ENEMY IN THE WIRE

Law firm cybersecurity and wire transfer fraud.

WRITTEN BY **JOHN G. BROWNING**

It's a nightmarish scenario that has become all too real for an increasing number of law firms nationwide: Someone purporting to be a client—and referencing an actual transaction like a sale of property or the funding of a settlement—sends an email directing the law firm to wire money to an account in consummation of the deal or settlement. But as it turns out, the firm has been scammed, leading to awkward conversations with the actual client, potential legal action involving the bank, and the uncertain prospect of claims to the law firm's insurance carrier.

All too many businesses have found themselves victimized in this or similar ways by such business email compromise, or BEC. The FBI estimates that in the U.S. during 2019 alone, it received 23,775 BEC complaints, with adjusted losses of over $1.7 billion.[1] Additionally, the FBI has found that losses from such scams have increased each year since the agency began tracking them in 2013. With the COVID-19 pandemic and law firms, like other businesses, embracing work from home policies, the potential for such BEC fraud has increased as bad actors exploit the challenges and changes brought on by remote working.[2]

It's a subject that law firms cannot afford to ignore from either an ethical perspective or a practical one. American Bar Association Formal Opinion 477 requires lawyers to adopt "reasonable" cybersecurity measures to protect client data and property. For Texas lawyers, cybersecurity is also a matter of professional competence. In Opinion 680, the Professional Ethics Committee reminded lawyers that they

> should remain continually alert to the vulnerability of cloud-based vendors and systems to data breaches … Data "hacking" by third parties is becoming increasingly well-known and can even occur with respect to client confidential information stored on a server within a law firm. Therefore, a lawyer should remain reasonably aware of changes in technology and the associated risks.[3]

Beyond being mindful of their ethical duties that impact cybersecurity, lawyers must also be aware of the headlines, as law firm after law firm makes the news for falling prey to wire transfer schemes. In a lawsuit filed this summer against Holland & Knight, plaintiffs Sorenson Impact Foundation and the James Lee Sorenson Family Foundation allege that the law firm was hired to oversee a $3 million stock sale. Somehow, according to the lawsuit, scammers intercepted emails between the firm and its foundation clients, then assumed the plaintiffs' identity and asked that the firm wire transfer the funds to a Hong Kong-based account rather than the original account.[4] The plaintiffs allege that Holland & Knight did not call to verify the account change or secure a guarantee from a financial institution (known as a medallion guarantee), as required in the merger agreement between Holland & Knight and the parties involved. Because of this, the plaintiffs' suit alleges breach of contract against the firm, along with negligence and breach of fiduciary duty. Holland & Knight maintains that its "information technology system was not compromised in any way" and that it "acted on wiring instructions received from the plaintiffs' email system by providing the instructions to the paying agent."[5]

While it remains to be seen whether Holland & Knight can escape liability, other firms in similar situations have not fared well. In a 2017 case involving the Vancouver, Canada, office of international law firm Dentons, an associate of the firm was duped into transferring $2.5 million (intended to pay off the mortgage on a client's property) into a scammer's Hong Kong account.[6] The law firm, through a "social engineering" fraud, had received emails purportedly from its client requesting that the firm wire the funds to an international account because its TD Canada Trust account was being audited. Although Dentons received no answer to its telephonic attempts to communicate with its client, it did request and receive signed authorization letters purporting to be from the client and a third-party account.[7] When Dentons ultimately received an email from its actual client days later inquiring about the status of the funds, it realized that the funds had been misrouted. Although the firm managed to recover $784,739.39, it notified its insurance carrier of the net loss of over $1.7 million. The insurer denied coverage (noting

that Dentons had turned down the opportunity to add a social engineering fraud rider), and a lawsuit began. In a December 2018 opinion, a Canadian court determined that further proceedings were necessary.[8]

In 2015, prominent Boston law firm Sarrouf Law fell victim to a similar scam, losing $311,500 after receiving an email from an overseas company that later sent a counterfeit check. The firm deposited the check into its trust account before instructing its bank to disburse the funds by wire transfer to banks in Hong Kong and Cambodia. When it sought to recover the funds from its bank, the firm lost at both the trial court level and the appellate level.[9] In 2017, Pennsylvania law firm O'Neill, Bragg & Staffin was scammed out of $580,000 when a hacker posing as named shareholder Gary Bragg directed fellow shareholder Alvin Staffin to send a wire for $580,000 on behalf of a firm client to a Bank of China investment account in Hong Kong.[10] When Staffin later called Bragg (who was traveling in Seattle at the time), he realized that the firm had been victimized and contacted Bank of America in an attempt to stop the transfer. The bank was unable to do so and was later sued by the firm. A federal court dismissed the suit, finding that Bank of America had not breached any agreement or violated any state or federal laws in wiring the money. Similar wire transfer frauds have befallen firms all over the country that have been scammed into wiring settlement funds to a criminal actor's account; this includes firms in Florida, West Virginia, and Virginia.[11]

