The Evolving Landscape of Business Email Compromise Litigation—A Focus on Texas

Business email compromises ("BEC") remain one of the most prevalent internet-related crimes, with businesses and individuals suffering massive financial losses—the scale of which has only risen since the onset of the COVID-19 pandemic. Between 2019 and 2021, the Internet Crime Complaint Center (the "IC3")[1] reported 63,098 BEC complaints, with adjusted losses exceeding $5.9 billion.[2] According to IC3 report statistics from 2019 to 2021, Texas reported the second-highest number of BEC of any state, while the amount lost almost doubled—from $124 million in 2019 to over $233 million in 2021.[3] While the amount of damage caused by BECs varies widely, some particularly damaging BECs have cost the victims upwards of $10 million.[4] Further complicating matters, courts across the country have not adopted a uniform framework for apportioning liability in litigation stemming from these incidents, and there are very few cases from Texas courts addressing this growing area of law. But before examining how Texas courts have treated these complex frauds, it is essential to understand how these frauds have evolved over the years.

---

[1] The IC3 is an online Federal Bureau of Investigation (FBI) portal that allows the public to report internet crimes to the FBI. *See IC3 Mission Statement*, FEDERAL BUREAU OF INVESTIGATION, https://www.ic3.gov/Home/About, (last visited Oct. 25, 2022).
[2] *Internet Crime Report 2021*, FEDERAL BUREAU OF INVESTIGATION, at 9, https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf (last visited Oct. 26, 2022); *Internet Crime Report 2020*, FEDERAL BUREAU OF INVESTIGATION, at 10, https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf (last visited Oct. 26, 2022); *2019 Internet Crime Report*, FEDERAL BUREAU OF INVESTIGATION, at 9, https://www.ic3.gov/Media/PDF/AnnualReport/2019_IC3Report.pdf (last visited Oct. 26, 2022).
[3] *2021 State Reports*, FEDERAL BUREAU OF INVESTIGATION, https://www.ic3.gov/Media/PDF/AnnualReport/2021State/StateReport.aspx#?s=48 (last visited Oct. 26, 2022).
[4] *14 Real-World Examples of Business Email Compromise*, TESSIAN, https://www.tessian.com/blog/business-email-compromise-bec-examples/ (last visited Oct. 25, 2022).

BEC Scams—A Brief Explanation

The FBI defines BECs as "a sophisticated scam targeting both businesses and individuals performing transfers of funds. The scam is frequently carried out when a subject compromises legitimate business email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds."[5] A BEC involves three parties: a company, its vendor, and a threat or bad actor. Historically, BECs have involved impersonating the email account of a company executive, a vendor, or some other trusted or authoritative source in an attempt to redirect legitimate outstanding payments from an unsuspecting target to the bad actor's account. An employee, believing they are exchanging emails with another employee within the company or their known vendor, is conned into transferring funds (often through wire transfers) to the threat or bad actor instead of the legitimate vendor.

However, since the COVID-19 pandemic increased the use of virtual meeting platforms, bad actors have turned to using these online platforms to perform even more sophisticated schemes. For example, the bad actor may invite an employee to a virtual meeting with a known company executive and, during the meeting, pretend to experience technical difficulties while instructing the employee to wire funds to the bad actor's account (created solely to receive stolen funds).[6] Once the transfer is complete, the bad actor quickly transfers the stolen funds from the bank account to cryptocurrency wallets—making recovery nearly impossible if not timely detected.

After a compromise is detected and the money is unrecoverable, a dispute will arise because the vendor still wants to be paid for the goods or services it provided. But the company

[5] *Internet Crime Report 2021*, *supra* note 3, at 9.
[6] *Id.*

believes they already paid the funds—that the funds were misdirected is the vendor's fault (because the vendor's computer systems or email was compromised or because the vendor was in a better position to know of the fraudulent scheme). Sometimes, the business will determine that it was an internal failure (for example, if the bad actor impersonated another employee, not the vendor). In such instances, the company may decide to absorb the loss. Other times, even if it can be established that the compromise was on the vendor's side, because the business partners would rather continue their relationship, they are able to reach a mutual resolution without litigation with the vendor agreeing to issue invoice credits, discounts, or similar reduction in the outstanding amount.

