Unit 8

Wire Fraud

In This Unit

The basics • Preventing and reporting wire fraud • Liability

Learning Objectives

When you have completed this unit, you will be able to accomplish the following.

- Describe wire fraud, how it happens, and how common it is.
- Describe how real estate professionals can help buyers and sellers protect themselves from wire fraud.
- Describe who is liable when wire fraud occurs.

THE BASICS

Example of Wire Fraud

Brian and Jean are scheduled to close on their dream home four days from now when they receive an email from their closing agent at XYZ Title Company:

> *Good Morning Jean and Brian,*
> *In reviewing the numbers for your upcoming closing, $78,985.88 is the amount needed for closing. You should wire these funds from your bank as soon as possible to our escrow account as shown below:*
> *Name of Bank: TrustShare Bank*
> *Routing Number 123456789*
> *Account Number 123456789*
>
> *Since we are currently receiving a high rate of calls in the office, it would be quicker if you respond to this email with any questions.*
>
> *Sincerely,*
> *Cathy Closer*
> *XYZ Title Company*
> *123-456-7890*

Brian promptly had the funds wired from his bank. Two days later, he received an email from Cathy Closer to wire $79,643 to the title insurance company's bank account. He called Cathy about the discrepancy. Cathy was confused. She told Brian that she had not sent the first email. When she suspected fraud, she suggested that he call the authorities right away. The FBI investigation included contacting the bank, located in the Cayman Islands. The bank reviewed the account and reported that the money had been deposited to the account and had been wired out of the account the same day. The funds were moved several times and were untraceable. Because the down payment was gone, Brian and Jean were unable to complete the purchase of their dream home.

While the story is fictitious, wire fraud happens more often that one would suspect. Email is part of every real estate transaction because the communication conveys important information with attached documents to buyers, sellers, real estate licensees, title companies, closing agents, attorneys, and mortgage lenders. Buyers who are excited about moving in to their new home sometimes blindly follow emailed instructions from a criminal posing as a title company, lender, or real estate agent.

FEDERAL AND STATE LAWS REGARDING WIRE FRAUD

Some of the federal and state statutes designed to prevent wire fraud include:

- The **Mail Fraud Statute** prohibits the use of mail to defraud or to scheme to defraud others. [18 U.S.C. 1341]
- The **Communications Act Amendments** apply to anyone who uses an interstate wire, television or radio communication, or the internet, with the intent to defraud. It is the law that covers wire fraud. [18 U.S.C. 1343]
- The **Computer Fraud and Abuse Act** outlaws conduct that victimizes computer systems. The CFAA protects computers that are connected to the internet and others from being used as instruments of fraud. 18 [U.S.C. 1030]
- The **Florida Communications Fraud Act** established penalties for schemes to defraud using legal precedent available under federal mail and wire fraud statutes. [F.S. 817.034]

Despite the increased occurrences, the FBI reports that only 15% of wire fraud incidents are reported.

Email is part of every real estate transaction and conveys important information and documents to buyers, sellers, real estate licensees, title companies, closing agents, attorneys, and mortgage lenders. Due to the common usage of email, the threat of fraud is often overlooked. Buyers, excited about purchasing their new home, are quick to follow instructions contained in an email without first verifying the sender. Title companies, closing agents, real estate companies, and mortgage companies may not have the proper controls in place to ensure their email communications are secure.

Ultimately, the unsuspecting buyer might send the funds for closing from their bank to an account set up by the fraudster rather than to the escrow account of the title company or closing agent. If the fraudulent account is in a bank outside of the United States, the buyer might be unable to recover the funds.

How Do Criminals Perpetuate Fraud?

Criminals use several steps to get the victim to let their guard down when using email.

Step 1: The fraudster begins by hacking the emails of real estate licensees, title companies or closing agents, and mortgage lenders by using malicious software (called malware) to gather pertinent information regarding real estate transactions. For example, a real estate licensee might receive an email to click a link to "receive a FREE smoothie," and when the link is opened, a malware program is downloaded to their computer. The fraudster might even search websites and social media posts looking for key words that would indicate real estate transactions are in progress.

Step 2: The fraudster will use the information gathered from the hacked email address to monitor the progress and get to know the involved parties in the transaction. The fraudster will use this information to create spoofed emails for the next part of the phishing scheme.

