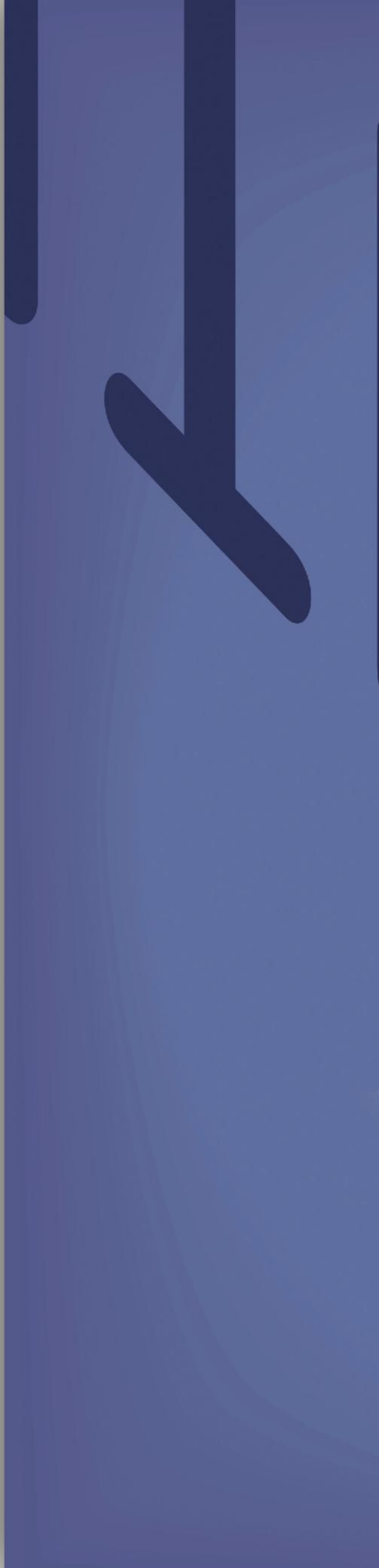
DON'T BE A VICTIM

Protect Yourself and Your Clients from Real Estate Wire Fraud

By Karen Queen



REALTOR® Ashley Jones (name changed to protect anonymity) knows the dangers of real estate wire fraud all too well. She and her husband nearly lost $183,000, which was intended for an investment home purchase, to an email scammer in one of the fastest-growing niches for cybercrime. Only quick and persistent action, along with the scammer's greed, saved Jones' money. Most victims never get their money back.

"I never thought fraud would hit me," Jones says. "My husband and I were buying a duplex as an all-cash deal. We were sending the cash from our brokerage account. We were in escrow, and I got an email with the wire instructions." That email, ostensibly from her escrow agent, was in fact from a scammer lurking in Jones' inbox. "Scammers targeted me because I am a REALTOR®," says Jones.

The scammer deleted the authentic email and substituted a similar email of his own with a key difference — the instructions were to wire funds to an account controlled by the scammer. That's when Jones' nightmare began.

Wire fraud scams are on the rise

Unfortunately, real estate is the second-highest targeted industry for cybercrime, according to the FBI. Most of these crimes target buyers' down payments.

From 2015-2017, there was a more than 1,100 percent rise in the number of email account compromise victims reporting issues related to real estate transactions, and an almost 2,200 percent rise in reported monetary loss.

"It has jumped exponentially in the past one to two years because criminals have figured out the best, most efficient process to execute the crime," says Robert Siciliano, CEO of CSI Protection, a provider of Cyber Social Identity Protection certification training for agents.

Another factor, Siciliano says, is that the communications are generally unencrypted — and no regulation exists regarding cybersecurity measures to force encryption.

"The real estate industry is one of the biggest targets of criminal hackers due to the fact that they are unregulated," he says. "If the industry doesn't do something about the issue now, it's only a matter of time before the government steps in and regulates." Absent any official regulations, it is up to individual agents to take action to protect themselves and their clients.

Criminals gain access to the email accounts of REALTORS®, title agents and others in the industry via data breaches or via phishing and spoofing (see table with definitions on page 24). Increasingly, cybercrooks are getting into email accounts via data breaches, Siciliano says. These emails appear legitimate because they are legitimate, since they're coming from the actual account as opposed to a spoofed account.

"All the crooks have to do is sort the [hacked] emails for RE/MAX, Century 21, Coldwell Banker and other real estate companies," says Siciliano. "Once they're in, they can just watch and wait."

This type of crime is on the rise partly because the potential benefit is high and

If you've been a victim of wire fraud, take these steps immediately:

Contact both the sending and receiving banks and place a fraud freeze on the affected accounts.

File a complaint with the FBI Internet Crime Complaint Center (IC3). You'll be issued a IC3 complaint number.

Call your local FBI office. Give them the IC3 complaint number so they can look up your details.

Contact a lawyer.

File a police report.

the risks are low.

"Unlike robbing a bank, wire fraud is fairly low risk," says Paul Benda, senior vice president of risk and cybersecurity policy at the American Banking Association. "It can be very lucrative. Criminals can walk away with tens of thousands, even hundreds of thousands of dollars."

While watching the target's email activity, the scammers study their manner of communicating, noting commonly used words and personal information about the target and their contacts. That's why emails from these scammers do not sound like the stereotypical Nigerian prince emails that are riddled with grammar, spelling and syntax errors. "The scammers know exactly what to say in an email and the most effective canned responses to any questions the buyer might have," Siciliano says.

