17-Apr-23

Caution - Be aware of fraudsters targeting your real estate transaction

HOMESMART
Real Estate Made Easy

Created by:

Randy Rought
REALTOR®
303-503-6210

Air Force Retiree still Serving my Community

[i]

There are numerous ways fraudsters will target your transaction.

- If you get an email or telephone requesting personal information, account numbers, changes in routing instructions, or any other activity which makes you suspicious. Don't tell them anything. No one from HomeSmart will contact you except for me. HomeSmart nor any of their agents, including myself, will ever deal with the wiring instructions. If we need to, we will visit the lender or title company in person to provide the information they need. We want you to provide this information and all personal information in person to the lender and Title Company.

Intercepted Emails


[ii]

- Scammers hack into the email of people involved in the transactions, such as agents or title companies, and trick home buyers into wiring funds to them instead of the appropriate parties. They often will use a generic email address indicating the funds should be wired to a specific account which will then vanish without a paper trail. The email sounds strange – some listings hide the email address when you send a message, so you might not be able to see the address if you respond to the listing. Scammers usually use free email servers and they'll often go by a series of random letters to make them less easily traceable.

iii

- The seller, lender rep, or title will appear to send you an email asking you to wire money or click some unknown link. If you see this term or something similar, red flags should go up. Many scams entail wiring of funds because it's more difficult to trace and enables the scammer to collect the money sooner. Scammers will come up with a variety of plausible reasons why the money should be wired rather than sent through a bank or lawyer.
- Changes made regarding payment details should always be done by the buyer in person if possible, or telephonically verifying the email, and not via email alone. Protect yourself by double checking everything, verifying all emailed instructions which deal with the purchase even if they're from trusted parties, any bank detail changes need to be accompanied by the required verification of the bank accounts in question. Money wired is often unrecoverable and lost forever.

Fraudsters posing as a Buyer band then seller

- A scam artist, who gained initial access as a buyer, takes what he has learned, and starts marketing the home online as the agent, often at a great price. They will grab photos off various websites, and then find a second buyer who is the target of the scam. The scammers are after the buyer's deposit money. The buyers will make an offer and pay a large deposit to the supposed agent. Make sure you check every detail when it comes to property sale transactions; documents can be falsified, and email addresses cloned.
- A second method is for a scammer to approach a seller privately and show keen interest in the property and put in a great offer. After a few days, the supposed buyer will contact the seller asking for a document(s) to be signed to help them get their home loan approved. The hope of the scammer is to get the seller to sign all the documents, (without reading them all), only for the seller to discover later one of the forms was a quit claim which gives support to a third party claim they bought the home.

iv

Identity Theft

- Criminals have become much more experienced and are using stolen identity details not only to empty bank accounts but to obtain various credit accounts and even home loans. They are able to delay detection of the fraud for long periods while the unpaid bills and installments mount up.
- The scammer will use false documents to pose as the property owner, register forged documents transferring a property to their name, and then get a new mortgage against the property. After securing a mortgage or line of credit, the criminal takes the cash and disappears.

PS: This isn't Groucho Marx. Groucho is dead [v]

Pushy Sellers

- The seller pushes you – the faster a scammer gets you to agree to a business deal, the faster they can steal your money and avoid getting caught. The seller will often use high-pressure tactics in an attempt to push you into acting quickly in order to purchase the home. Don't be prodded by any seller to send money.
- Never pay a deposit before you have viewed a property.
- Be wary of agents who seem too eager or pushy to get you to buy the property they are marketing. A legit agent will always conduct the necessary checks and will not be too disappointed when you don't show much interest in the property.
- If the selling agent is constantly making up excuses as to why they are not able to show the property, you should also be worried. The chances are good they don't have access to the property and are stalling for time until they can think of a clever way to get you to pay the deposit.

[vi]

Foreign sellers or buyers

- In this modern electronic world, scamming can be conducted from any point on the earth. Be cautious if the buyer or seller is foreign and wants to buy a home unseen – most people want to at least see a property and become familiar with the area before making a large investment. This doesn't mean you should be wary of all foreign inquiries, but many scams often occur overseas because it's harder to trace the person behind the fraud. Foreign buyers who don't ask questions, act in haste, and don't care to see the property indicate a high likelihood of fraud.


