OLD REPUBLIC TITLE

FLORIDA LEARNING CENTER

Fraud and Scams Affecting Real Estate Transactions

What you need to know!

Presented by:

Old Republic National Title

Disclaimer

This information is not intended for legal purposes. Please consult with legal council regarding the manner in which laws and regulations referenced herein may be interpreted. This information is for educational purposes only.

Why are Housing Scams so Prevalent?

- *"Real estate is a common target for criminals due to the large sums of money involved in transactions as well as the sharing of sensitive information among multiple parties. According to a study conducted by FinCen, real estate is the third most common sector for fraud attempts behind construction and commercial services."**

***2021 FBI Threat Overview**

Here's why....

- Smaller to mid-sized companies.
- Busy professionals focused on clients, closings, marketing.
- Multiple players in the transaction: buyer, seller, listing agent, selling agent, title agent, mortgage broker and banks and only one needs to be fooled!
- Real estate purchase equals large sums of money.
- The parties to the transaction are sometimes distracted and frazzled with so many things happening at the same time.

OLD REPUBLIC TITLE

FLORIDA LEARNING CENTER

Common Cyber Threats

BEC/EAC

- ***Business Email Compromise*** is a scam targeting businesses (not individuals) working with foreign suppliers and/or businesses regularly performing wire transfer payments.
- ***Email Account Compromise*** is a similar scam which targets individuals wherein the fraudsters compromise email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfer of funds.

Business Email Compromise (BEC)

- In our industry BEC targets both businesses and individuals performing transfer of funds.
- The cybercriminal hacks or “spoofs” a legitimate business email to request wire payments go to a fake bank account.
- BEC evolved in 2022 and is now targeting cryptocurrency exchanges and investment accounts.
- BEC has been reported in all 50 states and 177 countries, with over 140 countries receiving fraudulent transfers.
- Based on reporting to the Internet Crime Complaint Center (IC3), banks located in Hong Kong and China were the primary international destinations for the transfer of fraudulent funds.

What you need to know

- Any participant can be targeted with scams designed to gather email account details.
- The hacker poses as the real estate agent, title agent or anyone in the transaction and convinces your client to divert funds.
- Access to one email account means all parties to the transaction are exposed and as the closing approaches the potential to be targeted or spoofed increases.
- This attack leads to wire fraud wherein funds are directed to a fraudulent account.

Wire Fraud

- Involves the internet, phone calls, faxes, email, texts or social media messages.
- The FTC showed that consumers reported losing more than $10 billion to fraud in 2023.
- Today, more people to depend on wire transfers making it more attractive to cybercriminals.

Here is how it starts…

- The hackers knows how the MLS works and look for properties that catch their interest.
- The hacker gradually worms their way into the conversation and patiently waits until:
  - Documents containing figures are shared via email and/or
  - Wiring instructions are shared via email
- Patience pays off as the day of closing is imminent.
- Hacker poses as realtor or title agent and strikes!

Buyer Manipulation – day of closing

- The buyer receives an urgent email supposedly from their realtor or title agent (really from the hacker) stating:
- **"Urgent: Our wire instructions have changed or Urgent: New wire instructions as follows:"**
- Email may state that if they don't wire funds immediately to the new instructions, they may lose the home.
- Buyer is stressed, opens email and wires the money.
- Funds are transferred to an offshore account and usually not recovered.

Seller Proceeds **– day of closing**

- The realtor or title agent receives an email supposedly from the seller (really from the hacker) stating:
- **Please disregard the previous wire instructions and wire our proceeds to the following:**
- Title agent does not contact the seller to confirm the change.
- Funds are wired to the fraudulent offshore account and usually not recovered.

How can wire fraud affect you?

Bain vs Platinum Realty LLC

- In 2018 Jerry Bain was working with a real estate agent to purchase a property.
- Bain received an email from his “realtor” stating the title agent changed their wire instructions and was instructed to wire $196,622.67 to the title agent’s new account included in the email.
- Unbeknownst to the parties involved, a hacker was intercepting e-mails exchanged between the title company, real estate agent, and Bain.
- At a critical time before the closing the hacker sent the tainted email.
- Bain sued!

Federal court upheld jury's finding

- A Federal Court has upheld a jury's finding that a real estate agent and her broker were 85% responsible for a wire fraud that cost their client $196,622.67 (Bain v. Platinum Realty, LLC, Dist. Court, D. Kansas 2018).
- Why?
- The court emphasized several points which can provide valuable lessons to all agents and brokers:

Lesson 1

- The listing agent was serving as the middleman between the settlement agent and her client. Serving in this role made her responsible for the delivery of accurate instructions to her client.

