Articles + Publications | November 16, 2020

# WTF?! – Wire Transfer Fraud Litigation

Privacy & Cybersecurity Newsletter

**WRITTEN BY**

Molly McGinnis Stine | Matthew Murphy | Joshua Fliegel

Threat actors have recently and significantly increased efforts to defraud organizations and individuals through business email compromise (BEC). In BEC and related scams, the threat actors trick unsuspecting targets into sending money to the perpetrator, often either by fraudulent wire or ACH transfer instructions.[1] These scams, which target organizations from multinational corporations to small churches, rely heavily on the art of deception to defraud targets or to dupe them into desired action. The financial impact can be considerable and victims have turned to litigation to recover losses.

**The Schemes**

Generally, BECs involve communications with the target organization that are designed to appear legitimate. Threat actors have developed certain variants of BEC scams.[2] This article focuses on those schemes that look to trick people into sending funds to a fraudster. In some, the threat actors pose as the CEO or other executive of an organization to instruct subordinates to make a payment for a fabricated invoice or other expense. In others, the bad actors pose as a recognized vendor to send what appear to be (but are not) genuine invoices or payment instructions. Others target real estate transactions to send fraudulent payment instructions to buyers.

To execute these schemes, threat actors rely on impersonations and social engineering to collect or make an educated guess about some information about the target company to send communications that appear legitimate. Sometimes, threat actors may create a spoofed email account that is slightly different from a legitimate address. Threat actors may also send phishing emails to one or more individuals at the target organization to trick the individual into revealing confidential information or passwords or clicking on a link or attachment to deploy malware on the target's computer environment. Once a threat actor has access to the target's email account, the threat actor may change rules in the compromised email account to intercept and redirect emails. They may then use the compromised email to masquerade as the account owner and email directly with others to send fraudulent payment instructions.

In each of these scenarios, the goal is to reconnoiter information about the target organization, such as billing practices, details about a transaction, or even communication style. Later emails to the target organization leverage this intelligence to send fraudulent payment instructions.

BECs have become a big business for threat actors. The Federal Bureau of Investigation's Internet Crime Complaint Center ("IC3") tracks and analyzes BEC complaints and reports. They have reported that between June 2016 and July 2019, global victims suffered losses of more than $26.2 billion, with the U.S. making up over $10 billion of that total.[3]

In all too many instances, organizations are unable to reverse fraudulent wire transaction or ACH transfer instructions in time and the amount transferred cannot be recovered from the receiving bank before it is withdrawn by the threat actor.

**The Litigation**

As a result, victims may seek recovery from the other party to the affected transaction, service providers involved in sending funds, or their bank. In court cases throughout the country, plaintiffs have had a difficult time recovering their losses stemming from their payment of funds to hackers through wiring instructions sent via a compromised email, and also in their attempts to hold their banks or other parties liable. This is largely due to the states' adoption of the Uniform Commercial Code (U.C.C.), under which a party needs to be able to show that the counterparty to the compromised transaction did not exercise ordinary care or committed some sort of negligence outside of the contract or transaction parameters.

*Arrow Truck Sales Inc. v. Top Quality Truck & Equipment Inc.*[4] provides an example of how a threat actor may run a BEC scam, and the fallout that the affected parties must endure. In *Arrow Truck*, the parties exchanged numerous emails during the negotiations for the purchase of twelve trucks for over $500,000. One of those emails contained wiring instructions that the buyer had used for past purchases from the other party. However, evidence was presented to the court that threat actors had hacked into the email account of both buyer and seller parties' email accounts created spoofed email accounts to appear as though they were the buyer and seller's actual email accounts. The threat actor then used a spoofed email account to masquerade as the buyer and send the settler fraudulent wire instructions. Notably, the threat actor had also used legitimate email accounts of both the buyer and the seller to send communications to the other during the course of the fraud. Also, although the seller was unaware that the buyer had received fraudulent wire instructions, he then resent the legitimate instructions to the buyer. However, the buyer used the fraudulent instructions when he attempted to purchase the trucks. Upon discovery of the fraud, the seller, who had never received payment, refused to deliver the trucks.

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." Given that 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 it was the buyer that bore the responsibility for the loss as he was in the best position to prevent it. In reaching this decision, the court relied on the U.C.C.'s 'imposter rule' which places liability on parties whose lack of ordinary care contributed to the loss.

In another BEC case also involving the purchase of vehicles, the court cited *Arrow Truck* for the proposition that "losses attributable to fraud should be borne by the parties in the best position to prevent the fraud."[5] In *Beau Townsend Ford Lincoln Inc. v. Don Hinds Ford Inc*., the buyer agreed to purchase twenty SUVs from the seller. Unbeknownst to both, a threat actor had hacked into the seller's email account, changed email forwarding rules in the email 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 that the seller was "was at least partially responsible for its own losses"[6] In remanding the

case for further fact-finding, the court observed that the seller could point to the "suspicious nature of the wire instructions" to argue that the buyer could have prevented the loss. The buyer, on the other hand, could argue that it was the seller's email that was hacked, and therefore the seller was in the best position to avoid the loss.[7] Looking to the principles of the U.C.C., 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."[8] The parties eventually settled.

