WINTER 2023 E-NEWSLETTER

At Digital Mountain, we assist our clients with their electronic discovery, digital forensics, cybersecurity, and data analytics needs. For this E-Newsletter, we discuss Business Email Compromise and financial loss in litigation settlements, relevant court cases, and best practices for prevention.

Whose Fault is Business Email Compromise?

Business Email Compromise (BEC) is a crime, no doubt about it. While law enforcement can pursue cybercriminals and attempt to prosecute under criminal statutes, frequently, they cannot recoup BEC losses that legitimate businesses suffer when transactions are hijacked. In cases where funds were transferred via fraudulent wiring instructions to scammers' accounts, the courts have fairly consistently taken a position that highlights the need to prioritize email security. In this article, we'll look at some of the cases that have set precedents on the civil side of BEC lawsuits.

In *Parmer v. UNITED BANK, INC.*, No. 20-0013. (W VA: Supreme Court of Appeals, 2020), the plaintiff's counsel, as part of a legal settlement, wired approximately $212,500 according to instructions provided by the defendant's counsel. What would not be known until weeks later was that the instructions sent to the plaintiff's counsel were the product of a BEC scam and resulted in the funds being wired to a bank account unassociated with either party. The plaintiff claimed that the defendant was in the best position to know that they had been the victim of a BEC scam and that she should not have to pay the money a second time. The court disagreed, stating that because the plaintiff's counsel had previously wired funds to the defendant, they should have recognized the irregularity in the instructions and consulted with the defendant's counsel prior to executing the transfer. In its Memorandum and Decision, the court wrote, "In reality, had Ms. Parmer or her counsel exercised reasonable care and verified the wire transfer instructions her counsel received, the loss could have been averted."

And what about insurance coverage? Whether an organization invests in a commercial crime insurance policy or a cyber insurance policy, determining beforehand exactly what the policy covers in the event of a BEC scam is very important. The Fifth Circuit Court of Appeals upheld a lower court decision in *Realpage, Inc. v. National Union Fire Insurance Co. of Pittsburgh* (No. 21-10299, 5th Cir., 2021), where the plaintiff sued their insurance carrier for losses of rents and fees after a BEC attack. The plaintiff's employee clicked on a link embedded in a phishing email and

subsequently entered login credentials for the company's Stripe payment accounts. Not surprisingly, the scammers drained Realpage, Inc.'s account and their customer's account. Realpage, Inc. filed for an insurance reimbursement under their commercial crimes policy and ultimately sued when their claim was denied. Both courts sided with the defendant on the grounds that RealPage never actually "held" the funds stolen from the customers' Stripe accounts, and therefore, they didn't own those funds. No ownership, no loss. The courts did not see, as Realpage, Inc. argued, that the terms "held" and "controlled" were analogous to "owned." The important lesson from cases like this (and there are others) is that knowing what commercial crime policies will cover when it comes to BEC is vital.

Finally, in *Dentons Canada LLP v. Trisura Guarantee Insurance Company* (2018 ONSC 7311), an associate of the Canadian law firm wired more than $2 million from a client trust account in accordance with emailed wire transfer instructions. Unfortunately, even though the associate attempted to confirm the transfer instructions, the transfer was executed before a positive response was received by Dentons. While Dentons was able to act rapidly following the discovery of the fraudulent wiring instructions, they were only able to recover slightly less than $785,000, and filed an insurance claim for the remaining lost funds. Trisura, the insurance company, denied Dentons' claim stating that the Computer Fraud Policy didn't cover the loss because the transfer wasn't fraudulently executed. The scammer emailed fraudulent instructions, but Dentons ultimately chose not to wait for confirmation of the instructions and authorized the transfer. The case was referred for trial and should set a precedent for Canadian courts with regard to BEC and wire fraud.

Business Email Compromise isn't going away, nor will it become solely the jurisdiction of the criminal courts. We are going to continue to see cases that require the courts to determine the liability for the security of email systems used to communicate among businesses and individuals, especially those facilitating financial transactions. Our takeaway from these cases is that by taking appropriate steps and working with professional cybersecurity experts, organizations can not only help prevent BEC but also help establish themselves as careful, responsible, and proactive. While we hope you'll never become a BEC victim, if you do, Digital Mountain is here to assist with professional services, including incident response and expert testimony.

Please direct questions and inquiries about electronic discovery, digital forensics, cybersecurity, and data analytics to info@digitalmountain.com.

UPCOMING INDUSTRY EVENTS

UF LAW's 10TH ANNUAL E-DISCOVERY CONFERENCE
Gainesville, FL: February 8-9, 2023

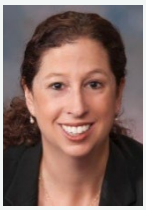
SOLID WEST 2023
San Francisco, CA: February 15, 2023

NETDILIGENCE CYBER RISK SUMMIT 2023
Ft. Lauderdale, FL: February 20-21, 2023

MASTER'S CONFERENCE FEBRUARY 2023
San Francisco, CA: February 22, 2023

ABA TECHSHOW 2023
Chicago, IL: March 1-4, 2023

Click here to see more upcoming events and links.



Digital Mountain, Inc. Founder and CEO, Julie Lewis, will be presenting at various upcoming industry events. Please send requests for speaker or panel participation for her to marketing@digitalmountain.com.

DIGITAL MOUNTAIN, INC.
4633 Old Ironsides Drive, Suite 401
Santa Clara, CA 95054
866.DIG.DOCS

www.digitalmountain.com

Contact us today!

FOLLOW US AT: