Proskauer

California Court Holds Defendants Liable for Fraudulent Wire Transfer

Proskauer on Privacy on **June 3, 2025**

Wire transfer fraud has long been a popular target for cyber criminals.

A case of first impression decided by the California Court of Appeal, Fourth Appellate District demonstrates the high stakes for victims of this crime. Specifically, on May 27, 2025, the Court of Appeal released an opinion addressing the issue of who bears the loss when settlement funds are fraudulently diverted via a wire transfer scam.

The case originated when Plaintiff Brian Thomas sued Defendants Corbyn Restaurant Development Corp. and two of its employees for personal injuries allegedly sustained during an altercation. Following mediation, Defendants agreed to pay a total of $475,000 to Plaintiff in full settlement and release of all Plaintiff's claims. The agreement stipulated payment to Plaintiff's attorney's client trust account by check.

One week after the agreement was reached, however, an imposter posing as Plaintiff's counsel requested by email that payment be sent via wire transfer, and it provided wire instructions to Defendants' counsel. After Defendants' counsel communicated telephonically with the imposter's associate–who posed as the purported "Head of Finance" at Plaintiff's firm–it proceeded to electronically transfer the funds in accordance with the provided instructions.

The fraud remained undiscovered until Plaintiff's counsel contacted Defendants' counsel to follow-up regarding payment, after which Plaintiff filed *ex parte* for an order enforcing the settlement agreement.

The trial court applied federal case law, which generally shifts the risk of loss to the party in the best position to prevent the fraud. In so doing, it found that the Defendants were in the best position to prevent the fraud, and that Plaintiff bore no comparative fault. It entered judgment in favor of Plaintiff for the full $475,000. Defendants appealed that judgment.

The Court of Appeal affirmed the trial court's judgment, observing that there was a lack of California authority on the topic of which party bears the risk when an imposter causes one party to a settlement to wire proceeds to a fraudulent operator.

The Court of Appeal concluded that the trial court properly applied persuasive federal case law borrowing a concept from the Uniform Commercial Code: the so-called "Imposter Rule." This rule provides that 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."

In determining which party was best positioned to prevent the fraud, the Court of Appeal looked to precedent. It noted that courts have typically 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 the targeted 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.

Applying these considerations, the Court of Appeal found that "there were red flags that should have alerted [Defendants'] counsel to the fraudulent scheme," including the fact that "the imposter's 'wiring instructions conflicted with the payment procedure established by the parties' written Settlement Agreement and Release.'" Accordingly, Defendants were still on the hook to pay Plaintiff $475,000.

As transaction volumes grow and fraud attempts become more and more sophisticated (including the emerging use of generative artificial intelligence, such as voice cloning, to bypass controls designed to prevent this type of crime), it has become even more critical for organizations to establish layers of controls to verify transfers. And it is equally important to appropriately train, test, and evolve those controls to minimize the risk that they will not hold up under an actual threat.

View original.

Related Professionals

- **Nolan M. Goldberg**
  Partner
- **Michelle M. Ovanesian**
  Associate