YOU'VE BEEN HACKED! NOW WHO'S LIABLE?

BY NICK VENTO

Email communications are increasingly used to conduct business, and those communications often lose formality in comfortable relationships. We trust that our email communications are secure when we have regular identifiable correspondence.

And then one day you receive a call from a client who has enjoyed a long-term, ongoing contractual relationship with a supplier. They communicate with the supplier regularly over email, including sending invoices and confirming payment. In the course of their business, the client received an email from the supplier: "We just switched bank accounts. Can you please change the wiring instructions on your payment for November's invoice? The new instructions are attached." The email address is familiar, and the client makes the payment on November's invoice to the new bank account, as instructed.

A week later, the client receives another email: "When do you expect to make payment on November's invoice? It is now overdue." They double-check their records, which shows the payment was sent the same day of the month as always. The client responds to their supplier with a copy of the wire confirmation. The supplier responds: "That's not our bank account. You still owe a payment." The client is horrified to discover that payment was not made to the supplier but to a hacker.

With the money long gone and the identity of the third-party fraudster unknown, the client is now looking to you to determine from whom they can seek recovery — after all, it was the supplier that allowed their email to get hacked. And shouldn't the bank have noticed the account name identified on the payment order did not match the account name associated with the bank account number identified in the payment order and halted the wire transfer?

Scenarios like this have now become common: A third-party fraudster sends an email message that appears to come from a known source making a legitimate request, tricking his target into sending money by fraudulent wire or ACH transfer instructions. The FBI refers to these schemes as business email compromise (BEC) and estimate they caused over $1.8 billion in losses in 2020 alone. *See* Internet Crime Report 2020, *available at* https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf (last accessed October 3, 2021).

Third-party fraudsters have targeted organizations large and small with equally devastating financial repercussions for their victims. It is rarely the case that the victims can reverse a fraudulent wire transaction in time, and the amount inadvertently transferred is usually withdrawn before it can be recovered from the receiving bank.

The question of who is liable from a BEC is difficult to answer today. The legal questions are still novel and applicable case law has provided limited guidance.

Victims of BECs have found little success in seeking recourse against their financial institutions. For example, in *Peter E. Shapiro, P.A., v. Wells Fargo Bank*, 795 F. App'x 741, 743 (11th Cir. 2019), the victim of a BEC sued his bank alleging the bank should not have processed a wire transfer that he initiated in connection with the closing of a business transaction, where the account name on the payment order conflicted with the name reflected on the deposit account. However, in affirming the lower court's decision, the Eleventh Circuit held that the bank was not liable under the Uniform Commercial Code (UCC), reasoning the bank "maintained and complied with reasonable routines" by processing the payment through its automated system based on a valid account number alone, without regard to a mismatch between names of the account holder and the intended beneficiary, which was noted in the system's audit trail but did not halt the transaction. *Id.* at 748.

In determining liability among victims of a BEC, courts have recently begun looking to Article 3 of the UCC (governing negotiable instruments). Generally, UCC § 3-420 provides that if a payor issues an instrument but fails to deliver the instrument into the payee's possession, the payor would still be liable for the obligation, as the obligation has not yet been satisfied. *See Bile v. RREMC, LLC*, 2016 WL 4487864, at *8 (E.D. Va. Aug. 24, 2016). However, where a negotiable instrument is subject to third-party fraud, UCC §§ 3-404 and 3-406 state the party whose failure to take ordinary care resulting in the loss must bear that loss, while the blameless party is entitled to rely on reasonable representations even when those reasonable representations were made by the third-party fraudster. This has come to be known as the "imposter rule." *Arrow Truck Sales, Inc. v. Top Quality Truck & Equip., Inc.*, 2015 WL 4936272, at *5 (M.D. Fla. Aug. 18, 2015) citing *State Sec. Check Cashing, Inc. v. Am. Gen. Fin. Servs.*, 409 Md. 81, 972 A.2d 882 (Md. App. 2009).

