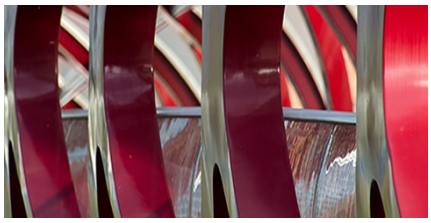
masuda funai



News & Types: Client Advisories

Beware of Business E-mail Compromise ("BEC") Schemes

1/5/2022

By: Kenton P. Knop

Practices: Commercial, Competition & Trade, Litigation

EXECUTIVE SUMMARY

Business e-mail compromise ("BEC") schemes have become cybercriminals' method of choice in defrauding businesses by impersonating a payee party and deceiving a payor party into sending funds to an account controlled by the fraudulent third party. In response to BEC schemes, courts are increasingly turning to traditional Uniform Commercial Code ("UCC") principles holding that the party that is in the best position to avoid the loss and that fails to exercise reasonable care to avoid the loss then becomes responsible for the loss. To protect against the ever-present risks of BEC fraud in today's business environment, it is more important than ever for businesses to educate their customers to first verify any changes in payment information by phone through a trusted number before sending any funds.

Popular media tends to depict cybercriminals as skillful hackers who infiltrate a target's computer system to steal sensitive data and money from the target's bank accounts. The reality is that cybercriminals are increasingly relying on simple deception to steal money and data from targets, in so-called BEC schemes. The Federal Bureau of Investigation Internet Crime Complaint Center ("IC3") stated in its *2020 Internet Crime Report* that in 2020 alone, the IC3 received 19,369 complaints of BEC fraud, with $1.8 billion of adjusted losses attributed to BEC fraud. In comparison, the IC3's report stated that ransomware attacks in 2020 accounted for only $29 million in losses.

BEC schemes typically involve two parties who conduct business primarily over e-mail, and a fraudulent third party who, usually through a phishing e-mail sent to a company employee or other fraudulent means, gains access to one party's e-mail account and is able to surreptitiously monitor the e-mail traffic between the two business parties. When the e-mail traffic indicates that the time has come for payment to be made on an invoice or a settlement payment, usually via wire transfer or ACH, the fraudulent third party inserts itself into the conversation by impersonating the payee party's personnel with an e-mail account from a fake domain made to resemble the payee's legitimate e-mail address. The third party sends an e-mail to the payor claiming that its bank information has changed, and then provides payment instructions to a new bank account controlled by the third party. The payor, seeing that the new bank information appears to come from the person with whom it has been communicating all along, usually does not think twice about sending the money to the new bank account. By the time the parties discover that the payment was sent to the wrong bank, the third

party has likely disappeared with the money and it is often too late for the sending or receiving banks to freeze or recover the funds.

When the innocent parties in a BEC scheme resort to litigation over the unpaid obligation, courts have turned to traditional UCC negotiable instrument principles under UCC Sections 3-404(d) and 3-406 discussing "imposters" and forged instruments to determine who bears the loss. In *Arrow Truck Sales, Inc. v. Top Quality Truck & Equip., Inc.*, Case No. 8:14-cv-2052-T-30TGW (M.D. Fla. Aug. 18, 2015), a Middle District of Florida case involving a BEC scheme that diverted the payor plaintiff's payments totaling $570,000 for trucks purchased from the payee defendant to a fraudulent third-party's account, the court applied the "imposter" rule from UCC Section 3-404(d), which provides that the party that was in the best position to prevent the fraud by using reasonable care and that fails to exercise such care bears the loss. The court in *Arrow Truck Sales* determined that the payee did not negligently handle its e-mail account to allow the third party access to commit the fraud, and found that in fact both parties' e-mail accounts were hacked and it was not possible to tell which party had been compromised first or how it occurred. The court then found that the plaintiff, upon receiving conflicting payment instructions, should have exercised reasonable care by calling the defendant to confirm the correct instructions before sending payment. Because the plaintiff failed to call the defendant first before sending payment to the fraudulent third party, the court held the plaintiff responsible for the loss associated with the fraud. Similarly, in *Beau Townsend Ford Lincoln, Inc. v. Don Hinds Ford, Inc.*, 759 F. App'x 348 (6th Cir. 2018), a BEC case in which the payor's payment meant for the payee was redirected to a fraudulent third party, the Sixth Circuit adopted the approach taken in *Arrow Truck Sales* and ruled that a trial was necessary to determine which party was in the best position to prevent the fraud, with the trial court apportioning the loss based on comparative fault principles. More recent cases in other jurisdictions have applied the "imposter" rule in similar BEC situations. See *Jetcrete N. Am. LP v. Austin Truck & Equip., Ltd.*, 484 F. Supp. 3d 915 (D. Nev. 2020) (rejecting the argument that the payee whose e-mail account was hacked in BEC scheme was liable for resulting losses, and holding that the payor was in the best position to avoid the loss by verifying conflicting payment instructions with the payee by phone and should therefore bear the loss); *Parmer v. United Bank*, No. 20-0013 (W. Va. Dec. 7, 2020) (holding that the payor of misdirected funds in a BEC scheme did not exercise reasonable care by failing to verify payment information with the payee before sending funds, and therefore must bear the loss).

In light of the recent caselaw involving BEC schemes, it is apparent that courts, recognizing that even well-implemented IT security measures cannot completely eliminate the risk of e-mail compromise, are placing less emphasis on which party was initially compromised and are instead placing responsibility on the party in the best position to avoid the loss. In most cases, the party in the best position to avoid the loss is the payor that has received conflicting payment instructions from the fraudulent third party and can resolve the issue by making a simple phone call to the payee to confirm the correct information before sending funds. Accordingly, businesses are strongly urged to implement protocols and educate their customers to protect themselves by emphasizing that any apparent changes in payment information must first be confirmed by a phone call using a trusted phone number before any payments are made. This low-tech method of phone verification is the best line of defense against what has become an inescapable risk of doing business in today's high-tech environment. If you have questions about BEC schemes or would like further information on how to protect

your business against such schemes, please contact your Masuda Funai relationship attorney for a consultation.