Compliance Adviser
An Exclusive Benefit for Members of:

IBSC
Independent Banks of South Carolina

Kelly Goulart, Sr. Manager – Regulatory Compliance
kgoulart@complianceadviser.org | 512.275.2231

eNews Headline: Who is Liable for Wire Fraud?

Question: We received an email from an accountholder instructing the bank to wire money. The customer's email address was correct, but the account was 'hacked' and the wiring instructions were not authorized by the accountholder. Which party is responsible – the bank or the accountholder?

Answer: This is complicated. Liability is a question of law based upon the circumstances and if the procedures used by both the bank and the accountholder were 'commercially reasonable' based upon the specifics for each and the transaction itself.

Under the Uniform Commercial Code, Article 4A.202, if the bank had promptly executed a payment order that had cleared the bank's 'commercially reasonable' security procedures and the bank had no independent reason to suspect the order was fraudulent, the bank met its burden of establishing it had acted in good faith and liability for the fraudulent transfer is the accountholders.

…snip

Sec. 4A.202. AUTHORIZED AND VERIFIED PAYMENT ORDERS. (a) A payment order received by the receiving bank is the authorized order of the person identified as sender if that person authorized the order or is otherwise bound by it under the law of agency.

(b) If a bank and its customer have agreed 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, a payment order received by the receiving bank is effective as the order of the customer, whether or not authorized, if (i) the security procedure is a commercially reasonable method of providing security against unauthorized payment orders, and (ii) the bank proves that it accepted 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. The bank is not required to follow an instruction that violates a written agreement with the customer or notice of which is not received at a time and in a manner affording the bank a reasonable opportunity to act on it before the payment order is accepted.

(c) Commercial reasonableness of a security procedure is a question of law to be determined by considering the wishes of the customer expressed to the bank, 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, alternative security procedures offered to the customer, and security procedures in general use by customers and receiving banks similarly situated. A security procedure is deemed to be commercially reasonable if (i) the security procedure was chosen by the customer after the bank offered, and the customer refused, a security procedure that was commercially reasonable for that customer, and (ii) the customer expressly agreed in writing to be bound by any payment order, whether or not authorized, issued in its name and accepted by the bank in compliance with the security procedure chosen by the customer.

(d) The term "sender" in this chapter includes the customer in whose name a payment order is issued if the order is the authorized order of the customer under Subsection (a) or it is effective as the order of the customer under Subsection (b).

(e) This section applies to amendments and cancellations of payment orders to the same extent it applies to payment orders.

(f) Except as provided in this section and in Section 4A.203(a)(1), the rights and obligations arising under this section or Section 4A.203 may not be varied by agreement.

Source link.

Below is from the FFIEC Wholesale Payment Systems Booklet Controls, stressing that all banks should have 'appropriate controls' for the verification of all payment orders.

…snip

The institution should have appropriate procedures in place to verify all processed payment orders. These procedures usually include the use of code words, call backs, and corporate resolutions authorizing certain employees to send payment orders. Verification and security procedures are extremely important in light of the potential for fraud or errors.

Source link.

What is 'commercially reasonable' is dynamic and subject to change. To protect against liability, banks and accountholders should all continually assess the 'commercial reasonableness' of their security measures, which may include: 1) the use of email accounts that require additional forms of authentication; 2) the use of digital signatures for messages; 3) the use of encryption to communicate; and 4) the frequency of password changes, among others.

Publish: 09/20