- **LESSON:** Have your client communicate directly with the settlement agent. Each transmission of an electronic message increases the risk that the transmission may be intercepted.

- **TITLE AGENTS RARELY CHANGE THEIR WIRE INSTRUCTIONS!**

Lesson 2

- The she failed to notice several irregularities in the both the e-mail messages as well as the wire instructions and forwarded it to her client.
- **LESSON:** Real estate agents must look carefully at electronic communications. Many fraudulent e-mails can be identified based upon a basic visual inspection. Any irregularities should be cause for alarm! Look for grammatical and punctuation errors.
- **It is still important to review an email for errors; however, AI has changed that. It is very difficult to determine if the email is AI generated or is created by your client. Hackers can spoof your email as well.**

Lesson 3

- Bain wired the money, and it was forever gone!
- **LESSON: Let your client know about this type of fraud. It is imperative they contact you and the settlement agent if they receive an email, voicemail or text from you regarding anything relating to the settlement agent's wire instructions**

Scare them!

- Add a fraud alert to your signature block.
- If your company does not have a formal notice you might want to add something like this to your signature:

"Online wire fraud is on the rise!

As your realtor, I will never send an email, text or call you with the settlement agent's wire instructions. If you receive an email from my address, a phone or text from my number regarding wire instructions DO NOT WIRE ANY FUNDS. Contact me and the settlement agent immediately as your funds may be at be at risk!"

- Discuss this issue with your clients during your first meeting, again at the signing of the contract and periodically throughout process.

OLD REPUBLIC TITLE

FLORIDA LEARNING CENTER

Current Scams

Seller Impersonation Fraud

- Scammers search public records looking for absentee owners – vacant land, rentals, investment properties are prime targets.
- These property types of property are being targeted because it may take several months or years to discover the fraud.
- Posing as the property owner, the scammer contacts a real estate agent to list the property unbeknownst to the property owner.

Why these types of properties?

- Vacant lots are usually surrounded by other vacant lots.
- Vacant lots have had the same owner for a long time.
- Owner is not local and cannot check on the property.
- Property has no open mortgages or other recorded liens.
- Owner recently deceased.

Red Flags

- Seller will only communication through text or email.
- Seller refuses to attend the signing for some reason.
- Seller wants to use their own notary.
- Seller wants a quick cash sale transaction.
- Sale price is set below market value.
- Schedule a video conference via Skype or Zoom.
- Request proof of ID be a part of the meeting.

Ask the questions…

- Ask the seller questions about the property that only the real owner of the property would know.
- Any unique features or the location in relation to shopping malls, Publix, etc.
- Ask how they decided to contact you, do they have any referrals or did they find you on the internet.
- Send the letter, via snail mail, to the owner's address shown on the tax collector or property appraiser website.

Foreign Nationals

- Consider FIRPTA implications which can bring fraud to light.
- Let the foreign national know that 15% of the sale price must be collected and sent to the IRS.
- Let foreign nationals know they must have documents notarized at the US Embassy or Consulate of their country of residence. An Apostille is required to be submitted with the documents.
- Consider a RON signing – sellers must answer KBA and credential analysis.

Entity owned property red flags

Fraudster claims they are the principal owner of the property, however, Secretary of State's site reveal recent changes to principal(s).

- Go to www.sunbiz.org - search for corporate listings immediately upon speaking with the seller.
- If changes were made ask for some type of documentation from the potential client.
- Don't waste your time.

10 minute break

Is AI the latest threat?

Answer: A BIG YES!

- AI is empowering fraudsters with new ways to enter your transaction.
- The new tools blur the lines between what is real and what is fake.
- Two of the latest ways they attach are voice spoofing and grammatically correct fraudulent emails.

Voice Spoofing

- Scam artist are using voice spoofing to mimic your voice.
- Criminals use voice cloning tools to scam people into sending money to fraudulent accounts.
- They can clone from TikTok, voice mail, social media etc.
- The voice can be cloned from a short clip of a person's voice – all they need is 3 seconds.
- If you do not recognize a phone number let the caller speak first.

How to protect your customer?

- Talk with them about voice spoofing.
- Suggest they only answer a call from you from a trusted number.
- BUT they need to wait a few seconds before they say anything.
- Remember, they can spoof your phone number also.

Grammatically correct emails

- Previously, you could determine if an email was spoofed because it contained incorrect grammar and spelling.
- AI platforms can produce emails that are grammatically correct and more efficient.
- The scammer can speak the text and AI will produce a grammatically correct email.