[vii]

Bargains

- If the price looks too good to be true, it probably is. Prices are considerably higher than they were a few years ago. Be well informed about market related prices within the area you are looking to buy. If a property is advertised way below the market related price for your area it should raise your concerns. It could be something as simple as it needs major repairs, or it could mean they are hoping to score a quick deposit.
- Be wary when you are requested to make a payment for something minor like a credit check or security deposit, in most cases, there's nothing you can do to get your money back because the scammer can't be tracked.
- If you found a "bargain" online you should call the estate agency to find out if the deal is for real. Don't call the number at the bottom of the ad because this number could lead to a fake office. Call the actual office number, and ask the receptionist to give you the number of the specific agent or branch you are looking for.

[viii]

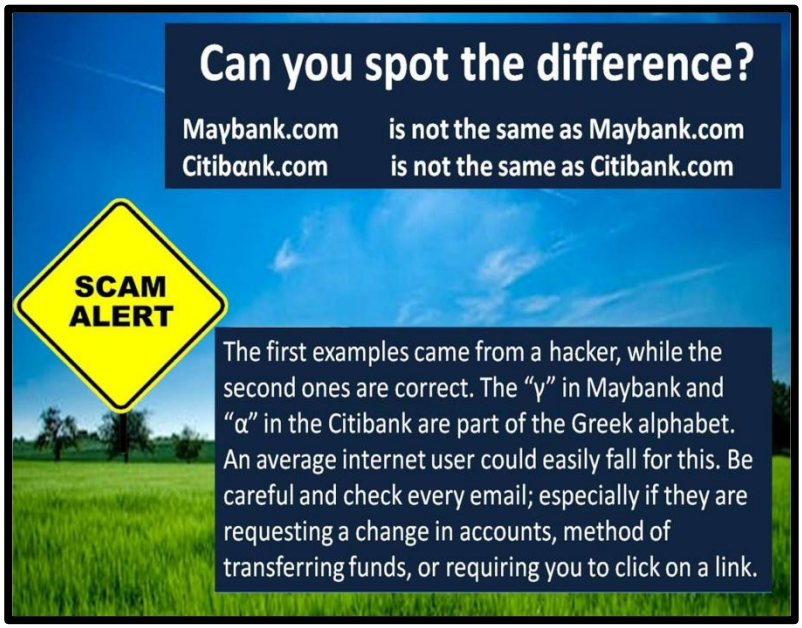
Bait and Switch Scheme

- This occurs when a prospective buyer offers an 'above market value' price to a seller. The seller, impressed by the high offer signs the contract, meanwhile the deceitful buyer has no intention to purchase the property.
- Once the seller signs the contract, the seller can only work with this buyer for the specified time. When the timeframe get close to the date, the fraudster asks to extend the contract a few weeks to work out closing details. Sounding reasonable, the seller agrees to the extension since it was a very high offer.
- In the meantime the seller keeps paying taxes, maintenance, utilities and insurance the buyer comes back to the seller with an excuse as to why this price no longer works, and requests a reduction to below market value and threatens to cancel if their demand is not met. Stressed by time and on-going costs, the seller agrees to the reduction.

ix

Wire Fraud/Phishing Fraud Disclosure

- Advice to prevent fraud by someone pretending to be with the Title Company and requesting personal data.
  - Criminals/hackers are trying to fake clients into wiring money to them. Never rely on email or an email with a link for wiring instructions.
  - Criminals hack email accounts of title agents, mortgage brokers, real estate agents, lawyers (and others) and send emails which look like legitimate emails from the proper party, but instruct the client to wire money to the accounts of the criminals.
  - There have been instances of phones being hacked, so the number and message looked like it came from client's REALTOR®, telling the client about a wiring instruction change.

