Section Four
WIRE FRAUD

1. Anya uses a free email account to communicate with her clients regarding brokerage transactions. She believes that this method of communication is secure because the networks at her firm and home office are password protected. Is Anya correct? Why or why not?

   _____

   _____

2. Broker Terrence's buyer-client is under contract to purchase her first home. Two weeks before closing, the closing attorney's paralegal emails Terrence the wiring instructions for the buyer's settlement funds, which Terrence forwards to the buyer.

   Two days before closing, the buyer receives another message from Terrence, alerting her that the wiring instructions have changed. The buyer, in turn, notifies her bank of the change.

   The closing attorney never receives the buyer's settlement funds. It is later determined that Terrence's email had been hacked, which ultimately resulted in the loss of the buyer's funds.

   What, if anything, should Terrence have done differently? Could Terrence be held responsible for the buyer's loss?

   _____

   _____

3. May is the accountant for ABC Properties. Bill, the property manager, sends May an email requesting a paper check to be sent to 123 Plumbing to pay an outstanding invoice immediately. May is slightly confused by the email because ABC Properties and other vendors are usually paid electronically at the end of each month. However, May follows the instructions in the email and sends the check.

   What should May have done? _____

4. Jim owns several properties in NC, and they are managed by 123 Properties, Inc. Jim was instructed to register an account with the firm's cloud-based management system to ensure timely receipt of payments and access to monthly statements.

   Once an owner establishes an online account, 123 Properties, Inc., has a policy that mandates employees are not allowed to change the account numbers for the owners. However, 123 Properties, Inc., receives an email from Jim asking them to change his routing and account number. How should they proceed?
   _____

5. Sue is a payroll specialist at Properties R' US. She receives an email from Tim, the receptionist. The email was sent from Tim's gmail account and requested that Sue change the financial institution in which he receives his direct deposit. A voided check was attached to the email with Tim's demographic information handwritten on the check.

   Sue processed the request and sent a confirmation email to Tim's work email address. Tim immediately called Sue and indicated he did not request this change. What should Sue do? _____

LEARNING OBJECTIVES

This section will review fraudulent activities that can occur in brokerage firms or transactions.

After completing this section, you should be able to describe:

- common fraudulent activity in the real estate industry; and
- best practices for real estate brokers to help protect themselves and their clients from fraudulent activities.

WHAT IS WIRE FRAUD?

Settlement Funds Scams

The following explanation is provided on investors-title.com:

> "When it comes to real estate-related wire fraud, thieves typically **target home buyers in the final stages of their transactions.**
>
> **Hackers gain access to the email accounts of key personnel** – whether it be attorneys, mortgage lenders, title companies, buyers, sellers or real estate agents – and monitor their messages for details of the deal as it unfolds.
>
> **The criminals then create a fake email address that mimics the seller, seller's agent, a title company, an attorney or other stakeholder in the transaction and sends a request to wire the closing money to a specific account.** By copying logos, email signatures and using language that sounds legitimate to the buyers, they are able to fool their victims.
>
> The victim, assuming that the email is a legitimate request and a logical next step in their deal, complies and wires the payment.
>
> Once the transfer is completed the money is in the hands of the thief and has likely been lost forever."

Excerpt from "Stay Protected from Wire Fraud in 2019." To read the full article, go to: https://investors-title.com/stay-protected-from-wire-fraud-in-2019/

THE THREAT IS GROWING

In a 2018 article titled, "Real Estate's Wire Fraud Vulnerability," Erica Christoffer stated:

> "Indeed, according to the FBI, there was a 136 percent increase between December 2016 and May 2018 in financial losses globally due to business email accounts being compromised, including sophisticated scams targeting both businesses and individuals performing wire transfer payments.
>
> **Scams specifically directed at the real estate sector rose 1,100 percent from 2015 to 2017. From June 2016 to May 2018, FBI data shows there was a loss of more than $1.6 billion in the U.S. alone.** What's more, cybersecurity company eSentire reported in October that real estate was the second highest industry hit with malware events in the second quarter of 2018."

Excerpt from REALTOR® Magazine. To read the full article, go to: https://magazine.realtor/for-brokers/network/article/2018/11/real-estate-s-wire-fraud-vulnerability

CAN REAL ESTATE BROKERS BE HELD ACCOUNTABLE FOR CLIENTS' LOSSES?

If a broker's email is hacked and a client's or customer's funds are compromised or stolen, could the broker be held responsible for the theft? The answer is yes.