Consequently, very few cases end up in litigation due to these incidents, and even fewer result in a court opinion. When the parties cannot resolve the dispute, and a lawsuit is filed, the courts must decide which party should bear the loss of the fraud—the company that sent the money or the vendor who should have received it. Sometimes, the company may also feel the bank should have detected an issue in the wire information (maybe a mismatch between the account number and account name) and may sue the bank. In other cases, a dispute may arise as to whether an insurance policy should cover the loss.

The Two Approaches—The UCC's Imposter Rule versus Common Law Contract/Tort Analyses

Courts around the country have taken varied approaches to these disputes, with most courts applying the statutory framework for the "imposter rule" under the Uniform Commercial Code and others considering general contract/tort principles.[7] The "imposter rule" takes its name

[7] *See Beau Townsend Ford Lincoln, Inc. v. Don Hinds Ford Inc.*, 759 F. App'x 348, 357 (6th Cir. 2018) (applying the imposter rule to an Ohio case); *Peeples v. Caroline Container, LLC*¸ No.

from the eponymous section of the Uniform Commercial Code ("UCC"),[8] which sets the framework for determining who should bear the loss when a negotiable instrument is delivered to an impostor. Under U.C.C. § 3-404(d), if one party to a transaction fails to exercise "ordinary care" in the process of delivering payment to a fraudulent entity, the party who suffered the loss may recover from the other for their failure to exercise ordinary care.[9] In other words, the fault is allocated based on the relative fault of each party. Some common factors that a court may consider when determining if a party exercised ordinary care may include (1) what protections the seller had in place to protect their emails; (2) whether the party that sent the wire tried to authenticate the payment instructions; (3) the nature of the fraudulent instructions; and (4) the nature of the fraudulent emails soliciting the fraud.[10] This approach is particularly fact intensive but appears to be the prevailing approach courts have applied to these disputes.[11]

Courts have also applied the general legal principles often used in contract and tort cases to determine risk allocation. When applying contract principles, courts usually find that the party that was supposed to pay based on the contract is still obligated to remit payment.[12] In reality, this often means that the company that has been defrauded must pay *twice*—by accident to the bad actor and by contract to the other party.[13] Some courts have also applied common law

---

4:19-CV-21-MLB, 2021 WL 4224009, *8 (N.D. Ga. Sept. 16, 2021) (applying contract principles to a BEC scam in a Georgia court); *Jetcrete N. Am. LP v. Austin Truck & Equip., Ltd.*, 484 F. Supp. 3d 915, 920–21 (D. Nev. 2020) (rejecting that a hacker may act as an agent for a company).

[8] U.C.C. § 3-404.

[9] *Id.*

[10] *See, e.g., Arrow Truck Sales Inc. v. Top Quality Truck & Equip., Inc.*, No. 8:14-CV-2052-T-30TGW, 2015 WL 4936272, at *6 (M.D. Fla. Aug. 18, 2015) (discussing these factors).

[11] *See, e.g., Beau Townsend Ford Lincoln*, 759 F. App'x at 357.

[12] *See, e.g., Peeples*, 2021 WL 4224009, at *8 (applying the contract approach).

[13] *See, e.g., id.* (determining that because the defendant had not paid the plaintiff as required by the parties' contract, the plaintiff was obligated to pay despite the fact that they had been defrauded).

doctrines, like agency, to these relationships. Courts applying agency principles often determine that the critical factor is whether the true vendor acted in a way that led the company to reasonably believe that the bad actor was the vendor's agent.[14] Despite these other approaches, most courts seem to favor the Imposter Rule.

Texas Courts Apply the Imposter Rule's Balancing Framework

There is scant case law and authority in Texas directly discussing this allocation of risk between contracting parties affected by BEC.[15] The few state and federal Texas cases have consistently applied the "imposter rule" of the UCC.

