KENTUCKY BAR ASSOCIATION

B&B

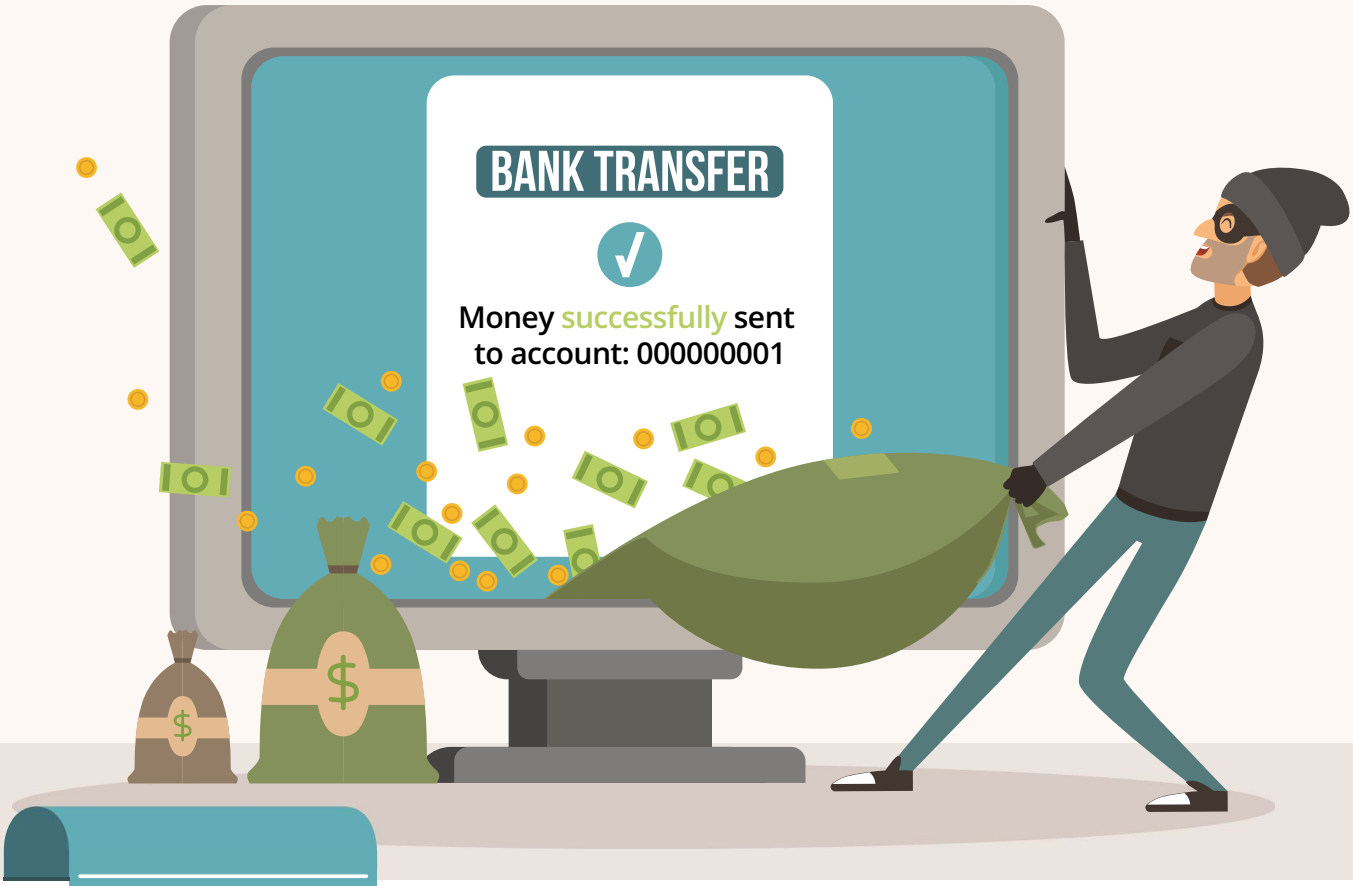
BENCH & BAR MAGAZINE MARCH/APRIL 2019

Passion with Respect

2019 KBA Annual Convention

6.12-14.2019
Galt House Hotel
Louisville

TURN TO PAGE 5 FOR
2019 KBA Annual Convention Details



Lessons from *O'Neill v. Bank of America*

Hacked Law Firms Left Holding the Bag

BY: ADAM C. REEVES

As a law firm, getting hacked is bad enough. But one Pennsylvania law firm learned an even harder lesson when it sued Bank of America to recover client funds stolen by hackers.[1] In *O'Neill v. Bank of America*, a federal judge dismissed a law firm's claim that its bank bore ultimate responsibility after one of the firm's shareholders unwittingly transferred $580,000 from the firm's IOLTA account to computer hackers in Hong Kong. While the hackers were, "of course . . . the real culprit[s]," the court announced that "as between the law firm and the bank, the law firm must bear the loss."[2] The law firm's hacking and the court's decision in *O'Neill* present important lessons for Kentucky practitioners about cybersecurity.

But first, how could a lawyer wire $580,000 of his clients' funds to computer hackers? In 2017, computer hackers gained access to the e-mail account of Gary Bragg, a shareholder of the law firm O'Neill, Bragg & Staffin, P.C.[3] Using Bragg's account, the hackers e-mailed Bragg's partner, Alvin Staffin, and asked him to wire $580,000 from the firm's IOLTA account held at Bank of America to a bank in Hong Kong.[4] Posing as Bragg, the hackers claimed a client needed to quickly transfer its money to close a loan transaction, but that Bragg would be out of the office and unable to authorize the transfer himself.[5] Staffin, then, instructed Bank of America to transfer the money.[6] By the time Staffin and Bragg discovered the ruse, it was too late. Staffin asked Bank of America to stop the transfer, but Bank of America refused, stating it could only request that the Hong Kong bank recall the transfer once that bank received the funds.[7] By the time the Hong Kong bank froze the hacker's account, less than $24,000 remained in it.[8]

Bragg, Staffin, and their firm sued Bank of America. They alleged the bank committed breach of contract and negligence, that the bank violated the Pennsylvania Commercial Code by refusing to halt the wire transfer.[9] The court, however, dismissed these claims.[10] It did so largely because Bank of America's deposit agreement prohibited an account-holder from cancelling or amending a wire transfer request after Bank of America received it.