Wire Fraud Schemes and Resulting Liability
By Mariana D. Bravo and Katherine C. Ondeck

"The money is not there!" These are words no real estate seller, purchaser, agent, broker, or title company ever wants to hear after a wire transfer. But as wire fraud schemes become more prevalent, these words are becoming a recurring nightmare throughout the real estate industry, and the legal aftermath of these schemes may implicate everyone involved in the transaction.
Picture this: Bob agrees to purchase a piece of real estate from Tom. XYZ Escrow is the escrow agent. Bob and Tom sign the contract, Bob deposits the purchase funds with XYZ, and all that's left to be done is for XYZ to wire the funds to Tom. Seems simple enough, but then things go terribly wrong. .,

The night before closing, XYZ receives an email from Tom's agent, Mary. Correction, it receives an email from someone claiming to be Mary. In actuality, it is really an email from someone who had hacked into Mary's email account and obtained just enough information to impersonate Mary. In the email, "Mary" explains that, because Tom is having problems with his bank account at Wells Fargo, the funds should be wired to an account at Bank of America. At first glance, nothing seems particularly unusual in terms of the email address or contents of the email. Consequently, XYZ honors the change in instructions and wires $500,000 to Bank of America.

A few days later, XYZ receives a call from the real Mary, who wants to confirm that the funds were wired. XYZ tells her that the wire went through a few days ago, and Mary says that she will check with Tom and the bank.

XYZ then gets the dreaded call back from Mary, who informs it: "The money is not there!" Bewildered by this news, XYZ goes back to its email from "Mary" containing the alternate wire instructions. Upon closer review, it discovers that, instead of the real Mary's email address, marytheagent@gmail.com, the email was actually from marytheagent@mail.com (notice the missing "g"). Although XYZ immediately calls the bank to try and freeze the wire, it is too late. The money is gone.

Who is liable for Tom's misfortune? What legal recourse does he have? Obviously, Tom could go after the perpetrator of the scam. For instance, he could notify the authorities, such as the FBI or Federal Trade Commission, with the hope that they will institute an investigation, or he could hire his own private investigator. He could also use judicial processes to try and discover the perpetrator's identity, such as filing a John Doe lawsuit and serving a subpoena on the transferee bank to obtain identifying

information about the fraudulent accountholder. These efforts, however, are usually futile, as the perpetrators are typically not located in the U.S.

Who else may be held liable?

Tom could file suit against his agent Mary for failing to take basic steps to secure her email account. This is what a New York City couple did after criminals broke into their attorney's AOL email account and used it to trick the couple into wiring nearly $2 million to Chinese hackers. The case was Robert Millard et al. v. Patricia L. Doran, case number 153262/2016, in the Supreme Court of the State of New York, County of New York. The Millards sued their attorney for malpractice, alleging that she was negligent in relying on AOL for sensitive communications involving their purchase of an apartment because AOL email accounts are "notoriously vulnerable" to hacking. Their complaint alleged: "The lack of basic cybersecurity measures or awareness ... meant that this hack was not detected by [the attorney]. These cybercriminals then learned when and how the Millards intended to pay for the Apartment, knowledge that permitted them to pose as the seller's attorneys and thereby steal the Millards' money." The case was discontinued before the court issued a ruling, and thus it is unclear whether the court would have held the attorney liable.

Tom could also sue XYZ Escrow, alleging negligence and breach of contract. A court or jury may be more inclined to hold XYZ liable because it ignored and/or failed to notice the red flags surrounding the change in wire instructions and failed to take reasonable measures to verify the change in instructions.

In these situations, liability will likely depend on whether the agent, broker, or title company employed commercially reasonable security procedures. This is the standard courts use in deciding whether transferee banks should bear the risk of loss for unauthorized wire transfers.
For instance, in Choice Escrow and Land Title, LLC v. BancorpSouth Bank, 654 F.3d 611 (8th Cir. 2014), the Eight Circuit affirmed the district court's finding that the customer bore the risk of loss when a Choice Escrow employee fell victim to a phishing attack and contracted a computer virus that led to a series of fraudulent wire transfers. The Eighth Circuit found that the bank's security procedures for authenticating a customer's identity for wire transfers-which included password protection, daily transfer limits, and device authentication-were commercially reasonable, noting that they complied with published guidelines for the security of online banking and that the bank's security measures had adapted to address the shifting strategies of cyber-criminals.

In the case of a broker, agent, or title company, relevant factors in assessing the commercial reasonableness of security measures would likely include:

(I) the use of an email account that requires additional forms of authentication ("freemium" email accounts, such as Gmail, AOL, Yahoo, often do not require additional forms of authentication and thereby make it easier for hackers to gain access to emails);
(II) the use of digital signatures for messages (i.e., signatures that use encryption to secure documents and authenticate the sender of messages);
(III) the use of encryption to communicate with clients (which seals messages, allowing only the intended recipient to open and read its contents); and
(IV) the frequency of password changes.

In addition to security measures, a court or jury will also likely consider the reasonableness of the agent, broker, or title company's wiring procedures, including the steps they took in reviewing a communication regarding wire transfers and verifying its authenticity. For instance, did the agent double check the email address of the sender? Did the broker have procedures in place to detect peculiarities in the communication, such as grammatical errors or a different time zone? Did the title company have more than one employee review the communication? And most importantly, did they confirm the wiring instructions in a second, alternative mode of communication? Wiring procedures aimed at ensuring that communications are carefully reviewed and authenticated will not only minimize one's susceptibility to wire fraud schemes, but will also minimize the chances that a court or jury will find negligence on the part of the agent, broker or title company.

In sum, everyone is at risk of this type of cybercrime, whether they are direct victims of the fraud or others involved in the fraudulent transaction who may be held liable. The prevalence of these wire fraud schemes and the potential liability those involved in the transaction may face make it increasingly important that companies and agents undertake basic precautions to prevent significant harm. Such precautions include: (1) requmng two forms of communication/authentication before issuing a wire; (2) educating employees about data security; (3) using a secure internet provider and secure passwords for your email accounts; and (4) using encryption to communicate with clients and digital signatures for messages. Employing these precautions will decrease the risk of falling victim to wire fraud schemes and make it easier to defend against civil litigation that arises in the wake of these schemes.