FAULTY WIRING: FRAUD'S GROWING THREAT TO CONSTRUCTION

BY MARC J. FELEZZOLA, ESQ. AND RYAN MCCANN, ESQ., BABST CALLAND

I. Blueprints for Disaster: Foundational Failures of a Different Kind

In construction, the biggest threat isn't a faulty foundation, it's a compromised inbox. Courts nationwide have seen a surge in cases involving fraudulent wire-transfer instructions due to bad actors inserting themselves into legitimate transactions and siphoning funds before anyone notices. Because progress payments routinely travel by wire and project timelines depend on fast, clean transfers, the construction industry is becoming an increasingly attractive target. Understanding how these schemes work, how to guard against them, and what remedies remain once the money disappears is now essential for every member of the industry.

II. How Wire-Fraud Schemes Operate

In 2024 and 2025, wire transfers were the payment method most frequently targeted by business email compromise scams. These schemes often unfold quietly: a hacker slips into a company's email system, studies the back-and-forth between parties negotiating a payment, and waits until transfer of funds is imminent. Then the hacker intervenes—diverting legitimate emails, impersonating one party by using a near-identical address, and sending counterfeit wire instructions in the hope that the recipient won't spot the subtle switch. Most businesses usually do not become aware of the fraud until it is too late. Additionally, scammers have found success through sending deceptive emails that appear to come from a trusted source to trick recipients into providing sensitive information. Similarly, hackers have also begun sending fake invoices that closely resemble legitimate ones from real suppliers leading companies to wire money directly into the scammer's account.

III. Why the Construction Industry is Uniquely Vulnerable

Despite the availability of safeguards, many construction companies operate without them, making the industry uniquely susceptible to the very risks these practices are designed to prevent. Few industries move money with the frequency, speed, and decentralization of construction. On any given project, payments may flow from owners to prime contractors, primes to subcontractors, subcontractors to suppliers, and all parties to equipment rental companies or specialty vendors. To further add to the problem, construction is perpetual, with new projects starting every day, and owners and contractors are continuously answering emails and making decisions while on the move. This creates an environment with several points of entry for fraud. In short, construction companies face a perfect storm: lots of money moving quickly, through lots of hands, via communication channels designed for convenience—not security.

IV. Prevention: Practical Safeguards for Construction Companies

Preventing these schemes takes more than luck—it requires clear processes and vigilance. Employees, especially those handling payments, should be trained to spot suspicious emails, and wire instructions should be verified by phone or require dual approvals. A review of recent decisions contains numerous cases where saving millions of dollars in fraud losses was just one phone call away. Strong email security, including multi-factor authentication and regular monitoring, is critical, as are written policies, segregation of duties, and escalation protocols to prevent any one employee from having unchecked control over wire transfers. But even if all these actions are undertaken, wire fraud may still occur. That's why it is crucial to understand the potential remedies in the unfortunate event that a construction company falls subject to these schemes.

V. Remedies: Laying the Foundation for Recovery

Remedies for wire fraud depend on whether the claim is asserted against the banks that sent or received the wire, or against a separate entity whose compromised systems set the fraud in motion.

Remedies against the banks are typically covered by the Uniform Commercial Code (UCC). Prior to the enactment of the UCC, every state had its own laws governing commercial transactions. This created significant confusion and complexity for businesses operating across state lines. Thus, the UCC was enacted to harmonize commercial laws nationwide and establish a uniform legal framework across the United States. Coincidentally, Pennsylvania was the first state to adopt the UCC in 1953. There are nine separate articles in the UCC ranging from the sale of goods, bulk sales and auctions, warehouse and shipping transactions, secured transactions and most importantly for this issue: funds transfers.

When initiating a cause of action against a bank, parties should look first and foremost to Article 4-A for guidance in bringing and resolving their claims. Article 4-A was added to the UCC in large part due to the drastic increase in wire transfers between financial institutions and other commercial entities in the latter stages of the 20th century. Because it was specifically added to the UCC for the purpose of combatting jurisdictional disputes and a lack of judicial authority, it is intended to be the exclusive means of determining the rights, duties and liabilities of the affected parties. However, this does not mean that it is the only remedy afforded to wire fraud victims. Instead, the analysis is simple: if a provision in Article 4 of the UCC squarely applies to the issue, any other remedies are preempted by the UCC, and Article 4 of the UCC provides the exclusive remedy. However, if the alleged

action is not addressed by the UCC, then a plaintiff may seek remedies at common law.