[11] Because Staffin had completed the wire transfer request, he "had no legal right to stop payment" of the clients' funds.[12] And because the relationship between Bank of America and Staffin's firm was "purely contractual," the court in *O'Neill* found that Bank of America upheld its "duty of ordinary care" in complying with the deposit agreement.[13]

Pennsylvania's Commercial Code did no more to shift the risk of loss to Bank of America. The court recognized the Pennsylvania Commercial Code's "clear presumption" that cancellation of a wire transfer request is ineffective after the request is accepted by the receiving bank (here, Bank of America).[14] Only if Bank of America had voluntarily agreed to halt the transfer, or if some other "funds-transfer system rule" otherwise allowed the cancellation would Staffin's cancellation request have been effective.[15] While it would certainly lead to "harsh results," the court believed this presumption appropriately alleviated banks of responsibility and risk for wire transfers made "due to a mistake by the sender that could be neither known nor anticipated by the bank."[16]

Even though this case was decided in Pennsylvania, the same result could very well occur in Kentucky. For one, hackers are targeting law firms—and their wealth of sensitive client data—at a growing rate. In 2017, 22 percent of firms surveyed by the American Bar Association reported experiencing a data breach, up from 14 percent in 2016.[17] What's more, the portion of Pennsylvania's Commercial Code that protected Bank of America against the risk of loss in *O'Neill* mirrors Kentucky's own provisions.[18] As such, any Kentucky law firm with a similar deposit agreement risks shouldering the same responsibility should it fall victim to a similar scheme.

The lessons from *O'Neill* should be clear, but are worth repeating. First: computer hacking schemes are not always obvious. After all, it's not like Staffin thought he was sending client funds to the deposed prince of Nigeria.[19] Rather, Staffin responded to an e-mail from his partner's actual e-mail account that concerned an actual client and referenced an actual IOLTA account number.[20] In retrospect, the only red flag was that the hacker's e-mail featured a noticeable number of typos and unusually poor grammar.[21] Staffin's example, then, reminds lawyers to scrutinize odd or suspicious requests, even when they appear to originate from real, known sources.

