ORANGE COUNTY BUSINESS JOURNAL

Walking the High-Wire

Defending Against Liability for an Unauthorized Wire Transfer in California

In less time than it will take you to read this article, a cybercriminal on the other side of the world could steal millions of dollars from your customer's bank account without your knowledge. Using sophisticated "man-in-the-middle" and "man-in-the-browser" attacks, cybercriminals have learned to infiltrate even the most sophisticated online banking systems to log in to valid online banking sessions and wire millions of dollars overseas. In the aftermath of these attacks, often courts are left to determine who bears the responsibility for the loss—the financial institution or its customer.

With adequate preparation and information, financial institutions can minimize the risk that they will be held accountable for these losses. The right counsel can help draft policies, procedures and agreements to minimize risks to financial institutions, while also putting financial institutions in a stronger position to defend against claims for reimbursement of unauthorized wire transfers.

The Law

The California legislature provided the framework for courts to answer the question of who bears the risk of loss for an unauthorized wire transfer when it enacted the Uniform Commercial Code—Funds Transfers. The risk of loss initially falls on the bank. However, if the bank can prove its good faith compliance with an agreed-upon, commercially reasonable security procedure, the risk shifts to the customer. The customer then must prove that the wire was not sent by one of its agents or by someone who obtained access to the account from a customer-controlled source to put liability back on to the bank, which is a very difficult hurdle for the customer to meet.

First, a bank must prove that it accepted the wire transfer order in compliance with a commercially reasonable security procedure. The court considers the following factors to determine whether the bank's security procedure is commercially reasonable.

1. The wishes of the customer expressed to the bank;
2. The circumstances of the customer known to the bank, including the size, type, and frequency of payment orders normally issued by the customer to the bank;
3. Alternative security procedures offered to the customer; and
4. Security procedures in general use by customers and receiving banks similarly situated.

Thus, the question of commercial reasonableness depends, in large part, upon the unique circumstances of the customer. Importantly, the question of commercial reasonableness does not require that the bank offer the best security procedures available on the market. Instead, the bank must offer procedures that are "reasonable" in light of the specific circumstances of the bank and customer. As a result, it is important for banks to understand the individual circumstances of each customer and the security procedures in use by similarly situated banks for similarly situated customers.

Even if the security procedure that was used to process the unauthorized wire was not commercially reasonable, the bank may avoid liability under a limited exception. A security procedure is "deemed to be commercially reasonable" if the following requirements are met:

1. The customer chose an alternate security procedure after the bank offered, and the customer refused, a security procedure that was commercially reasonable for the customer; and,
2. The customer expressly agreed in writing to be bound by any payment order issued in its name and accepted by the bank in compliance with the chosen security procedure—whether or not authorized.

In order to benefit from this exception, the bank must prove both elements. A bank may more easily establish the first element if the customer has signed a written acknowledgement that a particular security procedure was offered and that the customer voluntarily chose a different procedure.

On its own, a commercially reasonable security procedure is insufficient to insulate a bank from liability stemming from an unauthorized wire transfer. The bank must also accept the wire transfer order in good faith and in compliance with the security procedure.

The California Uniform Commercial Code defines good faith to mean "honesty in fact and the observance of reasonable commercial standards of fair dealing." The first prong—honesty in fact—means that the bank employees involved in accepting the wire transfer order did not know that it was fraudulent at the time the order was accepted. The second prong—the observance of reasonable commercial standards of fair dealing—requires that the bank accept the wire transfer order in accordance with the reasonable expectations of the other party.

If the bank can prove that it accepted the wire transfer order in good faith and in compliance with a commercially reasonable security procedure, the bank still may be liable if the customer can prove that none of its employees sent the wire and the actual sender did not obtain access to the customer's account from a source controlled by the customer. However, it will be a rare circumstance where the customer can meet this burden.

Best Practices

To minimize the risk that a bank will be held liable for an unauthorized wire transfer, planning and diligence are required at every step of the process—from the selection and implementation of a core processor to the first contact with a potential new customer to the investigation into any unauthorized or fraudulent wire transfer. The following are best practices to help ensure that your bank is prepared to defend itself in the event of an unauthorized wire transfer:

▶ Commercially reasonable security procedures begin with the bank's selection and implementation of a core processor. In doing so, it is important for the bank to understand what security procedures other similarly-situated banks are offering their customers. The majority of banks in the United States obtain their core processors from one of three major vendors—FIS, Fiserv and Jack Henry. However, banks cannot assume that the mere implementation of a big-name core processor will end the court's commercial reasonableness inquiry, particularly since the bank exercises its discretion in choosing the core processor settings. The bank should be familiar with the Federal Financial Institutions Examination Council ("FFIEC") guidelines when making these choices.

▶ Customer agreements regarding online banking also play an important role in determining the commercial reasonableness of a security procedure. These online banking agreements should clearly delineate the security measures available to the customer at both the login and transaction levels. These security measures may include multifactor authentication, dual control, antivirus software requirements, daily limits on the total amount of wire transfers per day, per transaction limits and out-of-band authentication.

▶ If a customer declines to use security measures offered by the bank, the bank should require that the customer agree in writing that it is voluntarily choosing not to implement the bank's offered security procedure and will be bound by any payment order issued under the customer's chosen security procedure, whether or not authorized.

▶ Customer interactions, whether in person, on the phone, or electronically, should be carefully documented in order to later prove that the bank complied with its obligations to operate according to the reasonable expectations of the customer.

▶ When a customer provides notice to a bank of an allegedly unauthorized wire transfer, the bank should promptly perform a thorough investigation. The bank should involve experienced counsel in this investigation to provide legal advice throughout this process. Under the attorney-client privilege and the attorney work product doctrine, an attorney's involvement also will protect the investigation from discovery in any future litigation.

With careful planning and diligence, a bank can minimize the risk that it will be held liable for an unauthorized wire transfer. To our knowledge, Stradling is the only firm in California that successfully proved at trial that a bank's security procedures were commercially reasonable. As a result, Stradling is uniquely positioned to assist financial institutions by reviewing and auditing online banking policies, procedures and agreements, as well as to defend against claims for unauthorized wire transfers.

Marc J. Schneider
Shareholder, Litigation
(949) 725-4137
mschneider@sycr.com

Jason Anderson
Shareholder, Litigation
(949) 725-4233
janderson@sycr.com

additional contribution by

David Keithly
Associate, Litigation
(949) 725-4172
dkeithly@sycr.com

Kristen Spada
Associate, Litigation
(949) 725-4120
kspada@sycr.com