Because Article 4A's scope is both technical and specific, and its application is largely decided on a case-by-case basis, its boundaries cannot be explored comprehensively in a single article. At a high level, Article 4A governs conduct occurring between the moment a payment order is initiated, and the moment the beneficiary's bank accepts that order. Within this window, the UCC governs disputes involving, among other things: (1) payment orders issued to nonexistent or unidentifiable beneficiaries; (2) situations where a beneficiary's bank executes a transfer based on an account number that does not match the named beneficiary; (3) whether a payment order was authorized by the originator; (4) payment orders fraudulently issued in the name of a legitimate customer; and (5) customer-initiated orders that were intercepted and altered by a fraudster prior to acceptance.

Be diligent, proactive not reactive, and make sure it is correct the first time around.

By contrast, claims that are based on alleged conduct occurring before or after the funds transfer are not governed by the UCC and therefore are not preempted. Instead, those actions would be governed by common law remedies such as negligence, breach of contract, aiding and abetting fraud, and the like. Thus, the UCC does not apply to: (1) failures to properly verify the identity of an individual opening an account under a false name; (2) failures to adopt reasonable safeguards before allowing withdrawals from an account; or (3) post-transfer actions, such as lifting a freeze on a fraudulent account, permitting the withdrawal of already-misappropriated funds, or a failure of a bank to attempt to retrieve funds after the fraudulent wire has been completed. These common-law claims are viable but not without obstacles. Nevertheless, they remain essential avenues when Article 4A does not apply.

Additionally, there is a separate analysis when bringing claims against another entity that was hacked. For instance, suppose a Contractor regularly buys construction materials from a Supplier. The Contractor sends a purchase order to Supplier and the parties engage in negotiations over price via email. During the negotiations, Supplier is hacked and a person purporting to be Supplier sends Contractor fraudulent wire instructions. The parties agree upon the price, and Contractor pays the invoice, but Supplier never receives the payment. Supplier alleges that Contractor breached the contract because Supplier delivered the goods but was never sent payment. In response, Contractor argues that it met its contractual obligations by paying money according to the instructions it received and that it had no independent obligation to ensure that the instructions were accurate. Thus, according to Contractor, it should be able to keep the goods without further payment. Who is correct?

In this scenario, courts have routinely held that the answer depends on which party was best able to avoid the fraud. In the example above, Contractor would argue that Supplier should have employed better security measures to prevent it from becoming hacked. Conversely, Supplier would argue that Contractor should have taken additional measures to ensure the transaction was valid, such as calling Supplier to confirm the transaction and the wire instructions. In short, whoever was in the best position to prevent the fraud will be held liable. This is ultimately a factual question which will be determined by looking at the totality of the circumstances on a case-by-case basis.

VI. Reinforcing the Foundation: Staying Ahead of Wire Fraud

Whether a company can recover after being victim to wire transfer fraud is a difficult and fact intensive inquiry. The ideal solution is one that mirrors good practice in the construction industry: be diligent, proactive not reactive, and make sure it is correct the first time around. However, anyone familiar with the construction practice knows that mistakes happen. With the fast-paced environment surrounding the construction industry, it is only a matter of time before construction companies are subject to more direct and clever attacks. Thus, while it may be impossible to eliminate fraud entirely, remaining vigilant and ensuring you are employing best practices should help ensure that if fraud does occur, you will not be the party who bears the financial consequences of it. BG

Mark J. Felezzola is a shareholder at Babst Calland. He focuses his practice on complex construction-related and environmental matters. Felezzola serves as outside general counsel for owners, developers, design professionals, and construction companies, and frequently represents them in a variety of commercial and construction-related disputes including construction bid protests, construction defect claims, differing site condition claims, delay and inefficiency claims, payment and performance bond claims, mechanics' lien claims, as well as all other types of payment and contract performance disputes. Contact Mark at 412-773-8705 or mfelezzola@babstcalland.com.

Ryan McCann is a litigation associate at the firm. He focuses his practice on complex commercial litigation, environmental litigation, and construction disputes. Contact Ryan at 412-773-8710 or rmcann@babstcalland.com.