Articles + Publications | October 15, 2021

Avoid Wire Fraud Losses

WRITTEN BY

Susan E. Flint | Mary C. Zinsner

Reprinted from the fall 2021 issue of the VBA Journal with permission of The Virginia Bar Association and authors Mary C. Zinsner and Susan Flint.

Most lawyers get a glazed look when recalling law school study of commercial transactions and the Uniform Commercial Code (UCC). The surge in cases involving wire fraud is causing lawyers to dust off their UCC volumes and revisit the elements of common law tort and contract claims. But the best way to avoid wire fraud losses is by taking simple precautions. Businesses of all sizes must educate employees of the red flags in typical wire fraud cases.

Business Email Compromise Cases Rise

Wire fraud cases arising from what the FBI calls “business email compromise” are on the increase. In 2020, the FBI reported that business email compromise and other internet-enabled theft, fraud, and exploitation resulted in adjusted financial losses of $1.8 billion. Even sophisticated parties and publicly traded companies are getting scammed. In this type of scheme, once the money is wired, it is typically not recovered and tracing the funds can become difficult. Who bears liability in these cases, and what claims can be asserted? These questions arise regularly in wire fraud cases, which often involve very large numbers and imposition of loss on unsuspecting parties.

In a typical business email compromise scheme, the fraudster impersonates a senior executive or trusted business partner reaching out to a member of the staff. The fraudster changes an account number or provides new wiring instructions to pay a debt, conduct a real estate closing, or fulfill a purchase order. The recipient of the email does not notice what can be subtle differences in an email address, such as a hyphen or an underscore, and complies with the request, believing the person to be the trusted partner. The money is wired by the originating bank to the fraudster’s account at the beneficiary bank (the bank receiving the transferred funds, which usually has no idea that its customer is a fraudster). The fraudster immediately withdraws the money or transfers the funds before the fraud is detected, and the sender or banks involved in the transaction can do little to claw the funds back.

Lawyers for victims of wire fraud frequently file lawsuits against the financial institutions involved, alleging common law negligence outside of the actual wire transaction itself to avoid the pre-emption challenges. For example, a complaint frequently will allege that the beneficiary bank was negligent in opening the account of the fraudster or failed to take prompt action to stop withdrawals from the fraudster’s account after the beneficiary bank was on notice of the wire fraud. Typically, however, the victim has no relationship with the beneficiary’s bank that can give rise to a common law duty of care. Standing and causation arguments also can be raised as defenses. Both banks

are insulated by the UCC and standard of care scheme therein, and common law claims of negligence and breach of contract ordinarily are pre-empted. Outside of the banking context, liability is often even more difficult to determine and allocate between the parties, and there are no bright-line rules.

Article 4A of the UCC

Article 4A of the UCC defines the duties, liabilities, and rights of parties to a funds transfer. States enacted Article 4A of the Uniform Commercial Code to provide norms and to ensure predictability with respect to fund transfers:

In the drafting of these rules, a critical consideration was that the various parties to funds transfers need to be able to predict risk with certainty, to insure against risk, to adjust operational and security procedures, and to price funds transfer services appropriately. This consideration is particularly important given the very large amounts of money that are involved in funds transfers.[1]

Typically, state common law claims are displaced by the UCC. Unless a party can allege that negligence by the bank occurred outside of the four corners of the wire transfer transaction, there is usually pre-emption. If the negligence occurred before or after the wire transfer process, a common law negligence claim may be appropriate. But these factual circumstances are rare and other common law defenses such as causation and standing can bar the claims.

The 11th U.S. Circuit Court of Appeals is one of the few federal circuit courts to analyze claims of negligence and Article 4A in the context of a business email fraud scheme. In *Peter E. Shapiro, P.A. v. Wells Fargo Bank N.A.*,[2] the case involved familiar parties: two lawyers involved in a closing, a fraudster, and the two banks involved in the wire transaction. A Florida lawyer engaged by family members to handle the sale of a car dealership in upstate New York received payment instructions by email from a lender's lawyer directing that the wire of funds for a loan payoff be sent to a bank account at M&T in New York. Then the Florida lawyer received another set of wire instructions by email purporting to be from the same lender's lawyer, but was actually from a fraudster, directing that the funds be wire $504,611.13 to what was the fraudster's Wells Fargo account. Wells Fargo received the wire transfer and processed it relying on the account number, notwithstanding that there was a name mismatch in the wire between the beneficiary's name and the name on the account that received the wired funds. The Florida lawyer sued Wells Fargo, alleging that it should not have processed the wire because the bank's automated systems knew that the beneficiary identified in the wire was not the owner of the Wells Fargo account identified in the payment order, asserting claims of common law negligence and violation of the Florida statute codifying UCC Article 4A. The Florida statute and Article 4A state that "if the beneficiary's bank does not know that the name and number refer to different persons, it may rely on the [account] number as the proper identification of the beneficiary of the order."[3] The district court dismissed the common law negligence claim on pre-emption grounds and granted summary judgment for Wells Fargo on the Article 4A claim. The federal appeals court affirmed.