J.F. Nut Company v. San Saba Pecan provides an example of how a Texas court might handle the risk allocation dispute.[16] There, San Saba had been making payments to J.F. Nut via email.[17] They later received different instructions, and the company sent several payments totaling over $1 million.[18] But J.F. Nut never received those payments and claimed they were victims of an email-impersonation BEC scam.[19] In considering the companies' pleadings, the court not only explicitly rejected the agency theory of liability[20] but also found Texas law generally silent regarding liability for redirected payments.[21] Reviewing case law from other

[14] *See, e.g.*, *Jetcrete N. Am. LP*, 484 F. Supp. 3d at 920–21 (rejecting that a hacker may act as an agent for a company).
[15] *See J.F. Nut Co., S.A. de C.V. v. San Saba Pecan L.P.*, No. A-17-CV-00405-SS, 2018 WL 7286493, at *3 n.4 (W.D. Tex. July 23, 2018).
[16] *Id.* at *1.
[17] *Id.*
[18] *Id.*
[19] *Id.*
[20] *See id.* at *3.
[21] *Id.* at *2–3.

federal courts, the court concluded that liability should be based on an allocation of fault between the two companies—effectively adopting the "imposter rule."[22]

The second case, *Prosper Florida v. Spicy World of USA*,[23] followed the same approach as *J.F. Nut* but took place in Texas state court. There, Prosper Florida tried to complete a payment to Spicy World, but a third party fraudulently caused the payment to be redirected away from its intended recipient via a BEC scheme.[24] The parties then sued each other over who was liable for the payment.[25] In summarizing case law, the Texas court came to the same conclusion as *J.F. Nut*—"that any loss resulting from fraudulently misdirected payments should be placed on whichever party to the contract the factfinder deems to be most at fault for the misdirection."[26]

That is not to say that a defrauded party might not have other options. If parties act quickly at the outset, for example, law enforcement agencies such as the FBI and the Department of Homeland Security ("DHS") can help trace and recover fraudulently transferred funds. As mentioned earlier, some defrauded companies have tried to sue the bank or other financial institution that facilitated the transfer, alleging the bank was negligent in processing the fraudulent payment, usually due to a mismatch between the account number and accountholder

[22] *Id.* at *3.
[23] *Prosper Florida, Inc. v. Spicy World of USA, Inc.*, 649 S.W.3d 661 (Tex. App.—Houston [1st Dist.], Apr. 28, 2022).
[24] *Id.* at 665.
[25] *Id.*
[26] *Id.* at 672.

name or other payment processing issue.[27] Such claims are typically unsuccessful,[28] and financial institutions have implemented better procedures to detect fraudulently transferred funds before they reach the threat actor (focusing on factors such as an unusually large transfer amount, the lack of past dealings, etc.). While many cyber insurance policies for data security and data breach incidents will cover a business's loss suffered from a BEC, sometimes, there are disputes over whether a particular policy covers the specific incident. These disputes tend to be very fact-intensive depending on the policy language, and require consulting with counsel on the applicability of such policies.[29]

In summation, while this area of the law is far from settled, Texas courts seem to follow the majority view and assign liability based on an allocation of fault, largely turning on the victim's diligence to prevent the fraud. This highlights the importance of establishing preventive company-wide procedures, including frequent training on detecting fraud and updating policies on payments disbursements, to avoid financial losses in the first instance. In the event of an unfortunate incident, prompt reporting, including consulting with counsel when working with authorities, financial institutions, and other agencies, is critical and could make the difference between recovering the funds and being on the wrong side of the law.

---

[27] *See, e.g., Meta Sols. v. First State Bank of Brownsboro*, No. 6:19-CV-329-JDK, 2020 WL 12991132 (slip copy), at *1 (E.D. Tex. Apr. 16, 2020). While financial institutions don't always catch bad actors before the money leaves the institution, they are getting better and better at detecting fraudulently transferred funds and preventing them from being transferred to crypto-wallets.

[28] *See id.*

[29] *See, e.g., Apache Corp. v. Great Am. Ins. Co.*, 662 F. App'x 252, 254–59 (5th Cir. 2016) (discussing the fact intensive inquiry into the fraud itself and the insurance policy that determine the outcome of such a case).