial court's finding that "it is unknown how the fraudster learned of the settlement."

Second, regarding the parties' cybersecurity efforts, the record is not as conclusive as Defendants assert. The only evidence about Defendants' efforts came from their attorney's brief description of his IT personnel's investigation. Defendants presented no evidence from the IT personnel themselves. (Cf. *Ostrich*, *supra*, 2023 U.S. Dist. LEXIS 105828, at pp. *6–*7 [the payee's "Director of IT Security" explained how the system was compromised]; *Bile*, *supra*, 2016 U.S. Dist. LEXIS 113874, at pp. *5–*6, *15 ["At the evidentiary hearing, Defendants presented the testimony of [a witness], accepted by the Court as an expert in information technology," whose "expert opinions [the court found] to be reliable and credible"]; *Beau Townsend Ford*, *supra*, 759 Fed.Appx. at p. 352 [discussing evidence from the seller's "IT manager"].)

Plaintiff's counsel also submitted a declaration explaining that his firm conducted an IT investigation and found no breach. Defendants argue on appeal that this declaration lacks evidentiary value because Plaintiff's counsel asserted the conclusion "on information and belief." But because it appears from the record that Defendants did not raise this objection in the trial court, they have forfeited it on appeal. (*In re Marriage of Kerry* (1984) 158 Cal.App.3d 456, 466 ["Even if the affidavit in support of a motion to vacate contains hearsay, legal conclusions or other objectionable contents, failure to object on these grounds in the trial court waives the defects, and the affidavit becomes competent evidence."]; see *City of Santa Cruz v. Municipal Court* (1989) 49 Cal.3d 74, 87 ["courts have long held that affidavits on information and belief may be sufficient in a variety of contexts where the facts would otherwise be difficult or impossible to establish"].)

For these reasons, the record does not support Defendants' proffered inference that Plaintiff's counsel's computer system must have been compromised.

Even if the record did support this inference, it would not require the trial court to apportion any of the loss to Plaintiff. Several courts have shifted the entire risk of loss to a payor who ignored red flags even after a payee's email system was compromised. (See *Erie Ins.*, *supra*, 2024 U.S. Dist. LEXIS 77140, at pp. *14–*15 [The payor's "argument that [the payee] failed to exercise reasonable care because its email system was compromised . . . completely glosses over the many communications and actions that led to remittance of the settlement funds to the imposter. Based on those intervening acts, it is evident that not only was [the payor] in the best position to prevent the fraud, but that it also failed to exercise reasonable care."]; *Jetcrete*, *supra*, 484 F.Supp.3d at p. 920 ["The hack of [the payee]'s email account created the scenario for the loss. But [the payor] was in the best position to prevent the loss by taking the reasonable precaution of verifying the wiring instructions by phone."]; *Ostrich*, *supra*, 2023 U.S. Dist. LEXIS 105828, at p. *14 [declining to shift the risk of loss to the payee where its counsel's email system was compromised, thereby preventing its "employees [from] . . . discover[ing] the fraud because all the incoming and outgoing emails were diverted and deleted," even where counsel's computer system had been breached a year earlier in an unrelated incident].)[11] As detailed above, numerous warning signs put Defendants' counsel on notice such that the trial court could reasonably find that those intervening events absolved Plaintiff's counsel of any fault.

---

11 The only case (among those discussed here) in which a court shifted the risk of loss to a payee because its computer system had been compromised is *Bile*, *supra*, 2016 U.S. Dist. LEXIS 113874, which did so only because the payee's counsel was aware before the compromise that "a malicious third party was targeting [the plaintiff's] settlement for a fraudulent transfer to an offshore account," yet counsel failed to disclose the attempted hack to the opposing parties, their counsel, or the court. (*Id*. at p. *11.) There is no evidence of any similar conduct by Plaintiff's counsel here.

Defendants argue Plaintiff's counsel's conduct *after* the fraud was perpetrated contributed to the success of the fraud. Specifically, Defendants fault Plaintiff's counsel for "allow[ing] the fraudster to string him along for nearly two months with" proverbial " 'the check is in the mail' " emails from a spoofed email account before "finally pick[ing] up the phone to question the status." This evidence was before the trial court, which could have reasonably discounted the evidence because the imposter first contacted Plaintiff's counsel only *after* Defendants' counsel wired $475,000 to the wrong bank account. Moreover, Defendants presented *no evidence* to the trial court showing that Plaintiff's counsel's conduct contributed to the fraud's success.

In short, substantial evidence supports the trial court's reasoned findings that, "[l]ooking at the totality of the circumstances of this case," Defendants were "in the better position to prevent the fraud" and that there is no "comparative fault on the part of plaintiff." The trial court's analysis shows, contrary to Defendants' contention, that the court did not simply "presum[e] the payor is in the best position to prevent the fraud."

The Judgment Did Not Alter the Parties' Settlement

As noted, Defendants argue in passing that the judgment is improper under section 664.6 because it "materially alters the obligations bargained for by the parties" in two respects: by "permitting plaintiff to seek prejudgment interest" even though it is not authorized by the Settlement Agreement, and by making Defendants "pay $950,000 to resolve this claim." Neither argument is persuasive.

First, the trial court did not award prejudgment interest. Rather, the court merely responded to Plaintiff's request for prejudgment interest — raised in an opposition brief — by directing that any request must be made by noticed motion.

Second, Defendants' double-payment theory rests on their flawed view that they should not bear the risk of loss for the erroneous wire of $475,000 to a fraudulent bank account. Substantial evidence supports the trial court's conclusion to the contrary.

Conclusion

Innovation in commerce makes financial transactions more efficient and convenient. At the push of a button, money moves around the world almost instantly. Criminals have likewise invented new ways to exploit these advancements — making the ability to remotely and rapidly transfer significant amounts of money now come with a risk that a criminal will exploit the convenience of remoteness by impersonating a party to the transaction and diverting the funds, often irretrievably. As cases show, criminals do this in a variety of ways, including by hacking a party's authentic email account or by using a spoofed email account that closely resembles a party's authentic account. The antidote to these innovative fraudulent schemes may involve sophisticated encryption and digital safeguards (e.g., multifactor authentication), or it may sometimes be as old-fashioned and simple as picking up the phone and calling opposing counsel at a verified phone number, or meeting face-to-face to confirm the identity of one's counterpart and the validity of the transaction details. Either way, this case demonstrates

that parties to modern, high-tech financial transactions must remain vigilant in ensuring they are dealing with their authentic peer. Failing to do so may be at their own financial peril.

DISPOSITION

The judgment is affirmed. Plaintiff is entitled to recover his costs on appeal.

RUBIN, J.

WE CONCUR:

DO, Acting P. J.

CASTILLO, J.