But if you are scammed and cannot recover from the bank making the wire transfer, at least you can recover from your insurance carrier, right? Well, the answer is a lawyerly "it depends." Not only may it depend on the wording of your policy, and whether you have a policy that covers such cybersecurity risks, but it also depends on your jurisdiction. In recent years, courts throughout the country have grappled with the issue of a policyholder's claims for insurance coverage stemming from "social engineering" losses—losses resulting from a criminal actor tricking the insured into wiring funds to the criminal's bank account. The results have been mixed. The U.S. Courts of Appeals for the 9th Circuit and 11th Circuit, for example, have ruled that computer fraud policies do not provide coverage in situations where an employee of the company, who was authorized to access its computer systems, acts to transfer funds to a criminal actor—even where the employee was tricked into doing so.[12] The U.S. Courts of Appeals for the 2nd Circuit and 6th Circuit, on the other hand, have reached the opposite result, holding that a policyholder *is* entitled to coverage after an employee wires funds to a criminal's account after receiving a spoofing email from the criminal (in the guise of a company executive or a known vendor).[13]

How has the U.S. Court of Appeals for the 5th Circuit ruled? Like its sister courts on the 9th and 11th Circuits, the 5th Circuit has held that mere trickery of an employee isn't enough to create coverage; there has to be fraud committed through the unauthorized use of the computer system, such as where hackers have made changes in the insured's system or embedded software that caused fraud.[14]

Knowing the dim prospects for recovery against either its bank or its insurance carrier in the event of falling prey to such wire transfer scams, what can a Texas law firm do to protect itself? First, review your cybersecurity or cyberliability policy and look at what it covers. If necessary, inquire about the availability of "fraudulent instruction coverage" that would apply in a situation of a firm employee with access and authorization being tricked into a fraudulent wire transfer. Second, educate yourself and your law firm staff about verifying information. This includes looking up the actual phone number of the company associated with the incoming email instead of relying on the information provided and contacting the company directly; verifying payment requests in person if possible or by calling the client or company directly; verifying any change in account number or payment procedure; and carefully examining the email address, URL, spelling, and syntax used, while being particularly wary if the person making the request is pressing for quick action. Vigilance and education are your best weapons. **TBJ**

NOTES

1. Fed. Bureau Investigation, Internet Crime Complaint Ctr., *2019 Internet Crime Report,* https://pdf.ic3.gov/2019_IC3Report.pdf.
2. Paul Hodkinson, *Remote Work Has Law Firm Cybersecurity in a Fragile State,* Am. Law. (Sept. 1, 2020, 1:00 AM), https://www.law.com/americanlawyer/2020/09/01/remote-work-has-law-firm-cybersecurity-in-a-fragile-state/?slreturn=20200813185526.
3. Tex. Comm. On Prof'l Ethics, Op. 680 (2018), 81 Tex. B.J. 798 (2018).
4. Dylan Jackson, *Law Firms Remain Vulnerable to Wire Transfer Scams, as Liability and Breach Costs Grow,* Am. Law. (July 28, 2020, 2:08 PM), https://www.law.com/americanlawyer/2020/07/28/law-firms-remain-vulnerable-to-wire-transfer-scams-as-liability-and-breach-costs-grow/?slreturn=20200813185831.
5. *Id.*
6. Michael McKiernan, *Firm in $1.7 million dispute with insurer,* L. Times (Jan. 21, 2019), https://www.lawtimesnews.com/news/general/firm-in-1.7-million-dispute-with-insurer/263383#:~:text=Global%20law%20firm%20Dentons%20Canada,victim%20to%20an%20alleged%20scam.
7. *Dentons Canada LLP v. Trisura Guarantee Ins. Co.,* 2018 ONSC 7311 (Sup. Ct. Justice–Ontario Dec. 11, 2018).
8. *Id.*
9. *Sarrouf Law LLP v. First Republic Bank,* No. 19-P-31 (Mass. App. Ct., Nov. 13, 2019).
10. *O'Neill, Bragg & Staffin, P.C. v. Bank of Am. Corp.,* Civ. Action No. 18-2109 (E.D. Pa. Nov. 13, 2018).
11. *See, e.g.,* Christopher O'Donnell, *Scammer tricked top Tampa law firm into wiring money to wrong account lawsuit says,* Tampa Bay Times (Feb. 29, 2020), https://www.tampabay.com/news/tampa/2020/02/29/top-tampa-law-firm-claims-scammer-stole-settlement-money/; Sharon D. Nelson, Esq., *Law Firm Wire Fraud: Your Money is Gone – Will Your Insurer Cover Your Loss?,* Ride the Lightning (Aug. 6, 2019), https://ridethelightning.senseient.com/2019/08/law-firm-wire-fraud-your-money-is-gone-will-your-insurer-cover-your-loss.html.
12. *See, e.g., Pestmaster Servs., Inc. v. Travelers Cas. & Sur. Co. of Am.,* 656 Fed. App'x 332 (9th Cir. 2016); *Interactive Communications, Int'l, Inc. v. Great Am. Ins. Co.,* 2018 WL 2149769 (11th Cir. 2018).
13. *See, e.g., Medidata Solutions, Inc. v. Fed. Ins. Co.,* No. 17-2492-cv (2d Cir. July 6, 2018); *Am. Tooling Ctr., Inc. v. Travelers Cas. & Sur. Co. of Am.,* No. 17-2014 (6th Cir. July 13, 2018).
14. *Apache Corp. v. Great Am. Ins. Co.,* 662 Fed. App'x 252 (5th Cir. 2016).

JOHN G. BROWNING
serves on the 5th Court of Appeals in Dallas. He is the immediate past chair of the State Bar of Texas Computer & Technology Section. The author of four books and numerous articles on social media and the law, Browning is a nationally recognized thought leader in technology and the law.