The *Beau Townsend* decision suggests that one factor that courts may consider is whose email account was compromised, and the circumstances surrounding that compromise. In *Tillage Commodities Fund LP v. SS&C Tech. Inc*.,[9] an investment fund sought damages from its fund administrator in connection with the administrator's processing of wire transfer requests using fraudulent instructions. The fund alleged that the administrator "breached the implied covenant of good faith and fair dealing by failing to take reasonable precautions to prevent the fraud and by frustrating plaintiff's recovery efforts."[10] The court denied the administrator's motion to dismiss, concluding that the fund had sufficiently alleged that the administrator's conduct "evince[d] a reckless disregard" for the fund's rights insofar as the administrator had "failed to comply with basic cybersecurity precautions and actively disregarded its own policies as well as obvious red flags."[11] As in *Beau Townsend*, the parties settled prior to an ultimate disposition.

Where transferred funds cannot be recovered, some victims of BECs also seek recourse from their financial institutions. For example, in *Peter E. Shapiro, P.A., v. Wells Fargo Bank*, the victim of a BEC sued his bank alleging that the bank should not have processed a wire transfer that he initiated in connection with the closing of a business transaction.[12] The victim alleged that the bank "should not have processed his wire because it knew—or with the exercise of reasonable due diligence should have known—that the account name identified [on] payment order did not match the account name actually associated with the Wells Fargo account number identified in the payment order."[13] The wire instructions named the proper beneficiary, but incorrectly identified the account information for a Nigerian citizen living in the United States that was not a party to the transaction. The victim did not confirm the wire instructions, and used them to wire more than $500,000. Notwithstanding this possible name mismatch, the bank processed the wire because the account number matched a valid account number at the bank.[14] The Eleventh Circuit affirmed the lower court's decision that the bank was not liable under the U.C.C. due to the bank's reliance on the fraudulent account numbers the plaintiff sent it, even though it did not match the beneficiary of the order. The Eleventh Circuit concluded that the bank "maintained and complied with reasonable routines, and thus exercised due diligence, with respect to the processing of [the] payment order"[15] through the bank's automated system when it processed the payment based on the name and number on the receiving account.

Likewise, in *Capten Trading Ltd. v. Banco Santander International*, a bank received a series of wire transfer requests from an account holder's designated account. However, the account holder never authorized the wire transfers.[16] The Southern District of Florida found that the state's statutes adopting the Uniform Commercial Code displaced the account holder's common law claims and granted summary judgment in favor of the bank, which had executed the instructions consistent with the instructions presented to it through the account holder's email account. The court in *Sarrouf Law LLP v. First Republic Bank*,[17] reached a similar result in 2020. There, the appeals court of Massachusetts affirmed a lower court's opinion finding a bank was not negligent nor acted in bad faith when it processed fraudulent wire transfers and processed a counterfeit check it believed was initiated by the client. The lower court had granted summary judgment for the bank because it found it had fulfilled its U.C.C.

obligations to exercise ordinary care in the handling of the transactions at issue, and was simply following the client's instructions, even though the transactions were initially red-flagged, reviewed, and deemed legitimate. And in another case from 2020, *Beins, Axelrod, PC v. Analytics, LLC*,[18] claims against Citigroup were dismissed because it was not shown that the bank knew about the hacked email sending fraudulent wire transfer instructions, nor did it help with the crime, but merely processed the payment according to what a third party had submitted. The court disagreed with the plaintiff's attempt to compare the bank to a "farmer who provided a temporary safe harbor for the robber's loot" and obligated when "unfamiliar people wearing ski masks . . . ask[ed to] hide bags of cash in its barn for a few days in exchange for a few of the twenties in the bag." However, the court ruled the analogy does not work as "Plaintiff does not provide any facts that indicate that the bank 'closed its eyes' to the hacker's obvious crime." If such an analogy was apt, according to the court, every bank would be liable every time it was used as part of a criminal's scheme. Because that cannot be, the claims were dismissed.

In contrast, in the unreported decision in *Essgeekay Corp. v. TD Bank*, an account holder noticed three unauthorized transactions totaling over $175,000.[19] Given that the wires were initiated from his business partner's account, which was not the usual process, the business partner tried to log into his account and discovered that the bank's security procedures had locked him out. The bank admitted that, before processing the transfers, it attempted to contact the business partner by phone and email to obtain approval for the transfers, but that it ultimately authorized the transfers even though it had never received approval from the business partner for any of the transfers. The bank later advised the account holder that and business partner that the funds had been lost and the wires would not be reversed. In the ensuing litigation against the bank, the court denied a motion to dismiss, observing that the plaintiff had sufficiently pled that the bank failed to accept the payment orders in good faith and in compliance with the security procedure.[20] The *Essgeekay* decision echoed an earlier ruling in the unreported decision of *Experi-Metal, Inc., v. Comerica Bank*,[21] where one of plaintiff's employees unknowingly opened a phishing email purporting to be a Comerica Bank form, and entered in his credentials in a fake site, which allowed the attackers access the plaintiff's bank accounts with Comerica. Over six hours, the attackers made 93 fraudulent transfers making transfers totaling over $5 million. The court found that under Michigan law, Comerica Bank failed to meet its burden that its employees met reasonable commercial standards of fair dealing in the context of the fraudulent transfers, especially in allowing unusual overdrafts of Experi-Metal's accounts, and ordered them to repay the sums lost. While there was no suggestion that any specific Comerica employee acted dishonestly, its failure to recognize the transfers as fraudulent was sufficient for liability.[22]