OLD REPUBLIC TITLE

FLORIDA LEARNING CENTER

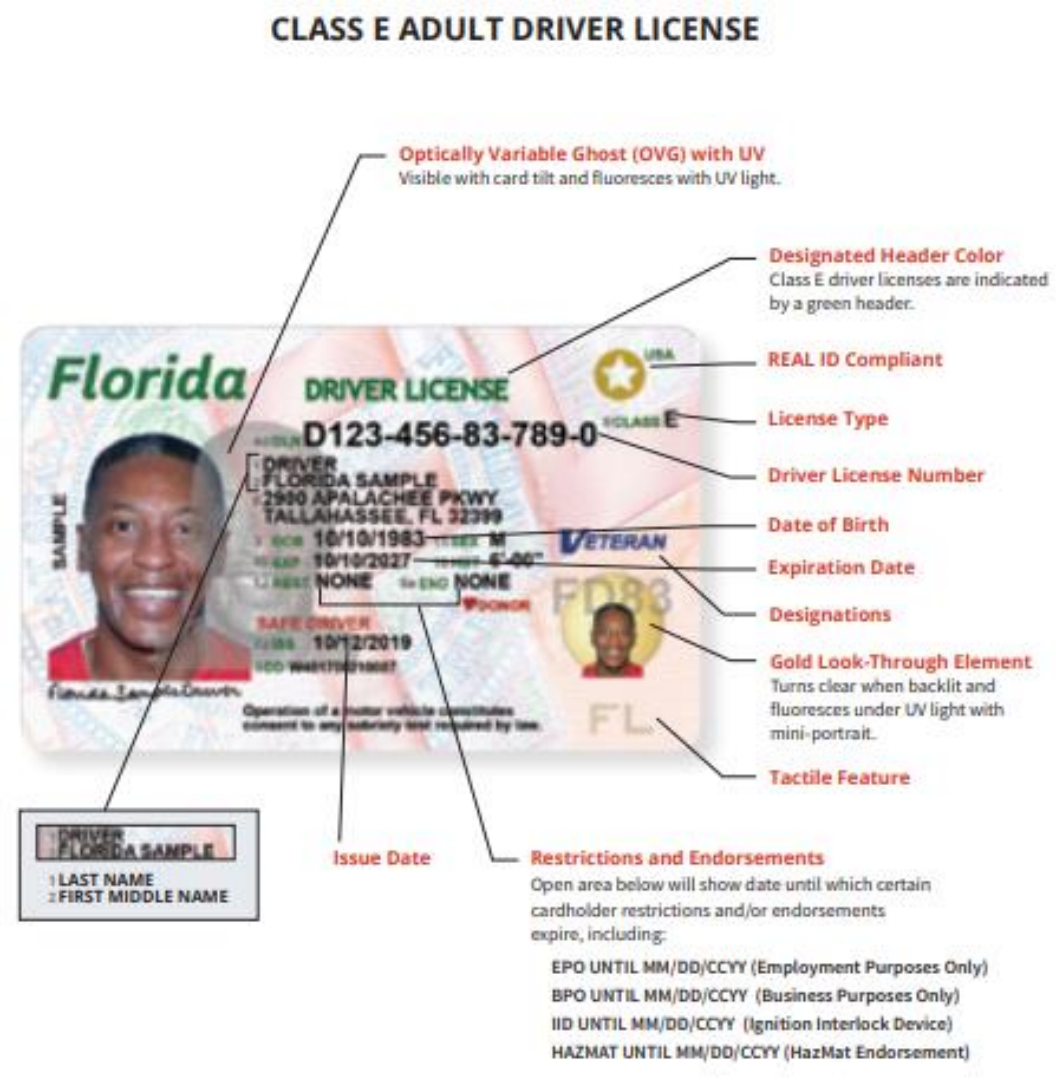
Review of Photo IDs

Grab your driver's license!

