Andrews Myers

Protect Your Business: Texas Court Rules on Liability for Fraudulently Misdirected Business Payments

In a case of first impression, the Houston (1st Dist.) Court of Appeals issued an important decision in *Prosper Florida, Inc. v. Spicy World of USA, Inc.* that addresses how courts should allocate losses when business payments are fraudulently misdirected to unauthorized parties. This decision provides two critical takeaways for businesses engaged in commercial transactions. First, when fraud causes payment to go astray, courts will look at which party is most at fault—not simply who initiated or received the payment. Second, businesses should implement verification procedures for wire transfer instructions, especially when banking details change mid-transaction.

Prosper Florida, Inc. v. Spicy World of USA, Inc.

Prosper Florida, Inc. ("Prosper Florida") and Spicy World of USA, Inc. ("Spicy World") entered into a contract for the sale and purchase of black pepper. Prosper Florida sold Spicy World a bulk shipment of black pepper, which Spicy World accepted. However, when Spicy World attempted to pay for the shipment via wire transfer, the payment was fraudulently misdirected to an unauthorized party. Prosper Florida sued Spicy World alleging failure to pay for the shipment. The fraud unfolded as follows: Prosper Florida's manager sent an email to Spicy World's manager requesting payment by wire transfer to an offshore account, citing a problem with Prosper Florida's usual bank account. However, within a month, Spicy World's manager received three different sets of wire instructions for three different bank accounts. Each email was purportedly from Prosper Florida's manager. The final set of instructions directed Spicy World to transfer funds to Barclays Bank, which Spicy World did, yet Prosper Florida did not have an account with Barclays Bank.

At trial, Prosper Florida's computer systems administrator testified as an expert and concluded that an unknown party had fraudulently accessed Prosper Florida's manager's email account by obtaining login credentials and then used it to send fraudulent emails to Spicy World.

Spicy World's manager testified that he called Prosper Florida's manager regarding the wire transfer but conceded that he did not confirm the specific bank or account information during the phone call. Spicy World's manager also testified that he did not notice the emails contained instructions for different banks because the bank information all looked the same from a casual inspection. He only learned that Prosper Florida did not receive payment after Prosper Florida's manager contacted him about the payment. The trial court entered a final judgment ordering that Prosper Florida take

nothing by way of its claims and pay Spicy World's costs and attorney's fees. On appeal, Prosper Florida argued that Spicy World must pay for the shipment, while Spicy World asserted that since Prosper Florida provided the wire instructions, Prosper Florida must bear the loss.

The Appellate Court turned to federal district court decisions addressing similar facts, which held that liability for misdirected payments should turn on the respective fault of the parties. Persuaded by this reasoning, the Appellate Court adopted a "fault-based" rule, holding that "any loss resulting from fraudulently misdirected payments should be placed on whichever party to the contract the factfinder finds to be most at fault for the misdirection." The Appellate Court acknowledged that this rule comports with Texas common law: when one of two parties must suffer due to a third party's misconduct, the loss should fall on the person who had knowledge and means to protect themselves but failed to do so.

Ultimately, the Court upheld the trial court's decision because the evidence established that Prosper Florida was most at fault for the loss.

Key Takeaways for Businesses

The *Prosper Florida* decision offers critical guidance for any business that sends or receives wire transfers. Both buyers and sellers should implement verification protocols when banking information changes. Nevertheless, Prosper Florida's compromised email system enabled the fraud in the first place. Businesses should ensure they have strong cybersecurity measures to protect email accounts, establish multi-factor verification procedures for wire transfer instructions (especially when banking details change), and document all verification efforts in writing.

For further information on these developments, please contact Lucas Diaz.