Plus there's the fact that once executed, wire fraud is nearly impossible to reverse. "You have to catch it within hours," Benda says. "A wire is just like cash."

To keep your clients' personal data and down payments safe, there are critical steps you can take, including: reviewing C.A.R.'s Wire Fraud Advisory with your clients, insisting they always call a known phone number to verify wiring instructions, and adding multi-factor authentication to your email. (See the sidebar on page 24 for detailed instructions.)

These scams are trickier to detect than you'd think

So, was Jones scammed because she was unprepared? No. After receiving the wiring instructions email, Jones did the right thing: She called her escrow agent to verify the email was legitimate.

Jones' escrow agent confirmed that she had just emailed wiring instructions. So, thinking she was in the clear, Jones wired the funds from her brokerage account to what she thought was the title company's

How Do Scammers Hack Their Way Into Transactions?

To Protect Your Clients

1

Review with your clients the Wire Fraud Adivsory (C.A.R. Form W.F.A.). This will help you make clear for your clients that they should never wire money based on email instructions. Tell them they shouldn't even call a phone number listed in an email with wiring instructions. Instead, clients should call their REALTOR® or escrow agent at a number they've already been in communication with.

2

Make sure clients understand that when they call to confirm the wire transfer, they need to verify the name and address of the financial institution, as well as the account number.

3

Add a tagline to your email signature saying: "Never wire funds based on an email request. Call a known number first."

4

Add multi-factor authentication to your email.

account at a major bank.

What Jones didn't do, however, still haunts her: "I didn't confirm the account number."

The scammer, who had gained access to Jones' email account, had intercepted and deleted the actual wiring instructions email from Jones' escrow agent. He then substituted his own email purporting to be from the escrow agent that directed the funds to be sent to the same bank, but to a different account number.

"The email was exactly like the [deleted] email that came from my title officer," says Jones. "All the scammer changed was the account number and the bank's address. There wasn't even a trace of them being inside my email. They covered their tracks very well."

Not all scammers are this smooth. In some cases, Benda notes, scammers might send an email from the title officer saying there's been a change and providing new instructions. The result remains the same: The money disappears.

Jones had expected her wired funds to clear in the title company's account by the end of that day. On day two, Jones called her escrow agent and learned the money never arrived in the designated account. Jones and her escrow agent compared account numbers and realized the wired funds went instead to a recently opened, different account at the same bank.

At a time like this, many would be paralyzed by panic. Thankfully, Jones and her escrow agent leapt into action.

Swift action can save the day

The escrow agent had recently attended a fraud seminar presented by an FBI fraud agent, who had provided his mobile phone number. After notifying the banks, Jones and the escrow agent called the FBI agent, and he walked them through the fraud-reporting process.

But even though the incident was reported so quickly, fraud investigations take time. Getting the money back was a long shot. "I was devastated," says Jones. "I felt like I had messed up pretty big."

Then, on day three, Jones called her brokerage account representative's assistant to see if she could get the wired money back — and got a strange response from the assistant.

"I told the assistant, 'There's been a problem. The wired funds never got there,'" Jones says. "The assistant responded, 'Then why are you emailing asking for more money?'"

The scammer had been posing as Jones and emailing the brokerage assistant from Jones' account, asking for even more money to be wired to the bogus account. Then to cover their tracks, the scammer had deleted their emails from Jones' sent email folder. Thankfully, the increas-

Terms You Should Know

WIRE FRAUD ADVISORY: A C.A.R. form (W.F.A.) that helps you advise your clients on how to avoid being victims of cyber fraud.

MULTI-FACTOR AUTHENTICATION: A security system that requires you to prove your identity twice before gaining access to an online account. For instance, in addition to entering your password, you might also have to open up an app on your phone.

PHISHING: When a hacker sends emails pretending be from a safe source with the intention of stealing sensitive information.

SPOOFING: When a hacker sends emails pretending to be from a safe source with the intention of causing you to download malicious software onto your system.

ingly suspicious brokerage assistant took all the correct precautions: She wrote back explaining she couldn't send more money based solely on email instructions and insisted on speaking to Jones or her husband. The scammer also deleted those emails and, posing as Jones, responded via email and made excuses to the brokerage assistant for why Jones and her husband were not available to talk.

While this exchange was taking place, the receiving bank reviewed the fraud report and froze the scammer's account, which still had Jones' $183,000 in it.

In these scams, fraudsters normally bounce the money out of the accounts as quickly as possible so the funds can't be frozen or sent back to the recipient. But this scammer had waited to transfer funds out of the account in hopes of getting even more money out of Jones. That greed is what saved Jones in the end. Her transaction was delayed two weeks and she had to borrow another $183,000 to close, pending the return of her original funds, but otherwise, no harm done.

As for Jones, she's breathing easier now — although the brokerage assistant was so rattled by the whole ordeal that she won't talk to Jones on the phone anymore.

"I would have felt unbelievably horrible if it had been one of my clients," Jones says.

As Jones found out, even a scam where the victim gets the money back can be disruptive in terms of time, stress and money lost. REALTORS® must be vigilant to prevent scammers from preying on their clients. Don't assume this won't happen to you; act as though your email is already compromised and make decisions accordingly. Educate your clients to verify wiring instructions and account numbers in person or by calling a known number. A 10-minute phone call could prevent your client from losing their life savings.