Front Card Diagram

The front of each Florida driver license and ID card contains the following personal identifying information:

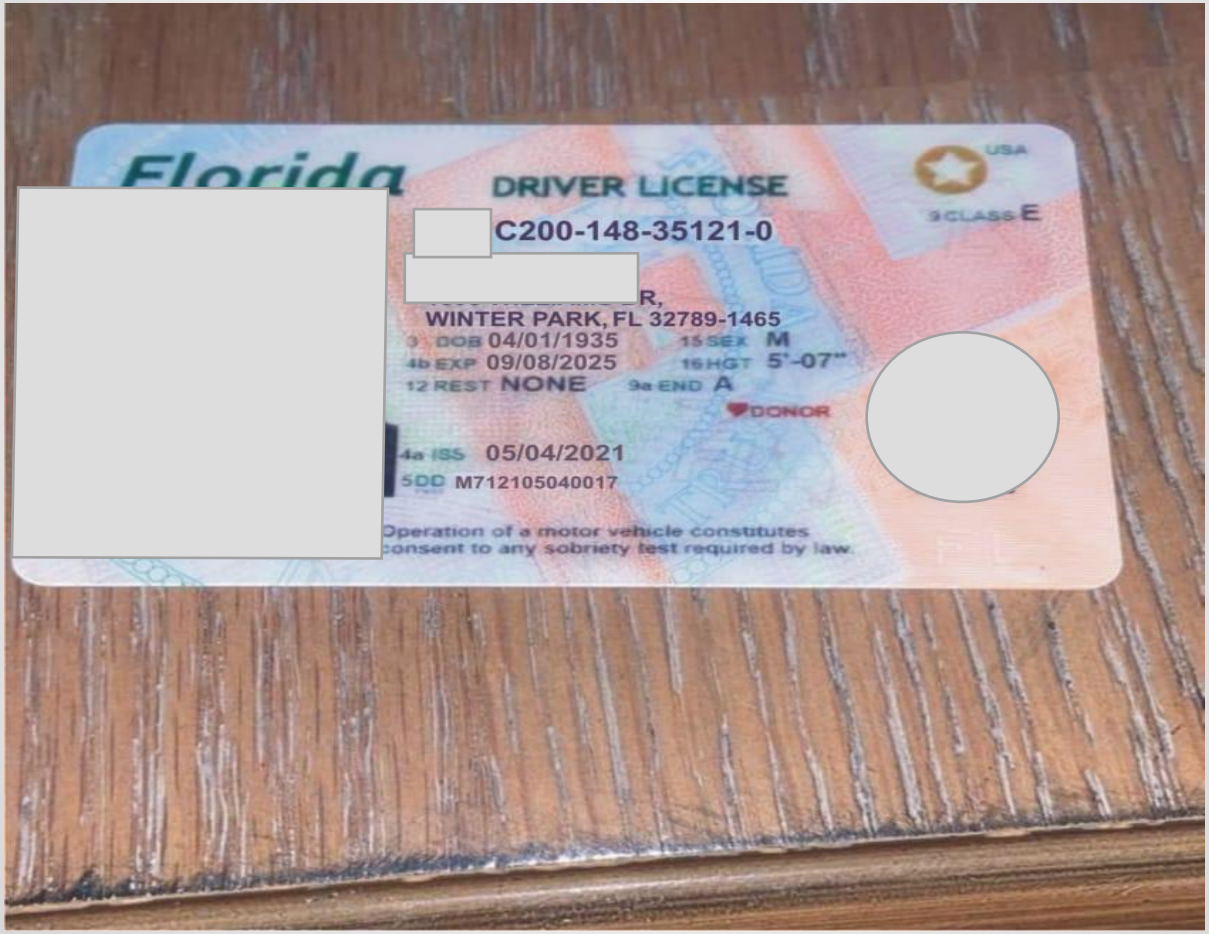
- Photograph of the individual overlapping the linear image of the Florida State Seal;
- Driver license or ID card number;
- License type (i.e. Class E);
- Family name/given names;
- Cardholder address;
- Date of birth;
- Sex;
- Date of expiration;
- Height;
- Issue date; and
- Restrictions, endorsements & designations