In applying the "imposter rule" to disputes involving BECs, courts will look to assign liability to the party that was "in the best position" to prevent the fraudulently induced mispayment. *See Beau Townsend Ford Lincoln, Inc. v. Don Hinds Ford, Inc.*, 759 F.App'x 348 (6th Cir. 2018) citing *Arrow Truck Sales, Inc. v. Top Quality Truck & Equipment, Inc.*, 2015 WL 4936272, at *6 (M.D. Fla. Aug. 18, 2015); *See also Jetcrete N. Am. Lp v. Austin Truck &*

Equip., 484 F. Supp. 3d 915 (D. Nev. 2020); *See also Bile v. RREMC, LLC*, No. 3:15cv051, 2016 WL 4487864 (E.D. Va. Aug. 24, 2016); *See also J.F. Nut Co., S.A. de C.V. v. San Saba Pecan, LP*, 2018 WL 7286493, *3 (W.D. Tex. July 23, 2018).

Determining which party was in the "best position" to prevent a BEC scam, and thus responsible for the misdirected payment, involves a thorough fact-specific analysis. *Arrow Truck Sales Inc. v. Top Quality Truck & Equipment Inc.* provides a good example in this regard. In *Arrow Truck*, the parties exchanged numerous emails during the negotiations for the purchase of twelve trucks for $570,000. One of those emails contained wiring instructions used in previous transactions between the parties. During the parties' negotiations, a third-party hacked into the email accounts of both buyer and seller, creating new email accounts that were almost identical to the actual accounts. Eventually, the third-party hacker used the seller's email account to send the buyer an email with new wiring instructions. The updated instructions specified an out-of-state bank and a different beneficiary, though the seller was listed somewhere on the instructions. The buyer followed the "updated" instructions and unknowingly wired the $570,000 to the hacker. The seller never received the money and refused to deliver the trucks to buyer. The buyer filed suit against seller.

Applying the UCC's imposter rule analysis, the *Arrow Truck* court determined that, although neither the buyer nor the seller were negligent in the manner that they maintained their respective e-mail accounts, the buyer had "more opportunity and was in the better position to discover the fraudulent behavior based on the timing of the e-mails and the fact that the fraudulent wiring instructions involved a different beneficiary, different bank, different location, and different account information from all of the previous wiring instructions." *Arrow*, 2015 WL 4936272 at *8. Furthermore, given the buyer had received conflicting e-mails containing two sets of wiring instructions — one legitimate and one fraudulent — he should have confirmed the information with the seller prior to wiring any funds. Therefore, the court concluded that the buyer was responsible for the loss since he was in the best position to prevent it.

In *Beau Townsend Ford Lincoln Inc. v. Don Hinds Ford Inc.*, the buyer agreed to purchase twenty SUVs from the seller. A third-party then hacked into the seller's email account, changed the email forwarding rules in the account, and used the email account to send the buyer fraudulent wire instructions, which the buyer used to send over $700,000. The Sixth Circuit reversed and remanded the lower court's summary judgment ruling for the seller, noting the seller "was at least partially responsible for its own losses." *Beau*, 759 F.App'x at 357. Applying the UCC's imposter rule, the Sixth Circuit observed that the factfinder would need to determine whether either the buyer's or seller's "failure to exercise ordinary care contributed to the hacker's success and would then have to apportion the loss according to their comparative fault." *Id.* In this regard, the seller could point to the suspicious nature of the wire instructions to argue that the buyer could have prevented the loss, while the buyer could argue the seller was in the best position to avoid the loss by better protecting its email servers. The parties eventually settled.

Conclusion

As third-party fraudsters that operate BEC scams are often able to abscond with the money from the receiving account before any fraud is discovered, the victims, faced with a devastating loss of funds, are now looking to courts for recovery. While the law has been slow to react to the realities of doing business in the 21st century, the growing body of case law around this issue suggests that losses attributable to a BEC should be borne by the parties in the best position to have prevented it. This, in turn, involves a fact-specific analysis of the circumstances surrounding the loss. Furthermore, banks will likely be shielded from liability if they reasonably follow instructions as provided. Thus, the victims' own policies and actions surrounding the BEC will play a key role in determining liability and potential recovery.

Nick Vento is a commercial litigator at Schneider Smeltz Spieth Bell LLP. Nick has been a member of the CMBA since 2016. He can be reached at (216) 696-4200 or at nvento@sssb-law.com.