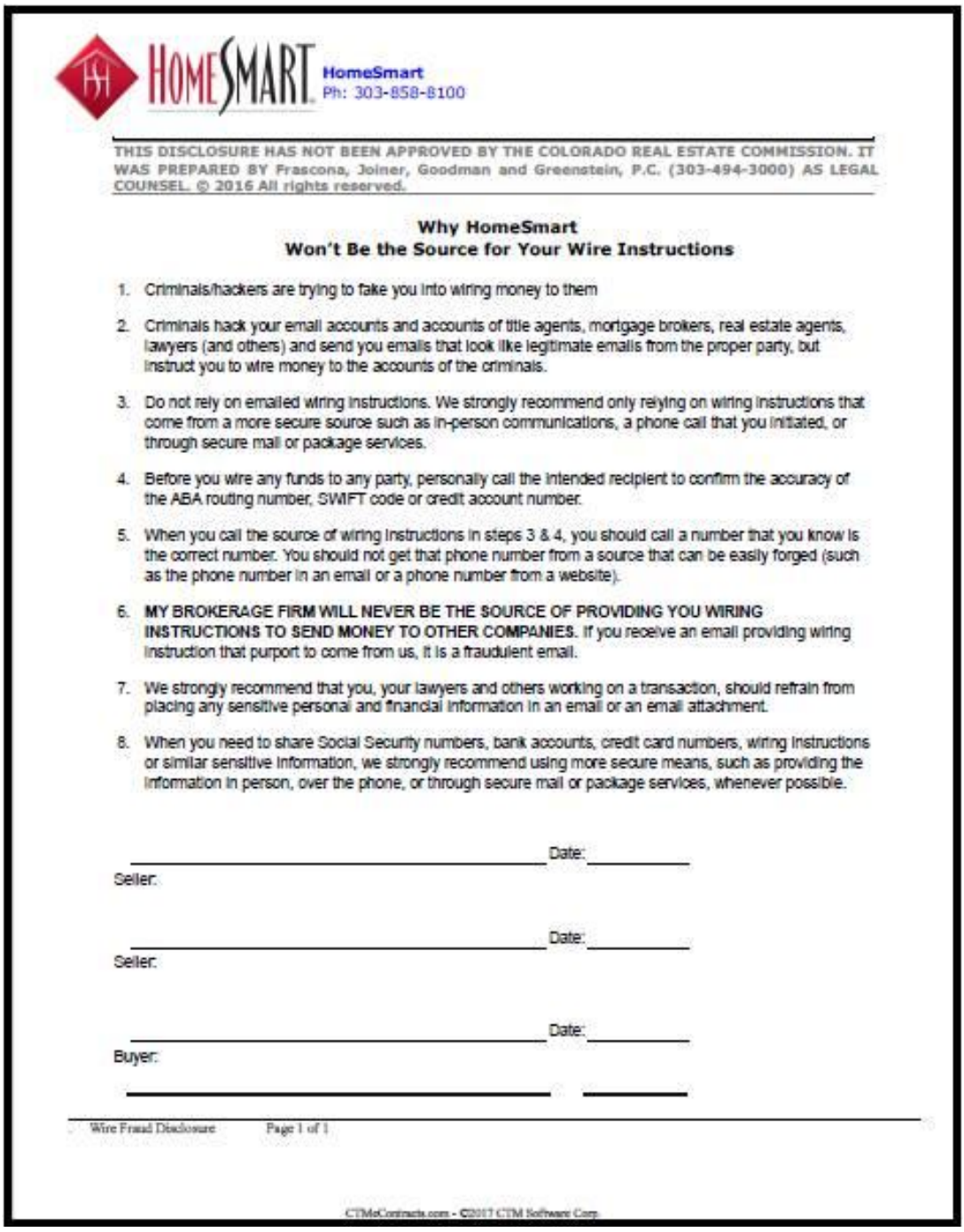


x xi

  - Ensure the client does not rely on emailed wiring instructions. It's strongly recommend they rely on wiring instructions which only come from a secure method such as in-person communications. Any other methods leave an opening for a scam. I cannot stress enough, the best way is for the client to share wiring instructions (especially confirming the accuracy of the ABA routing number and SWIFT code), Social Security numbers, bank accounts, credit card numbers, or similar sensitive information is to go personally to the Title Company or lender, and exchange this information with the proper representative face-to-face.
  - We strongly recommend everyone working on the transaction should refrain from placing any sensitive personal and financial information in an email or an email attachment.

