Corsican Controversy — Be Wary of Wire Transfers

by E. Duffy Myrtetus

An old friend from Miami now lives with his family in London, a renown international travel hub. They have made the most of their travel opportunities living there. Over the years, I have had to hear stories about trips they've made to a wide range of exotic destinations in Europe, the Mediterranean, Southeast Asia, etc. About eight years ago, he told me about a trip his family planned to Corsica. At the time, I knew little about Corsica but was intrigued.[1]

He researched and found a reputable, legitimate well known international travel agency with offices in Spain that handled rentals in Corsica. A beautiful villa was located to serve as a home base for a week-long trip traveling the island. Consistent with these types of transactions, half of the week's rental was due up front via wire transfer with the initial rental paperwork, passport information, etc. — the balance of the rental was due two weeks before arrival. He placed the initial wire, sent the paperwork, and called to confirm receipt. A confirmation email was sent from the travel agency acknowledging receipt. Two weeks before departure, he received an email from the travel agency confirming the details of his rental and providing directions for the wire transfer of the final balance owed. He placed the final wire transfer and excitedly tackled final planning details for the trip.

Their flight arrived in Corsica, they rented a car and drove to the villa. When they arrived, the front door was locked; so, they called the rental agency who sent local representatives out to the property. "*Quale* si?" (Who are you?) the locals inquired in the local Corsu language. "*The renters for this week,*" was the friend's response. "*No. The house is not rented this week,*" was the reply; and, thus, began negotiations of a major U.S.-Corsican international incident that culminated in a final (but expensive) solution for access to the villa.

Turns out the rental agency's email system had been hacked. The hacker obtained the details of my friend's rental transaction, including his email and the balance owed. It then provided fraudulent wire transfer instructions to my friend, which were later used for the transfer of the rental balance owed. That wire transfer never reached the rental agency, and the owner assumed there was no rental. The renters did not learn about the fraud until they were locked out at arrival on the front door threshold of their rental villa. By the time the renters figured out what had happened, the wired funds had long been transferred out of legally trackable recipients.

This was my first personal exposure to wire transfer risk — and it was eight years ago! In the interim, fraudulent and criminal activity relating to wire transfers has exploded in the U.S. and internationally. The FBI's Internet Crime Report for 2021 includes these staggering statistics: 1) $6.9 billion victim losses in 2021; 2) 2,300+ average complaints received daily; and 3) 552,000+ average complaints received per year (last five years).[2]

Wire fraud is an evolving form of fraudulent action or enterprises that involves the use of, among other things, electronic communications, and/or the internet. It can in various forms include the use of phone communications, faxes, emails, text messaging, social media communications and other online platforms. It is difficult to quantify the varied ways in which criminal actors explore a victim's systemic vulnerabilities, and then capitalize upon them in furtherance of fraudulent activity. As in the Corsican controversy above, hackers often penetrate systems and acquire data — or monitor communications or transac-

tions — for periods of time (days, weeks, months, or years) in order to assess the most efficient means to steal money or information before taking action.

Real estate transactions are viewed as a target rich environment for fraudulent activity. The Florida Bar's Practice Resource Center continues to receive reports of fraudulent activity targeting attorney trust accounts. The three most prevalent types of fraud are: 1) counterfeit bank checks; 2) compromised wire instructions; and 3) forged trust account checks. You can find a summary of each of the foregoing types of fraud at LegalFuel: The Florida Bar's Practice Resource Center website.[3]

Hacked emails are one of the major sources of fraudulent activity. In real estate transactions, attorneys and title agents are increasingly reporting that their email communications have been compromised and that third-party hackers are using illegally acquired data and information from emails to communicate fraudulent wiring instructions or other information to buyers, settlement agents, and others. Often, the emails or other communications appear to be legitimate. Consequently, when followed they result in lost funds that cannot be recovered. Unlike checks, wire transfers typically cannot be recovered once sent.

Many law firms and lay closing or settlement agents have begun using "old school" or law-tech practices to mitigate the risk of wire fraud. On the extreme end of that scale, some firms and agents require hardcopy/paper wire instructions that are signed and notarized by the issuing party. Few require an indemnity from the party providing the instructions. Others, require encrypted or secure emails only for receipt of wire instructions for use in a transaction; and, almost universally all make independent telephone calls (or take other steps to validate and verify) such instructions before utilizing them at a closing.

Increasingly, instructions like the following appear in pre-closing instructions, or in connection with requirements from closing agents in connection with wire transfers:

I. WIRE FRAUD ALERT. If you receive an e-mail from this office requesting that you wire or otherwise transfer funds, you must confirm the request and any corresponding instructions by telephone with this office before you initiate any transfer. Email accounts of attorneys, other professionals and businesses are being targeted by hackers in an attempt to initiate fraudulent wire requests.

