Wire Fraud in Commercial Payments: How Texas Law Now Allocates Loss-and What Your Company Should Do Next

I. SUMMARY

Business email compromise and payment-redirection scams continue to hit Texas businesses, with losses often surfacing only after funds are irretrievable. Under the Houston First Court of Appeals' decision in *Prosper Florida, Inc. v. Spicy World of USA, Inc.*, losses from fraudulently misdirected payments are allocated to the contracting party the factfinder concludes is "most at fault" for the misdirection, a common-law, fault-based rule that supplements the UCC where the Code is silent. This rule has immediate, practical consequences for Texas companies that exchange invoices and payment instructions by email.

II. THE CURRENT TEXAS RULE: A FAULT-BASED ALLOCATION OF LOSS

The *Prosper Florida* court held 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," adopting a fault-based rule grounded in longstanding Texas common law that places the loss on the party who enabled the fraud to happen. The court explained that Article 2 of the UCC does not answer who bears a loss when a wire is diverted by a fraudster, so common-law principles supplement the UCC unless displaced, which they are not here.

Prosper Florida therefore affirms that where both the seller and buyer are innocent of the fraud itself, the trier of fact weighs the parties' conduct to determine who bears responsibility for the loss. The case further confirms that the UCC's general duty of good faith cannot be used to rewrite contracts or displace the common-law fault analysis absent a specific contractual duty tied to the conduct at issue.

III. PROSPER FLORIDA IN PRACTICE: WHAT FACTS MOVED THE COURT

- The buyer's manager received multiple differing wire instructions that appeared consistent on casual inspection and testified that he telephoned the seller's manager to confirm that a United Kingdom bank should be used, though he did not confirm the specific account numbers. The trial court credited this testimony in finding the seller more responsible for the loss, and the court of appeals affirmed.
- The court emphasized there was no conflict between the UCC and the common-law fault rule because the Code is silent on misdirected wire payments, allowing resort to common law under Section 1.103(b).

- The court rejected a standalone "good faith" theory as a basis to shift loss where no specific UCC or contractual duty required different payment-record practices; good faith must be tied to a specific duty.
- Although the buyer prevailed on the contract claim, it could not recover attorney's fees under Section 38.001(8) in that posture.

Bottom line: Factfinders will closely examine what each party reasonably could and should have done to prevent the fraud and will allocate the loss accordingly.

IV. HOW FACTFINDERS APPLY THE PROSPER FLORIDA RULE IN PRACTICE

In disputes over misdirected wire payments, courts and arbitrators applying *Prosper Florida* focus on whether each party acted reasonably in preventing, detecting, and responding to payment-redirection fraud. The analysis is highly fact-specific and typically turns on the parties' communications about payment instructions, the presence and rigor of out-of-band verification, the security posture of their email and accounting systems, and the credibility of witnesses describing what was done and when.

Factfinders frequently examine contemporaneous emails and payment records, call logs memorializing verification steps, incident-response timelines (including prompt notices to counterparties and banks), and any available forensic evidence regarding account compromise. They also weigh whether contract terms required particular verification procedures or security controls and whether either side ignored red flags such as last-minute bank-change requests, offshore accounts, or unusual urgency. The practical takeaway is that the party who can show disciplined verification and reasonable controls is far more likely to avoid bearing the loss, while the party whose systems or practices enabled the misdirection is more likely to be assigned responsibility.

V. PRACTICAL CONSEQUENCES FOR TEXAS BUSINESSES

- Contracts for goods and services do not, by default, assign losses from misdirected wire transfers; courts will apply a common-law fault test to decide who pays. Parties should not assume the payer must always pay twice or that the payee must always absorb the loss.
- The party whose systems, processes, or communications "enabled" the fraud risks being saddled with the loss. Evidence of compromised email systems, prior warnings, missing administrative controls, or inattentive verification can decisively shift fault.
- A single verification step-such as an out-of-band telephone confirmation to a known number-can materially affect the factfinder's allocation of fault, even if account numbers were not recited digit-by-digit.
- Generalized "good faith" arguments will not displace the fault analysis absent a specific contractual duty tied to payment-instruction handling.
- Attorney's fee recovery may be limited even for prevailing parties, depending on posture and statute.

