As Appeared in the Daily Business Review | May 2, 2019

Limiting the Liability of Financial Institutions for Unauthorized Wire Transfer Claims

BOARD OF CONTRIBUTORS

COMMENTARY BY
JONATHAN SCHWARTZ | PRINCIPAL
BRESSLER, AMERY & ROSS

With the rapid increase in electronic banking and commercial transactions, banks and other financial institutions like brokerage firms are finding themselves left behind when it comes to preventing liability for potential unauthorized wire transfer claims.

Imagine a scenario where a bank customer makes five wire transfers. For each transfer, the customer sends a signed letter of authorization (LOA). After receiving each LOA, a bank representative calls the client's telephone number and confirms the LOA. Management also calls the client and confirms the LOA as well as answers to personal questions (such as the client's address, date of birth and email address) to verify the client's identity.

Finally, management compares the signatures on the LOAs against the signatures on file. All of the signatures match and all of the personal questions are answered correctly. Nevertheless, after the transfers, the client claims that they were unauthorized and files a lawsuit. Will the customer prevail? Shockingly, the answer is presumptively yes.

CONTINUED ON PAGE 2

While this result seems absurd, Article 4A of the Uniform Commercial Code (UCC), codified in Florida as Chapter 670 of the Florida Statutes, clearly defines when a bank or the customer bears the risk of loss for an unauthorized wire transfer. Per UCC Section 4A-204, a bank is presumptively liable for honoring unauthorized payment orders. A bank can avoid this liability, however, if it complies with the "safe harbor" provision contained in UCC Section 4A-202(b).

This section requires: the bank and customer have an agreement that the authenticity of payment orders issued to the bank in the name of the customer as sender will be verified pursuant to a security procedure, the security procedure is a commercially reasonable method of providing security against unauthorized payment orders, and the bank accepts the payment order in good faith and in compliance with the security procedure and any written agreement or instruction of the customer restricting acceptance of payment orders issued in the name of the customer.

If the bank complies with these three conditions, the loss from honoring an unauthorized payment order shifts to the customer. Unfortunately, many financial institutions have neither appropriately established a security procedure nor included language in their customer agreements.

DEVELOPING A SECURITY PROCEDURE

A security procedure is a procedure established by agreement between a bank and a customer for the purpose of verifying payment orders. The procedure must meet the prevailing standards of good banking practice applicable to the particular bank, which requires the bank to be cognizant of present industry standards and the procedures in place at similar institutions.

The commercial reasonableness of a security procedure is a question of law to be decided by a court. Factors considered include: the wishes of the customer expressed to the bank and the customer's circumstances known to the bank, such as the size, type, and frequency of payment orders normally issued by the customer; alternative security procedures offered to the customer; and (c) security procedures used by similarly situated customers and banks.

Typically, banks use secret codes, passwords, PIN numbers, encrypted messages and private information like passport and national identification card numbers as part of a security procedure. Banks may also use more basic measures like contacting a customer by phone or comparing a signature on a payment order with a signature that the bank has on file. While favored by courts, a signature comparison is not sufficient by itself, however. Similarly, while calling a customer's telephone number to confirm answers to personal questions and verify the client's identity would likely be considered commercially reasonable, a court may find that the security questions are inadequate (such as asking for publicly available or easily obtained information), thereby rendering this procedure insufficient.

There is one instance in which a security procedure is presumed to be commercially reasonable. Under UCC Section 4A-202(c), where a bank offers a customer a commercially reasonable security procedure, the customer rejects it and chooses a different procedure, and the customer agrees in writing to be bound by any payment order issued in the customer's name (whether or not authorized), the bank will likely be protected from liability as long as it follows the customer's alternate procedure and accepts the payment order in good faith.

CONTINUED ON PAGE 3

CUSTOMER AGREEMENTS

For new customers, banks should add a provision to their new account agreement setting forth the bank's wire transfer security procedure and stating that the customer agrees to the procedure and that it is commercially reasonable. Language should also be inserted in the summary above the customer's signature advising the customer of the presence of the security procedure.

For existing customers, execution of a supplement to the new account agreement should be required as a condition to acceptance of any future wire transfer instructions. The bank may also consider a mailing to existing customers explaining the security procedure and stating that, by giving wire instructions in the future, the customer agrees to the security procedure and to its commercial reasonableness. It is unclear, however, whether this "negative consent" approach would be upheld by a court.

Finally, it is important to remain proactive. A bank should make a record of the steps taken to verify a wire transfer because, even if it has adopted a commercially reasonable security procedure, a claim can still survive if there is a question as to whether that security procedure was followed. Banks should also monitor developments in this area as evolving industry standards may require reforming the security procedure.

JONATHAN SCHWARTZ IS A PRINCIPAL IN THE FORT LAUDERDALE OFFICE OF BRESSLER, AMERY & ROSS. HIS PRACTICE FOCUSES ON BUSINESS AND SECURITIES LITIGATION, INCLUDING CLASS ACTION LAWSUITS, AT BOTH THE TRIAL AND APPELLATE LEVELS, AS WELL AS IN FINRA ARBITRATIONS.

CONTACT HIM AT JSCHWARTZ@BRESSLER.COM.