SpencerFane®

Fraudulent Wire Transfers: Who Bears the Loss?

Wire transfer fraud continues to create significant losses for businesses, consumers, and banks. Business email compromise, compromised online banking credentials, fraudulent vendor instructions, and other schemes can result in hundreds of thousands – or even millions – of dollars being transferred before anyone realizes something has gone wrong. When that happens, one question quickly comes up: who bears the loss?

For banks, the answer often begins with Article 4A of the Uniform Commercial Code (UCC). Unlike many electronic transactions involving consumer accounts, wire transfers have traditionally been excluded from the federal Electronic Fund Transfer Act and Regulation E. Article 4A instead provides a comprehensive statutory framework governing the rights and obligations of parties to wire transfers.

Security Procedure is Critical

When a fraudulent wire is sent in the name of a bank customer, UCC § 4A-202 provides an important framework for determining whether the customer or the bank bears the resulting loss. A bank may generally shift the loss to its customer when four critical requirements are satisfied: (1) the bank and customer agreed to a security procedure; (2) the procedure was commercially reasonable; (3) the bank acted in good faith; and (4) the bank actually complied with the agreed security procedure. If those requirements are not satisfied, the bank may be unable to charge the customer's account for the unauthorized wire and may be required to refund the payment, potentially with interest.

This makes the bank's wire transfer agreement more than routine documentation. Article 4A defines a "security procedure" as a procedure established by agreement between the customer and the bank for verifying that a wire was actually authorized

by the customer or detecting errors in its transmission or content. Without an agreed security procedure, the bank may bear the loss from an unauthorized wire. Merely having a security procedure, however, is not enough. It must also be commercially reasonable.

Commercial reasonableness is determined by considering factors such as the customer's expressed wishes; the size, type, and frequency of the customer's typical wire transfers; alternative procedures offered by the bank; and procedures commonly used by similarly situated banks and customers. Importantly, Article 4A does not require the bank to employ the best security procedure available. The question is whether the procedure is reasonable for that particular bank and customer.

Banks must also follow the procedure they establish. A well-drafted agreement provides little protection if employees bypass required authentication steps when processing a wire. Likewise, Article 4A requires the bank to act in good faith – meaning both honesty in fact and observance of reasonable commercial standards of fair dealing.

What if a Hacker Compromised the Customer?

Even where the bank satisfies these requirements, the analysis may not be over. Under UCC § 4A-203, the customer may avoid liability by establishing that the fraudulent order was not caused, directly or indirectly, by someone entrusted with wire responsibilities, someone who obtained access to the customer's transmitting facilities, or someone who obtained security information from a source controlled by the customer. That can make the source of the compromise enormously important. If a fraudster gained access through the customer's own systems or transmitting facilities, the customer may ultimately bear the loss even though the customer did not intentionally authorize the transfer.

Don't Overlook Beneficiary Name and Account Number Discrepancies

Another increasingly important issue involves fraudulent wire instructions that identify the intended beneficiary by name but provide an account number belonging to the fraudster. UCC § 4A-207 generally permits a beneficiary's bank to

rely on an account number in processing a wire under specified circumstances. Banks should therefore ensure that their account and wire agreements clearly explain that payment may be made based on the account number supplied by the originator even when the beneficiary name identifies someone else. Banks should not assume, however, that § 4A-207 eliminates every possible source of liability. Some courts have permitted a negligence theory against a beneficiary bank when the allegations identified significant problems surrounding the opening and maintenance of the fraudster's account and the bank's knowledge of discrepancies involving the beneficiary information.

Takeaway for Banks

Wire fraud liability frequently turns on decisions made long before the fraudulent wire arrives. Banks should periodically review their wire agreements and security procedures, confirm that the procedures remain commercially reasonable for their customers, document alternative security measures offered to customers, train employees to follow established procedures consistently, and include appropriate beneficiary name / account number provisions in their agreements.

When a fraudulent wire occurs, speed matters – but so does the bank's documentation. A bank that can demonstrate exactly which security procedure was agreed upon, why it was commercially reasonable, and how it was followed will be in a substantially stronger position.

This blog was drafted by Shelli Clarkston, an attorney in the Spencer Fane Banking and Financial Services practice group. For more information, visit spencerfane.com.

*Click **here** to subscribe to Spencer Fane communications to ensure you receive timely updates like this directly in your inbox.*