VI. RISK-MITIGATION PLAYBOOK: CONTRACT TERMS AND OPERATIONAL CONTROLS

Given *Prosper Florida's* focus on comparative fault, companies can materially improve their position before any dispute by integrating targeted contractual provisions and disciplined payment operations.

A. Contract drafting and allocation

- Include a payment-instruction verification clause requiring out-of-band confirmation to a pre-designated, verified phone number for any new or changed bank instructions; specify that failure to follow the protocol allocates resulting loss to the non-complying party. Tie the obligation to the manner in which instructions are transmitted, not just payment timing.
- Require parties to maintain reasonable administrative, technical, and physical safeguards for email and finance systems, including MFA, least-privilege, and logging, and to promptly notify of suspected compromise; expressly state that a party's failure to maintain safeguards will be considered in allocating responsibility for any misdirected payment.
- Establish a standing, signed "funds flow" schedule and designate a secure portal or encrypted channel for transmitting any account changes; prohibit bank-change instructions by free-form email.
- Add lien and credit/offset language clarifying that payments made in accordance with agreed verification protocols satisfy payment obligations, even if funds are later discovered to have been misdirected by fraud, and require removal of liens in that circumstance.

B. Operational controls

- Implement a strict "no change by email" rule. Treat any bank-change request as presumptively fraudulent pending verification via a known, pre-verified phone number or in-person confirmation documented in writing.
- Harden email systems: enforce MFA for users and administrators, restrict and monitor admin access, deploy DMARC/DKIM/SPF with reject policies, and retain and review message-trace and audit logs; attackers with admin rights can pass SPF and alter messages, as the forensic evidence in the briefs demonstrates.
- Train accounting and project teams to spot red flags (bank changes, urgency, offshore accounts), and require dual-control approvals for any payment to new or revised accounts.
- Document your verification steps contemporaneously. In a later dispute, those records can be the difference in the fault analysis.
- Prepare an incident-response playbook for payment fraud: immediate notices to counterparties and banks, FBI IC3 filing, preservation of headers and logs, and rapid forensic triage-all of which featured in the briefs' evidentiary record.

C. Insurance and Risk Transfer

As a backstop to your controls, review cyber insurance and commercial crime policies for payment-redirection and social-engineering fraud. Prioritize: (1) social-engineering/"voluntary parting" coverage; (2) wire-transfer fraud limits and exclusions;

(3) any requirements for dual-control or call-back verification; (4) coverage for vendor-caused loss and how it coordinates with indemnities and liability caps; (5) first-party incident-response benefits (forensics, counsel, notices) and any business-interruption coverage; and (6) strict notice, police-report, and bank-recovery cooperation conditions. Make sure policy terms align with your verification protocol and allocation language to avoid gaps.

VII. HOW PROSPER FLORIDA INTERSECTS WITH YOUR PROJECTS AND DEALS

For Texas real estate, construction, and commercial supply chains, *Prosper Florida* reshapes leverage in payment disputes triggered by BEC schemes. Owners and contractors exchanging pay apps and ACH instructions by email are particularly exposed. Conversely, a payer that can show a consistent verification protocol and timely incident response can avoid paying twice, even if the payee ultimately goes unpaid, because the UCC does not require a different result and the common-law rule controls.

VIII. CLOSING TAKEAWAYS

- *Prosper Florida* cements a fact-intensive, fault-based rule for misdirected wire payments under Texas law, supplementing the UCC where silent. Your best defense is a written protocol rigorously followed.
- Update your contracts and payment operations now. Allocation provisions, verification requirements, and security controls can materially influence outcomes-and may be outcome-determinative in arbitration or court.

If you would like, we can adapt these recommendations to your existing form contracts and payment SOPs for Texas projects and cross-border supply arrangements, aligning verification steps with your bank's capabilities and your counterparty mix.

For further information on these developments, please contact Breton Rycroft.