II. WARNING! WIRE FRAUD ADVISORY: Wire fraud and email hacking/phishing attacks are on the increase! If you have an escrow or closing transaction with us and you receive an email containing Wire Transfer Instructions, DO NOT RESPOND TO THE EMAIL! Instead, call your escrow officer/closer immediately, using previously known contact information and NOT information provided in the email, to verify the information prior to sending funds.

III. Wire Transfer — Security (sent via encrypted e-mail or letter):

Attached please find wire transfer instructions for the transfer of funds to the [closing agent]. Since wire instructions are provided, we are required to send this message via secure e-mail. Please confirm receipt by responding with an acknowledgement that you received and accessed these instructions.

When you place the wire, your bank will issue a wire confirmation number. Please provide the wire confirmation number to my attention immediately when the transfer is placed, so that we can track it on our end for receipt and credit.

Given the prevalence of wire transfer fraud, under no circumstances should you accept any changes or request for changes to the wire transfer instructions I provide, or any directions to alter or change such wire transfer instructions or recipient, from any person or entity other than me directly.

The American Land Title Association (ALTA) provides a number of incredibly helpful resources for use in preparing for, verifying and using wire transfer instructions in real estate transactions.[4] The materials include proposed checklists and suggested practices. In addition to outgoing wire transfer checklists, these ALTA materials also include suggested practices for a "Rapid Response Plan for Wire Fraud Incidents," available in Excel or .PDF formats.[5]

There are some additional suggested practices from The Florida Bar's LegalFuel[6] for protocols that might help mitigate or avoid risk for fraud from hackers. They require attorneys and law firms to engage and constantly emphasize these points to their attorneys and staff: 1) Immediately delete unsolicited email (spam) from unknown parties; 2) Do NOT open spam email, click on links in the email, or open attachments, which often contain malware that will give subjects access to your computer system; 3) Use strong passwords and frequently change passwords on all devices; 4) Never click on a link, open an attachment, or reply to a suspicious email; 5) Check your online bank account daily and change your banking passwords often; 6) When out of the office, avoid free WiFi to protect against hackers capturing a password; 7) Never send wire transfers or any sensitive information by email, unless it is encrypted; and 8) Install all the updates for your virus protection software and anti-spyware.

While these forms of fraud affect all types of businesses and professions, attorneys have a number of unique duties,[7] among other things, to protect client information as well as client funds. Arguably, the risk for the legal profession is greater than others. Cybersecurity insurance and software tools may help, but diligence in the office and with staff is likely one of the best defenses.[8]❑

[1] Corsica is the birthplace of Napoleon Bonaparte, who "was the second of eight children born to Carlo Buonaparte, a lawyer descended from Tuscan nobility." National Gallery of Victoria "Melbourne Winter Masterpieces"; see National Gallery of Victoria, Who Was Napoleon?, https://www.ngv.vic.gov.au/napoleon/napoleon-and-josephine/who-was-napoleon.html.

[2] *See* Federal Bureau of Investigation, *Internet Crime Report 2021* (2021), *available at* https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf.

[3] LegalFuel, Florida Bar Practice Resource Center, *Frauds Targeting Attorney Trust Accounts* (Mar. 5, 2020), https://www.legalfuel.com/frauds-targeting-attorney-trust-accounts/.

[4] American Land Title Association, *Protect Your Money*, https://www.alta.org/business-tools/wirefraud.cfm.

[5] *See id*.

[6] LegalFuel, Florida Bar Practice Resource Center, *Hacked Emails Can Lead to Wire Transfer Fraud* (Nov. 7, 2016), https://www.legalfuel.com/hacked-emails-can-lead-to-wire-transfer-fraud/.

[7] *See* LegalFuel, Florida Bar Practice Resource Center, *Ethical Obligations — What Must Lawyers Do to Maintain Privileged Information and Comply with Applicable Regulations* (Feb. 4, 2022), https://www.legalfuel.com/ethical-obligations-what-must-lawyers-do-to-maintain-privileged-information-and-comply-with-applicable-regulations/.

[8] Other resources, besides LegalFuel and the American Land Title Association, include: U.S. Federal Trade Commission, https://consumer.ftc.gov/articles/you-wire-money; Wells Fargo, The Ins and Outs of wire Transfers, https://www.wellsfargo.com/financial-education/basic-finances/manage-money/payments/ins-outs-transfers/.

AUTHOR

E. DUFFY MYRTETUS *is a member of Eckert Seamans in its Richmond, Virginia, office, where he maintains a general practice in Florida and Virginia, focused upon transactional and commercial litigation matters related to real estate and mortgage financing, and commercial litigation. He is a member of The Florida Bar's Board of Governors and its Technology Committee.*