

# Michael Saunders & Company

Licensed Real Estate Broker

## Cyber Security/Wire Fraud Notice

You are being provided with this Disclosure because wire fraud committed by cybercriminals is a very real and costly concern in today's real estate market. No one is immune. Hackers can intercept email accounts and passwords without the account holder's knowledge by using viruses, malware, and spoofing emails which appear like legitimate email from a business. Therefore, everyone who participates in a real estate transaction must institute best practices to safeguard against this unique type of crime. The seller, buyer, Realtors®, lenders, mortgage brokers, title companies and attorneys all play a vital role. Below are recommended procedures which we ask you to follow for your own protection and to ensure the integrity of the transaction. Remember the loss of funds are often not recoverable. Prevention is the key.

**STEP 1:** When you know who will be conducting the closing – ***call the title company or law firm and confirm*** how you will transmit to them your sensitive/financial information (\*bank accounts, social security numbers, etc.). This is the critical time to confirm their *full names, titles* and *official* telephone numbers. **Ask for the Wiring Instructions at this time**, which should include the account name, ABA routing number or SWIFT code, and the account number. These instructions and numbers are the ***only*** ones you should use when calling to confirm **prior** to sending your wired funds in STEP 3. (\*NOTE: *If the designated escrow agent is not either a title company or a law firm, you should expect to receive two (2) different wiring instructions; one in the beginning from the real estate broker who is the named escrow agent, and then a second one from the title company or law firm conducting the closing. Follow these steps any time funds are to be wired.*)

**STEP 2:** **Unless you are initially provided with an encrypted email or a secure portal for your communications or wire or document transfers with the sender,** advise all participants in advance you will ***not*** respond to any email request asking for sensitive or financial information nor will you send any such information in an email attachment. If you have any questions or concerns whether the email is encrypted or the portal is secure, call to confirm prior to sending. Otherwise, advise all participants that any request for sensitive/financial information must be made in person, by mail, by phone or facsimile.

**STEP 3:** Refer to the *Wiring Instructions* you received originally from your closing agent/ attorney. **Wire Instructions do not change!** DO NOT SEND ANY WIRED FUNDS until you have called the number initially provided to you to confirm the wiring information.

**STEP 4:** NO EXCEPTIONS to Steps 1, 2 & 3.

### **BE ALERT**

If you do receive an email asking for sensitive or financial information, be alert! Below are some common ploys used by the hackers to commit cyber-wire fraud.

- **They use similar but *not exact* email addresses.**

Confirm you are responding to **exactly** the same email address.

For example:

name@michaelsaunders.com (correct), name@mihcaelsunders.com (incorrect).

client@yahoo.com (correct), client@yahoos.com (incorrect).

name@michaelsaunders.com (correct), name@michaelsaunders.net(incorrect)

name@michaelsaunders.com (correct), name.michaelsaunders@gmail.com (incorrect)

- They ask for information they should already have. (i.e. the closing date, the amount of the wire, the bank name)
- The grammar is poor or words are misspelled.
- You are addressed in a general way, not by your specific name.
- Lack of details about the transaction.
- Logos, names, and layout of an email may look similar, but are not exact.
- The name of the sender is inconsistent or does not match. (i.e. the name of sender in the body of the email does not match the exact name of the sender you have previously received original communications from in prior emails or documents; or the sender's contact information is not the same.)
- Validate the FULL EMAIL address each and every time. When you want to respond to any email, do not simply hit "reply". One option is to type in the original email address you received at the beginning of the transaction to ensure it is being sent to the correct sender. A second option is to hit "REPLY" (but DO NOT HIT SEND YET). When you select "reply," the full email address will be revealed and you can check to determine if it is exactly the same. If the email address is not correct, DELETE and do not send.

**IF YOU WERE SCAMMED OR ALMOST SCAMMED**

If you discover you have been contacted in this manner, immediately contact the closing agent, any Realtors®, your attorney, any lenders or mortgage brokers to alert them as they too might have been affected.

If you discovered you sent funds to a "fake" account, *immediately* contact the following entities/persons: 1) Your bank, to stop the transfer, if possible, 2) Your local law enforcement agency, and 3) The FBI's Internet Crime Complaint Center: <http://www.ic3.gov/default.aspx>.

\_\_\_\_\_  
Seller

\_\_\_\_\_  
Date

\_\_\_\_\_  
Print name

\_\_\_\_\_  
Seller

\_\_\_\_\_  
Date

\_\_\_\_\_  
Print name

\_\_\_\_\_  
Buyer

\_\_\_\_\_  
Date

\_\_\_\_\_  
Print name

\_\_\_\_\_  
Buyer

\_\_\_\_\_  
Date

\_\_\_\_\_  
Print name