Beware Compromised Business Email . . . And The Litigation That Follows

Bill Butler, Jim McLoughlin and Chris Tomlinson
MVA COVID-19 Resource Center
04.2020

Businesses are facing this system hack with ever-increasing frequency: An accounts payable employee receives new or updated payment instructions from a vendor via email. The email appears to be from a familiar counterpart at the vendor; it contains accurate details specific to a current transaction; the new bank is well known; and the new instructions have the vendor's name, or a version of it, as the beneficiary. The accounts payable employee executes the electronic transfer payment consistent with the wiring instructions. In an instant, the payment goes not to the vendor, but into the account of a cyber-criminal posing as the vendor, with almost no chance of recovery because the funds leave the criminal's bank account immediately.

The COVID-19 pandemic has seen this social engineering fraud, often referred to as "business email compromise," become even more prevalent. As businesses have rushed to mobilize at-home workforces in response to shelter-in-place measures—for many this an entirely unfamiliar experience—the new procedures, makeshift security measures, and decentralized oversight have left their business more vulnerable to cyber-criminals. The FBI has warned of the rise in business email compromise schemes related to the COVID-19 pandemic. Healthcare providers and other businesses scrambling to purchase personal protective equipment are favorite targets.

When a business is the victim of these schemes, the legal system may offer little help. Although there is ample guidance on how to avoid business email compromise schemes (the most effective method is to verify wiring instructions through a telephone call to a known contact at the recipient and an oral request for a confirming email from that contact), there is much less guidance on how to allocate the loss between the payor and the bona fide vendor, particularly with the vendor who did not receive its payment having little interest in accepting a loss. There are still relatively few cases addressing this situation, but it is important to understand the principles that likely will be applied by the courts to determine who bears the loss from the misdirected payment.

Faced with this 21st century problem, the courts have looked to 20th century principles, including the Uniform Commercial Code's Article 3 (Negotiable Instruments)[1] and Article 2 (Sales)[2]. For example, the courts have treated an electronic transfer as the equivalent of a negotiable instrument such as a check, looking to § 3-404 (Imposters; Fictitious Payees), § 3-403 (Unauthorized Signature), and § 3-406 (Negligence Contributing to Forged Signature or Alteration of Instrument) for guidance. Courts have looked also to basic contract principles and the law of agency (agency by estoppel) to allocate losses. Cases have allocated 100% to one party or allocated based upon comparative fault.[3]

Laws expected to apply in the wake of business email compromise may not. Financial data protection and data security statutes require companies to protect customers' personal data, but hacked email accounts that facilitate payment fraud may not implicate customer data, so may not apply.[4] Tort law, including claims for negligent maintenance of email servers, may not apply because the business that is hacked owes "no general duty to avoid the unintentional infliction of economic loss" on another.[5] Instead, the following principles likely will determine the outcome of a business email compromise dispute:

- The presumption is that party who was in the best position to prevent the fraud should bear the responsibility.[6] Courts have also asked which party had the "last clear chance" to prevent the loss.
- Whether each party exercised "ordinary care" given the circumstances is a critical factor. Whether a party ignored red flags strongly influences case outcomes. Red flags may include odd syntax or wording in the fraudulent email, a request by an unknown or unexpected individual, a request that is out of context for the transaction, or failure of a transfer to a new bank. It also is relevant whether a party followed its own protocols for certifying transfers.
- The fact that a party's email system was compromised is relevant to, but not dispositive of the responsibility determination. The duty to ensure that one's email system is not hacked is not a duty commercial parties owe to one another, and the courts recognize that sophisticated hackers are sometimes successful despite ordinary care.[7] However, if a party's email system was compromised because it did not have in place or follow reasonable security measures, it likely will be found not to have exercised ordinary care.
- Once a party has notice from an odd email or other anomaly that a hacker may be targeting a transaction, it likely has a duty to investigate and to warn all counterparties to any prospective transfers.[8]
- Courts may be reluctant to create duties by analogy where no legal doctrine clearly applies, leaving the party whose payment was misdirected with the loss.[9]
- Which party was in the best position to prevent the fraud is heavily dependent upon the facts of each case, meaning a "quick" resolution before trial is unlikely. Because the determination is fact-specific, and the facts are often disputed, courts are reluctant to allocate the loss before trial.

There is no bright-line rule for determining responsibility in business email compromise disputes. It is important to analyze the specific facts surrounding the business email compromise scheme, including red flags missed or systems failures by all parties involved, when litigating a business email compromise dispute or attempting to negotiate a resolution.

Cybersecurity firms are reporting significant increases in all manner of cyberattack and social engineering involving COVID-19, including business email compromise, credential phishing, malware, and spam email campaigns.

When assistance concerning business email compromise is needed, Moore & Van Allen's Litigation and Privacy and Data Security practice groups have extensive experience assisting clients in responding to business email compromise and other cybersecurity threats, minimizing their harm, and, if necessary, litigating the resulting disputes.

[1] *Bile v. RREMC, LLC.*, 2016 U.S. Dist. LEXIS 113874 (E.D. Va. August 24, 2016) (U.C.C. Article 3 supplemented by Restatement (Second) of Contracts); *Arrow Truck Sales, Inc. v. Top Quality Truck & Equip., Inc.*, 2015 U.S. Dist. LEXIS 108823, 2015 WL 4936272 (M.D. Fla. August 18, 2015).

[2] *Russell Barnett Ford of Tullahoma, Inc. v. H&S Bakery, Inc.*, 398 F. Supp. 3d 287, 2019 U.S. Dist. LEXIS 129197, 99 U.C.C. Rep. Serv. 2d 895, 2019 WL 3535906 (E.D. Tenn. August 2, 2019) (U.C.C. Article 2 displaces common law tort remedy).

[3] *Beau Townsend Ford Lincoln, Inc. v. Don Hinds Ford, Inc.*, 759 Fed. Appx. 348, 2018 U.S. App. LEXIS 33225, 2018 WL 6181643 (6th Cir. November 27, 2018) (discussing U.C.C. Article 3, the Restatement of Agency (agency by estoppel), and the Restatement (Second) Contracts).

[4] *Prime Foods for Processing & Trading v. Greater Omaha Packing Co.*, 2019 U.S. Dist. LEXIS 93169, 2019 WL 2358445 (D. Neb. June 4, 2019).

[5] *Prime Foods for Processing & Trading*, 2019 U.S. Dist. LEXIS 93169, 2019 WL 2358445 (citing Restatement (Third) of Torts: Liability for Economic Harm § 1 (Tent. Draft No. 1, Apr. 4, 2012).

[6] *Beau Townsend Ford Lincoln, Inc.*, 759 Fed. Appx. 348, 2018 U.S. App. LEXIS 33225, 2018 WL 6181643; *Arrow Truck Sales, Inc.*, 2015 U.S. Dist. LEXIS 108823; 2015 WL 4936272.

[7] *Compare*, *Deutsche Bank Nat'l Trust Co. v. Buck*, 2019 U.S. Dist. LEXIS 54774, 2109 WL 1440280 (E.D. Va. March 29, 2019) (no general common law duty to protect an individual's private information from an electronic data breach) and *2 Hail, Inc. v. Beaver Builders, LLC*, 2017 Colo. Dist. LEXIS 1294 (D. Colo. November 29, 2017) (rejecting court's analysis in *Bile* and finding no legal theory applicable to allocate responsibility based on relative fault and imposing liability on the party's whose payment was misdirected).

[8] *Bile*, 2016 U.S. Dist. LEXIS 113874.

[9] *2 Hail, Inc.*, 2017 Colo. Dist. LEXIS 1294.