Reno/Sparks Association of
REALTORS®
5650 Riggins Ct., Ste. 200
Reno, NV 89502

Wire Fraud in Real Estate Transactions

By Doug McIntyre, President
Reno/Sparks Association of REALTORS®

According to a recent article in the Chicago-Sun Times, the FBI reported that in fiscal year 2017, nearly $1 billion ($969 million) was “diverted or attempted to be diverted” from real estate transactions, and wire to “criminally controlled” accounts. It occurs every day. Consumers, particularly those involved in a real estate purchase or rental, are prime victims.

How it happens in a real estate purchase

It might be helpful to understand how this criminal activity is occurring. Hackers are monitoring emails of lenders, real estate agents, title companies and maybe even you. They identify a pattern of communication between the parties that clearly indicates that a party is involved in a transaction to buy or sell real estate. From the communications between the parties, they determine when the transaction will be closing. Then they spoof an email, which may look very legitimate, to the potential homebuyer or seller with a change in wiring instructions. The unwitting party, excited about the prospect of closing escrow on his/her home, complies with new wiring instructions and wires funds to the wrong place. It’s happening across the country.

There are things you can do to protect yourself from becoming a victim of a wire fraud scam, and tips for keeping a real estate transaction secure:

1. At the beginning of the real estate transaction, your REALTOR®, the escrow officer and the lender should have a conversation with you about their communication practices.
2. Avoid free Wi-Fi with no firewall to protect against hackers capturing an email password or other sensitive information.
3. Always use strong passwords and change them regularly. It also wouldn’t hurt for you to change your password before wire instructions are sent.
4. Obtain the name phone number and email address of the lender, REALTOR® and escrow officer.
5. Avoid sending personal information in email or text (e.g., social security numbers, bank account information, etc.) Provide this information in person or

over the telephone directly to the verified phone number of the escrow officer or lender.
6. Be suspicious of a request for secrecy or pressure to take action quickly.
7. Immediately report and delete unsolicited email spam from unknown parties. Do not open spam email, click on links in the email or open attachments. These often contain malware that will give access to your computer system.
8. If you expect to engage in a wire transfer, instruct the title company or REALTOR® that the wiring instruction must be sent to via an encrypted email including attachments, via a landline fax, USPS or overnight delivery or hand delivery. Be aware that using encrypted email is not sufficient protection against fraud to the wrong email address or person. Make sure you are sending it to the correct email address based on the information you obtained at the start of the transaction.
9. Once you receive an instruction, call the known party you will be transferring funds to on the phone immediately prior to the transfer of funds so you know you are wiring money to the legitimate source. Do not call the phone number that is in an email instruction to wire funds. It is likely not legitimate just as the email wire instruction is also not legitimate. Title companies warn that if you receive an email with a change in wiring instructions, be suspicious. Title companies rarely change their wiring instructions.
10. Call the known recipient and ask them to confirm when they have received the funds.

How wire fraud and leasing scams occur

Scammers locate a home for sale or for lease, copy the pictures and sometimes the description. The scammer then posts a fake listing on an online rental database – the most common is Craigslist. The scammer lists the property for below market rent to gain interest in the property. Once a prospective victim reaches out to the scammer via email, text or phone, the scammer will proceed to communicate with the prospective victim with lies, and pressure the victim to wire the funds to hold the home. In many situations, the prospective victim becomes a victim of wiring funds to the scammer and later signing a fake lease.

Here's how prospective renters can avoid these situations

1. If it's too good to be true, it probably is. Ask yourself why is the rent on this home is substantially less per month than a home around the corner? This is the most obvious indication of a scam.
2. Never wire funds to obtain a rental. It's not done in the normal course of business in acquiring a rental, and you incur unnecessary costs to wire funds.
3. If you're communicating directly with a landlord/owner (not a licensed and permitted property manager), request to meet the landlord in person. Before you meet them, look up the landlord's name on the County Assessor's website in the county where the home is located.

4. If the landlord isn't using the services of a licensed permitted property manager, and the lease is not signed by that property manager, the lease must include a standard disclosure required pursuant to NRS 118.200. The disclosure substantiates for law enforcement officials that there is a rebuttable presumption that the tenant has lawful occupancy to the property. More important, when a lease is initiated by other than a licensed and permitted property manager, for your protection it should be notarized. The Notary will need to verify the identity of the landlord and you. You and the landlord/owner should meet with the Notary together.
5. Wait to provide funds until that time.
6. Finally, the best way to avoid scammers is to consider leasing a home from a business that has a licensed and permitted property manager. Any and all property managers must hold a real estate license and property management permit which can be verified through the Nevada Real Estate Division online license search at: https://red.prod.secure.nv.gov/Lookup/LicenseLookup.aspx

What should you do if you think you have become a victim of a wire fraud scam

1. Immediately contact the bank to try and stop the funds
2. Contact the escrow officer, lender and REALTOR®
3. Contact the local police department
4. Report it to the following agencies:
   Federal Bureau of Investigation: https://www.fbi.gov/
   FBI Internet Crime Complaint Center: www.ic3.gov

The National Association of REALTORS® has created an informative video that provides helpful information to prospective home buyers:

http://bit.ly/BuyerWireFraudAlert

Other resources on this topic:
National White Collar Crime Center https://www.nw3c.org/

Protect yourselves from wire fraud. And talk to your REALTOR® if you have any additional questions or concerns. The knowledge you have today can help you in the future.

Article will be released in the Northern Nevada Business Weekly the week of February 5, 2018