Article 4A provides that in cases involving payment orders that identify both an account name and account number, where the bank lacks "actual knowledge" that the account name and number do not match, the beneficiary bank may rely on the number as the proper identification of the beneficiary of the order. The 11th Circuit relied on the comments to § 4A-207, ruling:

A very large percentage of payment orders issued to the beneficiary's bank by another bank are processed by

automated means using machines capable of reading orders on standard formats that identify the beneficiary by an identifying number or the number of a bank account. The processing of the order by the beneficiary's bank and the crediting of the beneficiary's account are done by use of the identifying or bank account number without human reading of the payment order itself. The process is comparable to that used in automated payment of checks. The standard format, however, may also allow the inclusion of the name of the beneficiary and other information which can be useful to the beneficiary's bank and the beneficiary but which plays no part in the process of payment. If the beneficiary's bank has both the account number and name of the beneficiary supplied by the originator of the funds transfer, it is possible for the beneficiary's bank to determine whether the name and number refer to the same person, but if a duty to make that determination is imposed on the beneficiary's bank the benefits of automated payment are lost.[4]

Who Bears the Loss?

In cases between vendors and third parties, typically the party in the best position to avoid the loss bears it.

While the UCC establishes bright-line rules for the banks involved in wire transactions, for other parties to a transaction there is no definitive liability scheme for determining responsibility. Courts examine the specific facts of the case, including issues of comparative fault. For example, in *Bile v. RREMC, LLC*,[5] the district court applied UCC and contract theories and concluded that the wire transfer of settlement proceeds to the fraudster's account constituted payment under the settlement agreement. Plaintiff's lawyer was on notice that his account had been hacked and should have advised defense counsel of a possible attempt to misdirect the funds. The U.S. Court of Appeals for the Sixth Circuit took a similar approach in *Beau Townsend Ford Lincoln, Inc. v. Don Hinds Ford, Inc.*[6] In this case, the seller, Beau Townsend Ford, transacted to sell 20 Explorers for $736,000. The seller's email was hacked, and purchase funds transmitted by the buyer were misdirected. The buyer received the Explorers, but Beau Townsend Ford never received payment. Beau Townsend Ford sued the buyer for nonpayment. The district court granted summary judgment on a breach of contract claim against the buyer but the Sixth Circuit reversed and remanded, holding that the determining factor is "whether either [party's] failure to exercise ordinary care contributed to the hacker's success," which may result in apportioning the loss by comparative fault. The parties subsequently settled the case.

Stay Vigilant and Take Precautions

Law firms, title companies, and virtually every entity in America conducting business by wire and fund transfer must be aware of the risks from business email compromise. The best steps parties can take to avoid losses are precautionary, rather than reactionary. Here are a few tips to prevent email wire transfer scams.

- **Be vigilant.** Verify information, even from trusted sources.
- **Place verification calls to parties,** using phone numbers found in business records rather than those provided in an email that could be fraudulent, and confirm the authenticity of instructions verbally, not by email. In most of these cases, the loss could have been avoided if the party sending the wire had verified the wiring instructions orally with the true trusted partner rather than rely on email.
- **Be extra vigilant if wiring instructions change.** Fraudsters target emails with wiring instructions and then send a modified email with updated directions for wiring money into their personal account. Be wary of wiring instructions coming from a free email service such as Gmail or Yahoo.
- **Educate employees to double check email addresses** providing wire instructions and look for slight variations, such as hyphens or underscores. Fraudsters use alias accounts with slight modifications so that the

emails appear as though they are coming from a trusted partner.

- **Be suspicious of wires going to an account with a geographic location different from the seller or party receiving the funds.** If the seller receiving the funds lives in Freeport, Maine, and a bank account at a branch in Miami, Florida, is provided, ask questions. There can be possible explanations for locations that vary, but this is a red flag that should be explored, not via email.
- **Consult with your financial institution** and make sure you have the processes and procedures in place and security protocols necessary to prevent wire fraud before wires are transmitted.
- **Consider whether there is any applicable insurance coverage.** When renewing your insurance, explore whether your insurance program includes coverage for social engineering fraud. If it does not, ask whether your insurer offers business email compromise coverage for an additional premium. Check the language of the policy closely as insurers sometimes deny coverage for business email compromise losses on grounds that it was not the "direct" result of a use of a computer.
- **Companies and financial institutions of all sizes should know how to reach the local FBI field office,** which can assist in freezing funds and tracking fraudsters. If you are defrauded, your first call is to your bank so that it can attempt to claw back the wire. The second call should be to the FBI.[7]

The new normal requires companies and individuals to be vigilant with respect to wire transfers. The virtual work environment creates even more risks and exposes lawyers and clients to potentially large losses from wire fraud. Be careful out there.

---

[1] § 4A-102, Cmt.

[2] *See Peter E. Shapiro, P.A. v. Wells Fargo Bank N.A.*, No. 18-15014, 2019 U.S. App. LEXIS 35604 (11th Cir. Nov. 27, 2019) (unpublished).

[3] *See* Fla. Stat. § 670.207(2)(a).

[4] 2019 U.S. App. LEXIS 35604 at *11-12.

[5] *Bile v. RREMC, LLC*, No. 3:15cv051, 2016 U.S. Dist. Lexis 113874 (E.D. Va. Aug. 24, 2016).

[6] *Beau Townsend Ford Lincoln, Inc. v. Don Hinds Ford, Inc.*, 759 Fed. Appx. 348 (6th Cir. 2018).

[7] *See* https://www.fbi.gov/contact-us/field-offices.

RELATED INDUSTRIES + PRACTICES

- Consumer Financial Services
- Financial Services