These types of cases are beginning to pop up across the country. The first significant case, Bain v. Platinum Realty, LLC, happened in July 2018. Here is a recap of that case, courtesy of nar.org:

> **Licensee Liable for Wire Fraud Losses**
>
> Kansas federal court upholds jury verdict that determined that a real estate licensee was 85% responsible for the buyer's losses, which occurred when the buyer transferred purchase money to fake account after licensee allegedly forwarded email containing fake wiring instructions to the buyer.
>
> A real estate buyer ("Buyer") purportedly received an email from the listing broker ("Broker") that provided new wiring instructions for the upcoming closing on a property. The Buyer used the false instructions to wire the purchase money to the fraudulent account and lost $196,622. The criminal had infiltrated the email exchanges between the parties to the transaction and created fake email accounts that were very similar to the email accounts used by the parties. The criminal had used these accounts to transmit the false wire instructions that were eventually sent to the Buyer.
>
> The Buyer brought a lawsuit against a number of parties, including the Broker. The Broker claimed that she had never sent the email with the false wiring instructions. She had initially forwarded an email with the false wire instructions but she had sent it to one of the fake accounts set up by the criminal. She claimed that she had not sent the later email that the Buyer did receive and used to send the purchase money to the fraudulent account.
>
> The case went to trial, and the jury found that the Broker was 85% responsible for the loss and the court entered judgment against the Broker for $167,129. The Broker filed a post-trial motion seeking a determination in her favor.
>
> The United States District Court for the District of Kansas affirmed the jury verdict. The court rejected the Broker's argument that she did not send the email to the Buyer that was used to send the wire, finding this was an issue of fact for the jury to resolve as there was some evidence that the Broker had sent the later email. The jury determined that the Broker had sent the email, and so the court affirmed the jury verdict in favor of the Buyer.
>
> *Bain v. Platinum Realty, LLC*, No. 16-2326-JWL, 2018 WL 3105376 (D. Kan. June 25, 2018). [This is a citation to a Westlaw document. Westlaw is a subscription, online legal research service. If an official reporter citation should become available for this case, the citation will be updated to reflect this information.]

Reprinted from https://www.nar.realtor/legal-case-summaries/licensee-liable-for-wire-fraud-losses

HOW CAN YOU PROTECT YOUR CLIENTS AND YOURSELF?

NAR's "Window to the Law: How to Avoid Wire Fraud in Transactions" video provides excellent tips for brokers, including:

1. Educate [clients] about schemes.
2. Never send wire instructions via email.
3. Monitor email for unrecognized activity.
4. Never click attachments.
5. Use strong passwords.

Watch video: https://www.youtube.com/watch?v=C9lIZtIoYJs&feature=youtu.be

Security in Electronic Communications

Security DO's

- DO maintain multiple email accounts for your various purposes, e.g., one for online shopping, a separate account for personal emails, and a third account for business purposes.

- DO enable **Two Factor Authentication** (**2FA**); this process requires both a password and a second identifier.

- DO install firewalls, and use anti-virus and anti-malware/spyware applications.

- DO choose ***strong passwords*** and change all passwords periodically.

  The more unique the password is to you, the harder it is to crack. A "strong" password should be at least 12 characters, including upper and lower case letters, numbers and permissible symbols, or alternately, three random words (that you can remember) containing the foregoing features.

- DO choose tough security questions.

  If you can't create your own question and must select from a menu of questions, consider providing a false answer (but remember what the false answer is!). For example, if the question asks for a town where you were born or raised, name a town in which you never lived or a school you never attended, etc.

- DO encrypt your server, devices, and messages.

  Encryption is a process to protect data by converting readable data (called *plaintext*) into unreadable data (called *cipher text*) by using an algorithm (called a *cipher*). Decryption is the reverse process to convert unreadable text into readable text. The conversion is accomplished with ***paired keys***. So long as the decryption key is protected, the data is safe.

  There are various encryption software products available for protection of data on networks, desktop computers, laptops, and other portable devices. Brokers and firms should consult with an IT specialist to determine the products that will best protect their data and devices.

- DO monitor your account for suspicious activity.

- DO turn your electronic devices off when you leave your office or aren't using them.

Security DON'Ts

- DON'T use unsecured public Wi-Fi sites or public computers to check your email, financial accounts, or transaction files, as none of it is private or protected.

  If you must check email or a document, either use a mobile data service, e.g., 4G, or if you must use a public computer or Wi-Fi, use Virtual Private Network (VPN) which will encrypt the data passing through the VPN.

- DON'T open messages from unknown senders or click on links within or attachments to a message, particularly if there is no subject specified or the subject is generic.