1. *Spoofing* is a common way that information, such as an email, sender name, phone number, or a website address, is disguised to deliberately mislead and appear to be from a credible or trusted source like a title company, real estate agent or broker, or a mortgage lender. It usually involves changing one letter, number, or symbol of the legitimate source. For example, the company name in an email may be misspelled, like mortgagelender@lender123.com would be mortgagelender@lender723.com.
2. *Phishing* is where an unsolicited (spoofed) email is sent to trick the receiver into revealing sensitive information such as passwords, financial information, or other personal information. Other variations of phishing occur over the phone or voicemail (vishing), through text (smishing), or when malware is used to redirect a user to a fake website (pharming) in order to collect information about a user.[1]

Step 3: As the transaction nears the closing date, the fraudster sends a spoofed email that appears legitimate from the title company or closing agent to the buyer explaining that there has been a last-minute change for the closing costs and giving the buyers new wiring instructions. This email might even discourage the buyer from calling the title company or closing agent by encouraging them to reply to the email with any questions.

Wire Fraud Statistics

According to the National Association of REALTORS®, wire fraud is one of the fastest-growing cybercrimes in the United States.

In the FBI's 2022 Internet Crime Report, the Internet Crime Complaint Center received 801,000 cyber fraud cases resulting in more than $10.3 billion in losses to individuals and businesses, a 50 percent increase from 2021. Of these cases, real estate wire fraud accounted for 397 million in losses.[2]

The Business Email Compromise (BEC) and the Email Account Compromise (EAC) complaints also increased from 20,373 victims and over $2.4 billion in losses in 2021,[3] to 19,950 victims and over $2.7 billion in losses in 2022.[4]

Practice Questions

1. Wire fraud is the crime of transmitting or causing to be transmitted using the internet with the intent to defraud or scheme to defraud someone.
   a. True
   b. False

2. Phishing is a common way that an email address or website is disguised to deliberately mislead and appear to be from a credible source?
   a. True
   b. False

1. https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/spoofing-and-phishing
2. https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf
3. https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf
4. https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

3. According to the National Association of REALTORS®, wire fraud is one of the fastest-growing cybercrimes in the United States.
   a. True
   b. False

4. When information in an email is disguised to appear to be from a trusted source, it is called *spoofing*.
   a. True
   b. False

PREVENTING AND REPORTING WIRE FRAUD

Protecting the Public From Wire Fraud

With the growing sophistication of real estate wire fraud schemes, making it harder to detect fraudulent activity, real estate professionals must become more diligent in protecting the home buyers and sellers with whom they work.

Prevention There are multiple recommendations real estate professionals can use to prevent wire fraud.

1. Educate home buyers and sellers about potential wire fraud schemes and how they work. Many real estate brokers now require a wire fraud disclosure to be signed or acknowledged by all parties in the transaction. The Florida REALTORS® created the Wire Fraud Prevention Notice (WFPN-3 Rev 2/20) for the brokerages to use with both buyers and sellers.
2. Include a wire fraud notice in email signatures. The National Association of REALTORS® suggests that real estate professionals should add a disclaimer to their email signature line (see the following sample notice). The use of the notice about wire fraud is not sufficient by itself and should not prevent real estate professionals from educating buyers and sellers about wire fraud in real estate transactions.

IN PRACTICE

IMPORTANT NOTICE: Never trust wiring instructions sent via email. Cyber criminals are hacking email accounts and sending emails with fake wiring instructions. These emails are convincing and sophisticated. Always independently confirm wiring instructions in person or via a telephone call to a trusted and verified phone number. Never wire money without double-checking that the wiring instructions are correct.[5]

3. Never send or forward wire instructions or financial information through email, especially if using public Wi-Fi or hotspots.
4. Advise home buyers and sellers to call the title company or closing agent using an independently verified phone number (not the phone number on the email):
   a. to verify wiring instructions prior to initiating the wire transfer and
   b. to verify their money has been received after the wire transfer is sent from their bank.
5. Advise buyers and sellers to watch incoming emails for red flags:
   a. For potential errors in the web address or sender's email address (e.g., closing@tilecompany.com instead of closing@titlecompany.com).
   b. That contain the words "urgent" or "time sensitive."