**Conclusion**

All too often, the threat actors that operate BEC scams withdraw the money from the receiving account before the fraud is discovered. The victims, faced with sometimes devastating loss of funds, have increasingly looked to courts for recovery. The growing body of case law around the issue suggests that "losses attributable to fraud should be borne by the parties in the best position to prevent the fraud." It also suggests that banks will likely be shielded from liability if they reasonably follow instructions as provided. These observations indicate that an entity's own behavior, including its interactions with its business partners, with others in transactions, and with its banks, plays a key role. In our next article, we will discuss some practical tips for organizations to consider in best avoiding falling prey to schemes and best being ready if a scam succeeds.

---

[1] Wire transfer and ACH fraud are just two ways in which threat actors try to profit from BECs. Others include, for example, diverting direct deposit of payroll by seemingly changing account information or encouraging recipients

to buy gift cards and then share the card codes with the trickster. Also, bad actors could use BECs to try to gain access to an organization's systems or data for financial purposes other than redirecting a specific payment.

[2] We note that successful scams may attempt business email compromise but may successfully hijack funds whether or not the victim's email system is actually compromised. In fact, system compromise may not be the fraudster's goal with the threat actor hunting only for information to use for a scheme or requesting certain actions by the recipient. While this article discusses all of this generally within the context of BECs, the distinction is important as the risks and solutions will differ for technological infiltrations and for social engineering efforts.

[3] https://www.ic3.gov/Media/Y2019/PSA190910 (last accessed October 28, 2020).

[4] No. 8:14-CV-2052-T-30TGW, 2015 WL 4936272 (M.D. Fla. Aug. 18, 2015).

[5] *Beau Townsend Ford Lincoln, Inc. v. Don Hinds Ford, Inc*., 759 F. App'x 348, 357 (6th Cir. 2018).

[6] *Id*. at 357.

[7] *Id*. at 358-59.

[8] *Id*. at 357. The court also examined the issue under the principles of agency law, noting that the Restatement (third) of Agency states that if a person "carelessly caused [the] belief" that "an actor has authority as an agent," the person "is subject to liability to a third party who justifiably is induced to make a detrimental change in position because the transaction is believed to be on the person's account." Id. The court concluded that it could not resolve this factual dispute at the summary judgment stage. Id. at 359.

[9] *Tillage Commodities Fund, L.P. v. SS&C Techs., Inc*., 151 A.D.3d 607, 608, 58 N.Y.S.3d 28 (2017).

[10] *Id*. at 608.

[11] *Id*.

[12] *Peter E. Shapiro, P.A. v. Wells Fargo Bank N.A*., 795 F. App'x 741, 743 (11th Cir. 2019).

[13] *Id*.

[14] *Id*. at 744.

[15] *Id*. at 748.

[16] No. 17-20264-CIV, 2018 WL 1558272, at *2 (S.D. Fla. Mar. 29, 2018).

[17] 97 Mass. App. Ct. 467, 471, 148 N.E.3d 1243, 1248 (2020).

[18] No. CV 19-3794 (JEB), 2020 WL 19527 99 (D.D.C. Apr. 23, 2020).

[19] No. CV183663ESCLW, 2018 WL 6716830, at *1 (D.N.J. Dec. 19, 2018) (not reported).

[20] *Id*. at *4.

[21] No. 09-14890, 2011 WL 2433383 (E.D. Mich. June 13, 2011) (not reported).

[22] *See also Patco Construction Company, Inc. v. People's United Bank*, 684 F.3d 197 (1st Cir. 2012), where fraudsters gained access to the plaintiff's account and made 6 withdrawals through the bank's eBanking platform. Because these transactions were unusual, they were flagged by the bank's security system, but the bank failed to manually monitor these reports, which went unaddressed for 6 days before the transactions were stopped. While the lower court granted the bank's summary judgment motion on the grounds that while not perfect, the banks security procedures were commercially reasonable. The First Circuit reversed, finding multiple issues with the bank's security procedures, such as 1) setting the security question threshold at $1 substantially increased the risk of fraud, 2) failing to implement supplemental security features after it was on notice that its features posed inherent risks, and 3) failing to manually monitor the risk reports which indicated the transaction in question were fraudulent, which as a whole, made the banks procedures unreasonable. The parties eventually settled.

**RELATED INDUSTRIES + PRACTICES**

- Data + Privacy
- Privacy + Cyber