- DON'T use the same password for all your online accounts.

  Since most people don't use multiple passwords or change them that frequently, hackers will use passwords found in one account to break into other accounts of the same user.

OTHER TYPES OF SCAMS

Employment Scams

An employer receives:

- a "phishing" email from a hacker that looks similar to the employee's email address, is grammatically correct, and bypasses email spam/junk filters, or
- a request from a hacker to change the direct deposit information of an employee before the next pay cycle.
    - The tone of the email is urgent, and
    - provides new routing and accounting numbers for the employee that is linked to an offshore bank account or prepaid debit card.

Property Management Scams

A property management firm receives:

- an email from an owner requesting the firm to update their account information in the owner's portal.
    - The tone of the email request is urgent, and
    - the owner is not available to speak over the phone.

OR

The property management firm receives:

- a telephone call from the owner requesting a change to their account in the owner's portal.
    - The owner indicates that they cannot log into the system and need the property management firm to update their information before the next disbursement.

Note: Wire Fraud Scams do not only happen in real estate closings. These types of scams can happen to employers and property management firms as well. It is important for brokers, attorneys, human resource personnel, office assistants, etc. to have established polices to contact individuals via a telephone conference to confirm receipt of the request and validate requested changes.

ANSWERS TO DISCUSSION QUESTIONS

PAGE 55-56

1. A broker uses a free email account to communicate with his clients regarding brokerage transactions. He believes that this method of communication is secure because his internet connection at the firm and his home office is password protected.
   Is this broker correct?

   Answer: It depends. The broker should be using a secure server to send and receive emails, and have the capability to encrypt attachments and all files. If the sender of the emails and the broker's servers are not secure, then the emailed information is at a greater risk of being hacked.

2. Broker Terrence's buyer-client is under contract to purchase her first home. Two weeks before closing, the closing attorney's paralegal emails Terrence the wiring instructions for the buyer's settlement funds, which Terrence forwards to the buyer.

   Two days before closing, the buyer receives another message from Terrence, alerting her that the wiring instructions have changed. The buyer, in turn, notifies her bank of the change.

   The closing attorney never receives the buyer's settlement funds. It is later determined that Terrence's email had been hacked, which ultimately resulted in the loss of the buyer's funds.

   What, if anything, should Terrence have done differently?

   Answer: Terrence should have verified the initial information with the paralegal first, before forwarding it onto the buyer, and then verified that it reached the buyer. Terrence should have also educated the buyer about possibility of scams and told her to call and question any future changes.

   Ideally, Terrence should not have been serving as the go-between for the wire instructions. Such information would be best communicated directly between the paralegal and the buyer.

   Could Terrence be held responsible for the buyer's loss?

   Answer: Yes, he could. There are many questions to consider, such as (but not limited to): Had Terrence educated the buyer about the possibility of scams? Had he taken steps to secure his email?

3. May is the accountant for ABC Properties. Bill, the property manager, sends May an email from his email account requesting a paper check to be sent to 123 Plumbing to pay an outstanding invoice immediately. May is slightly confused by the email because 123 Plumbing and other vendors are usually paid electronically at the end of each month. However, May follows the instructions in the email and sends the check.
   What should May have done?

   Answer: May should have called Bill to verify that he sent an email with instructions to pay a vendor for business using a paper check when the company usually performs these transactions electronically and monthly.

4. Jim owns several properties in Elk, NC, and they are managed by 123 Properties, Inc. Jim was instructed to register an account with the firm's cloud-based management system to ensure timely receipt of payments and access to monthly statements.

   Once an owner establishes an online account, 123 Properties, Inc., has a policy that mandates employees are not allowed to change the account numbers for the owners. However, 123 Properties, Inc., receives an email from Jim asking them to change his routing and account number. How should they proceed?

   Answer: 123 Properties, Inc., should contact Jim and verify that he sent the email and inform him of their policy. If they ascertain the request was valid, they should instruct Jim to change the information in his owner's portal.

5. Sue is a payroll specialist at Properties R' US. She receives an email from Tim, the receptionist. The email was sent from Tim's gmail account and requested that Sue change the financial institution in which he receives his direct deposit. A voided check was attached to the email with Tim's demographic information handwritten on the check.
   Sue processed the request and sent a confirmation email to Tim's work email address. Tim immediately called Sue and indicated he did not request this change.

   Answer: Sue should have noticed that the email was sent from a domain outside of the company and included financial information in an unencrypted email. Next, she should have called Tim to verify whether or not he sent the email before she changed his payroll information.