Second: talk on the phone. Staffin only learned that Bragg had not actually requested the wire transfer after he had called Bragg on the phone.[22] Indeed, Staffin thwarted a second effort by the hackers to secure another, larger wire transfer when he offered a phone call to discuss the request.[23] Deception like this over e-mail only works if the victim never stops to call the sender to confirm the validity of the request. Particularly when dealing with a client's sensitive data or money, lawyers are well advised to confirm transactions like the one in *O'Neill* over the phone or in person.

Third: lawyers should review their IOLTA account deposit agreements. Staffin's lawsuit failed mainly because Bank of America's deposit agreement placed the risk of a mistaken wire transfer request on the firm and not the bank. That same agreement also permitted Bank of America to overdraw the IOLTA account to sufficiently fund the wire transfer.[24] That meant that even though Bragg's client had only deposited $1,900 in his firm's IOLTA account, Bank of America used the funds of clients held in the same account to complete the transfer.[25] Lawyers maintaining IOLTA accounts should carefully review the allocation of risk posed by their bank's deposit agreement.

Finally, *O'Neill* gives lawyers reason to consider obtaining "cyber insurance." Cyber insurance policies may cover liability for costs arising out of privacy breaches and cyber extortion.[26] Indeed, the risk of a data breach or cyber-attack, despite a lawyer's best efforts, may prove the warning by the American Bar Association's Standing Committee on Ethics and Professional Responsibility that firms fall into two categories: "those that have been hacked and those that will be."[27] Kentucky firms should accordingly pause and take note to avoid what befell Bragg and Staffin in *O'Neill*. B&B

ABOUT THE AUTHOR

ADAM C. REEVES is a member at Stoll Keenon Ogden PLLC. Reeves is chair of the firm's appellate practice group, and maintains a business and healthcare litigation practice. Before joining Stoll Keenon Ogden, he worked as an Assistant United States Attorney, and before that, clerked for Judge Eugene E. Siler, Jr., of the United States Court of Appeals for the Sixth Circuit.

ENDNOTES

1. *O'Neill v. Bank of Am. Corp.*, 2018 WL 5921004, 2018 U.S. Dist. LEXIS 193302, at *2-4, (E.D. Pa. Nov. 13, 2018).
2. O'Neill, 2018 U.S. Dist. LEXIS, 193302, at *28-29.
3. *Id.* at *3-4.
4. *Id.* at *3-5. IOLTA accounts – or "Interest on Lawyers Trust Accounts" – are maintained by law firms and used to hold nominal or short-time client funds. *See*, e.g., Kentucky SCR 3.830.
5. *Id.* at *4-5.
6. *Id.* at *5-6.
7. *Id.* at *7.
8. Staffin, Bragg, and their law firm ultimately recovered just $58,730.11 from the hacker's account after engaging Hong Kong counsel to recover the stolen funds. *Id.* at *8-9.
9. *Id.* at *10-28.
10. *Id.*
11. *Id.* at *11.
12. *Id.*
13. *Id.* at *25.
14. *Id.* at *19-20 (citing 13 Pa. Cons. Stat. Ann. § 4A211(c)).
15. *Id.* at *20.
16. *Id.*
17. David G. Ries, 2017 Security, American Bar Association (Dec. 1, 2017), https://www.americanbar.org/groups/law_practice/publications/techreport/2017/security/ (last visited Jan. 16, 2019).
18. Compare 13 Pa. Cons. Stat. Ann. § 4A211(c), with Ky. Rev. Stat. § 355.4A-211(3).
19. The Nigerian Prince: Old Scam, New Twist, Better Business Bureau, https://www.bbb.org/new-york-city/get-consumer-help/articles/the-nigerian-prince-old-scam-new-twist/ (last visited Jan. 16, 2019).
20. O'Neill, 2018 U.S. Dist. LEXIS 193302, at *3-5.
21. *Id.* at *4-5.
22. *Id.* at *6.
23. *Id.* at *8.
24. *Id.* at *11-13.
25. *Id.*
26. Jeffrey A. Franklin, Cyber Insurance for Law Firms, American Bar Association (June 29, 2017), https://www.americanbar.org/groups/gpsolo/publications/gp_solo/2016/may-june/cyber_insurance_law_firms/ (last visited Jan. 16, 2019).
27. Formal Opinion 482: Lawyers' Obligations After an Electronic Data Breach or Cyberattack, American Bar Association's Standing Committee on Ethics and Professional Responsibility (Oct. 17, 2018), https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_op_483.pdf (last visited Jan. 16, 2019).