5. https://www.nar.realtor/law-and-ethics/wire-fraud-email-notice-template

c. That contain a change in wiring instructions (it is extremely rare that wiring instructions change at the last minute).
d. That encourage a response to the email rather than calling to verify information.
e. That contain unknown or suspicious links or attachments (clicking on these links or opening attachments could open a malware download allowing access to email accounts or computer systems).

6. Advise buyers and sellers to ask their bank to confirm the name on the receiving account before sending a wire transfer.
7. Warn buyers and sellers:
   a. Sending financial information through email is not secure.
   b. Make sure a website is secure before giving financial information on the website. Look for the URL that begins with https (the "s" stands for secure).
8. Make sure office and sales staff and transaction coordinators are extra diligent about scrutinizing emails.
9. Use an email service that has the capabilities of scanning emails for spam and malware.

Reporting If it is suspected that wire fraud has occurred, the buyer or the seller should do the following:

1. Immediately contact their bank to stop or recall the wire transfer.
2. File a complaint on the FBI's Internet Crime Complaint Center website (https://www.IC3.gov).
3. Contact the local law enforcement and the local FBI office to file a report.

Practice Questions

5. One way to protect homebuyers from wire fraud is to educate them about the possible scams.
   a. True
   b. False

6. Brokers and sales associates should forward any wire instructions that they receive from the title company to the buyer and/or seller.
   a. True
   b. False

LIABILITY

Who Is Liable?

When wire fraud has occurred, the question as to who is liable becomes an interesting one because there is no definitive answer. While the individual who committed the crime is obviously liable, the different parties who participate in the real estate transaction might be liable as well. The potential liability when wire fraud occurs in a real estate transaction can include all the parties involved: the real estate licensees, the real estate brokerages, the title company, and the bank.

In the case *Bain v. Platinum Realty, LLC*, in 2018, a Kansas Federal District Court upheld the original 2016 ruling that found the seller's real estate broker and sales associate liable for 85% of the losses incurred by the buyer because the fraudulent email had come from the seller's agent. The bank and the title company involved in the transaction (and originally named as defendants in the case) settled with the plaintiff in mediation.

With wire fraud increasing in frequency, real estate professionals need to recognize their responsibility for protecting buyers and sellers and acknowledge their potential liability in each and every transaction.

Case Study

A BROKER'S LIABILITY FOR WIRE FRAUD

Bain v. Platinum Realty, LLC

In *Bain v. Platinum Realty, LLC*, a Kansas federal court upheld a jury verdict that determined that a real estate licensee was 85% responsible for the buyer's losses. The losses occurred when that buyer transferred money to purchase their new home to a fake account after getting wire instructions from who he thought was his agent, but the instructions were from a criminal posing as the agent.

The buyer received an email from the agent that provided new wiring instructions for the upcoming closing on a property. Unwittingly, the buyer had been sent false instructions by the criminal, not his agent. The buyer used the instructions to wire money to the criminal's account, thus losing $196,622.

As this scam was uncovered, the agent learned that a criminal infiltrated the email exchanges between the agent and the buyer, created fake email accounts similar to the email accounts used by the agent, and used these accounts to transmit the false wire instructions that were sent to the buyer. The buyer blamed the agent for poor communication and negligence for conveying the incorrect wiring instructions.

The buyer sued everyone he could think of, including the agent. The agent claimed that she had never sent the email with the false wiring instructions. The agent did initially forward an email with the false wire instructions, but said she sent it to one of the fake accounts set up by the criminal, not to the buyer. In this case, she was using hindsight as a defense while at the time she simply hadn't paid close attention to the paperwork.

The agent believed she was innocent because she had not communicated the misinformation to her client.

The case went to trial, with the jury finding the agent 85% responsible for the loss with a judgment against the agent for $167,129. The agent filed a post-trial motion asking that the decision be reversed.

The United States District Court for the District of Kansas affirmed the jury verdict. The court rejected the agent's argument and found that her lack of attention in directing the buyer was the reason for the loss. The jury determined that the broker had, indeed, at one point, sent an email with the incorrect information to the buyer and gave further validity to the misinformation.

Had the agent simply reviewed the details of the instructions being sent, she would have identified the scam and saved the buyer the money for his home.