HomeSmart will never provide wiring instructions.

- HomeSmart will never provide client with wiring instructions. If you receive an email with wiring instructions which purports to come from HomeSmart or me, it is a fraudulent email. Please contact your agent quickly so we can contact the local authorities. HomeSmart provides a wire fraud disclosure form to their clients and requires clients sign the statement to show their understanding of this.



HomeSmart
Ph: 303-858-8100

THIS DISCLOSURE HAS NOT BEEN APPROVED BY THE COLORADO REAL ESTATE COMMISSION. IT WAS PREPARED BY Frascona, Joiner, Goodman and Greenstein, P.C. (303-494-3000) AS LEGAL COUNSEL. © 2016 All rights reserved.

Why HomeSmart
Won't Be the Source for Your Wire Instructions

1. Criminals/hackers are trying to fake you into wiring money to them
2. Criminals hack your email accounts and accounts of title agents, mortgage brokers, real estate agents, lawyers (and others) and send you emails that look like legitimate emails from the proper party, but instruct you to wire money to the accounts of the criminals.
3. Do not rely on emailed wiring instructions. We strongly recommend only relying on wiring instructions that come from a more secure source such as in-person communications, a phone call that you initiated, or through secure mail or package services.
4. Before you wire any funds to any party, personally call the intended recipient to confirm the accuracy of the ABA routing number, SWIFT code or credit account number.
5. When you call the source of wiring instructions in steps 3 & 4, you should call a number that you know is the correct number. You should not get that phone number from a source that can be easily forged (such as the phone number in an email or a phone number from a website).
6. **MY BROKERAGE FIRM WILL NEVER BE THE SOURCE OF PROVIDING YOU WIRING INSTRUCTIONS TO SEND MONEY TO OTHER COMPANIES.** If you receive an email providing wiring instruction that purport to come from us, it is a fraudulent email.
7. We strongly recommend that you, your lawyers and others working on a transaction, should refrain from placing any sensitive personal and financial information in an email or an email attachment.
8. When you need to share Social Security numbers, bank accounts, credit card numbers, wiring instructions or similar sensitive information, we strongly recommend using more secure means, such as providing the information in person, over the phone, or through secure mail or package services, whenever possible.

_____ Date: _____
Seller:

_____ Date: _____
Seller:

_____ Date: _____
Buyer:

_____ _____

Wire Fraud Disclosure Page 1 of 1

CTMeContracts.com - ©2017 CTM Software Corp

[i] https://cdn.pixabay.com/photo/2022/02/02/21/26/scam-6989424_960_720.jpg
[ii] https://cdn.pixabay.com/photo/2022/03/03/20/29/scam-7046018_960_720.jpg
[iii] https://cdn.pixabay.com/photo/2022/03/03/20/29/scam-7046018_960_720.jpg
[iv] https://images.pexels.com/photos/11798029/pexels-photo-11798029.jpeg?auto=compress&cs=tinysrgb&w=600
[v] https://cdn.pixabay.com/photo/2014/06/04/16/58/cigar-362183__340.jpg
[vi] https://upload.wikimedia.org/wikipedia/commons/a/ab/Money-1428594_1920.jpg
[vii] https://cdn.pixabay.com/photo/2016/03/11/09/05/mask-1249929__340.jpg
[viii] https://cdn.pixabay.com/photo/2018/08/30/08/54/truth-3641636__340.jpg
[ix] https://cdn.pixabay.com/photo/2018/10/13/17/53/chasing-3744753__340.jpg
[x] https://cdn.pixabay.com/photo/2022/03/03/20/29/scam-7046018__340.jpg
[xi] https://images.pexels.com/photos/440731/pexels-photo-440731.jpeg?auto=compress&cs=tinysrgb&w=600