BURR FORMAN LLP

Bank Liability for Business Email Compromises and Fraudulent Payments

Article
05.12.2023

While at your place of business, you receive an email from a trusted source with an established vendor, notifying you that the vendor's bank account information has changed. Do you note the change in your business records and proceed accordingly to pay outstanding invoices from the vendor? Or, do you call a trusted source with the vendor to confirm that the vendor in fact changed its bank account information? If the former, your business likely has fallen victim to a business email compromise (BEC). If the latter, you have successfully evaded a BEC and did the right thing by calling and talking to a known and trusted source to confirm the correct account information.

Business email compromises are rampant. According to Proof Point's *Threat Advice*, direct financial losses from successful phishing incidents increased by 76% in 2022.[i] BECs often take the form of fake invoices from real vendors or business partners, fake requests from upper management to transfer funds to a bank account that actually belongs to the attacker, and fake notifications from real vendors and business partners of changes in banking account information.

Once funds are transferred to the attacker's bank account, they are usually immediately withdrawn and difficult or impossible to recover. If a business is able to detect the fraud in the first day or so after sending the wire, the funds sometimes may be recovered. Usually, however, businesses learn weeks (or months) after the electronic transfer that the intended recipient vendor did not receive payment. By that time, it is probably too late to recover the funds. In those cases, businesses should review their cyber and

RELATED PROFESSIONALS

Elizabeth B. Shirley, CIPP/US, CIPM

RELATED CAPABILITIES

Cybersecurity & Data Privacy

other insurance policies to determine whether the loss may be covered.

What is a bank's potential liability in BECs such as the one described above?

The Uniform Commercial Code (UCC) Section 4A-207 provides that if a payment order (including wire transfers) received by the beneficiary's bank includes the beneficiary's name and a different account number than the beneficiary's real account number, the bank is not liable for the misdirected wire unless the bank had "actual knowledge" that the beneficiary name and account number referred to different persons or entities. The bank does not need to affirmatively determine whether the name and number refer to the same person. UCC 4A-207(b)(1).

The Comments to UCC 4A-207 explain the rationale behind this law. The Comments recognize that "[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." UCC 4A-207, Cmt. 2. Additionally, the "[m]anual handling of payment orders is both expensive and subject to human error." Id. Thus, while it may be possible for the beneficiary's bank to determine whether the name and number refer to the same or different persons, banks have no duty to do so.

That said, if a bank has "actual knowledge" of the mismatched beneficiary and account number, then it may be liable. The question then becomes, what is "actual knowledge"? This is a fact specific inquiry, but the United States District Court for the Eastern District of Virginia held on December 18, 2020, that the plaintiff in that case stated a claim against the defendant bank of actual knowledge of a mismatch between the beneficiary name and account number.[ii] More specifically, the payment order in that case was commercially coded as "CCD" to a beneficiary business name that did not exist as a bank customer. Additionally, the fraudulent account number actually belonged to an individual, not a business. Note that the Eastern District of Virginia did not find that the plaintiff prevailed – only that it stated a claim in face of the defendant bank's motion to dismiss.

The takeaway is that banks enjoy broad protection from mismatched beneficiaries and account numbers in wire transfers and other payment orders – unless they have some actual knowledge of a mismatch. If you are with a banking institution and would like advice on whether your organization's procedures protect against imputed actual knowledge in fraudulent wire transfers and other payment orders, please contact us.

---

[i] Proof Point, "2023 State of Phishing," *Threat Advice*, 2023 State of the Phish Report - Phishing Stats & Trends | Proofpoint US, 5/8/2023.

[ii] *Studco Building System U.S., LLC v. 1st Advantage Federal Credit Union, et al.*, Case No. 2:20-cv-417 (E.D. Va. Oct. 18, 2020).