OLD REPUBLIC TITLE

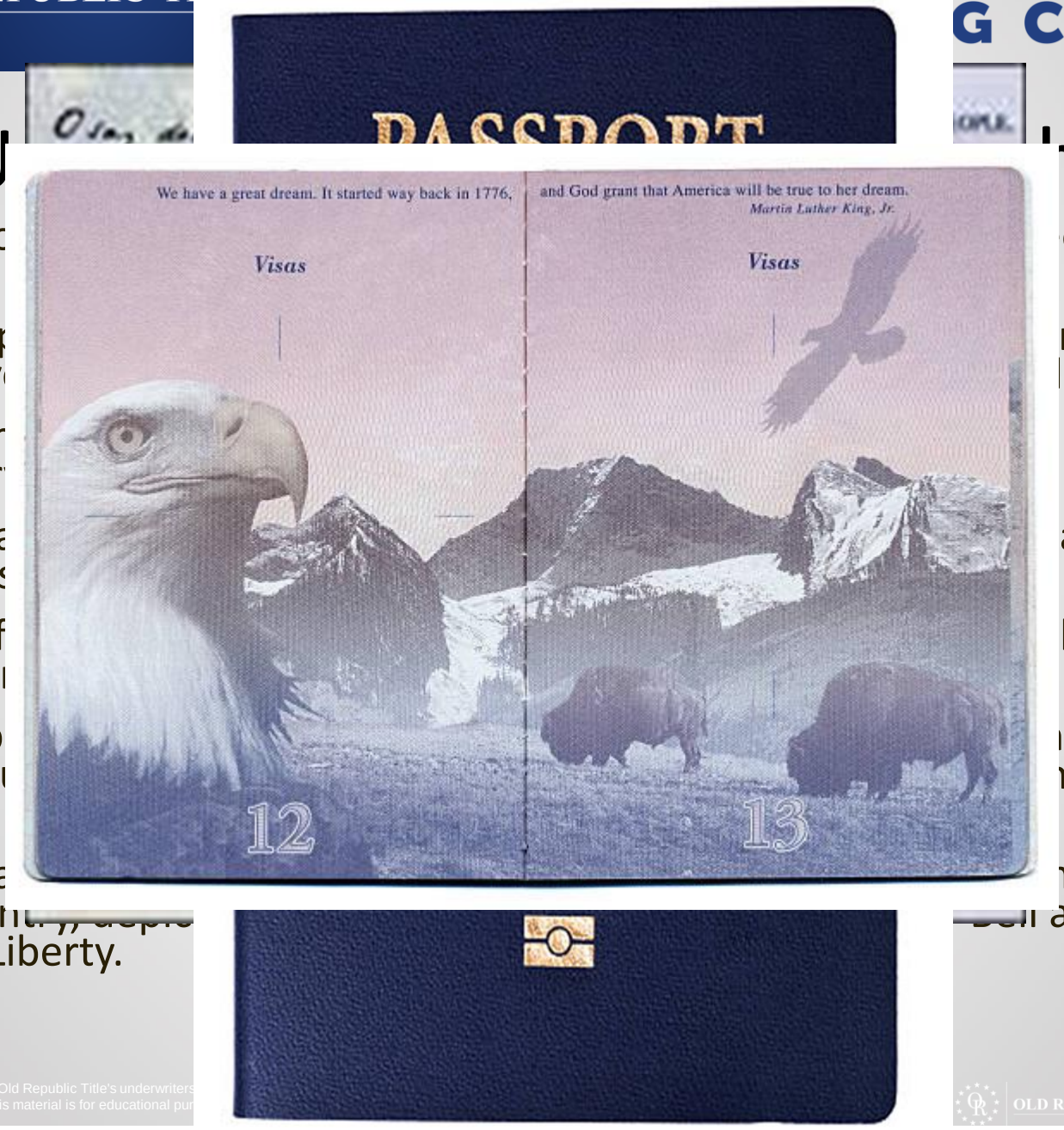
FLORIDA LEARNING CENTER

Drivers License Fraud



How U hers

- The color c en passports.
- American p ry is printed on the cov , too.
- Many cour celebrate the countr
- The first pa am Lincoln and a mess
- The rest of lly American images pri
- The data p g details and signatu d bald eagle.
- The visa pa holder enters a new coun and the Statue of Liberty.



Wi-Fi

- Do not use public Wi-Fi .
- Access Wi-Fi using VPN (Virtual Private Network) only.
- VPN uses encrypted tunnels to keep information safe while traveling the internet.
- Personal hotspot is not secure.
- Use multifactor authentication.
- Use a password generator – Dashlane, Fastpass

"Juice-jacking"

- Juice-jacking is another form of cyber-theft.
- Do not use public USB charging stations at airports or on airplanes.
- Bad actors can load malware onto public charging stations to export personal data and passwords directly to the perpetrator.
- Instead use an AC power outlet, carry an extra battery, or portable charger.

Advice to your client

1. Buyers call the settlement agent to let them know you are getting ready to send the wire and confirm wire instructions. Call the settlement agent after the wire transfer was initiated.
2. Sellers – the day of closing, confirm the wire instructions you gave to the settlement agent.
3. Never wire based on an unexpected email, phone call or text from me. Always call the settlement agent at a trusted, verified number to confirm that any changes are necessary!

Title agents never change their wire instructions!!

OLD REPUBLIC TITLE

FLORIDA LEARNING CENTER

Thank you for attending today!