WIRING FRAUD ADVISORY NOTICE

For use with eXp Realty® (in the United States and Canada) and eXp Commercial®

Cybercrime is a potential threat in real estate and business brokerage transactions. Instances have occurred where criminals hack into the email accounts of real estate and business brokerage transaction service providers (such as, for example, law firms, escrow companies, and financial institutions), and from these email accounts, criminals proceed to send emails containing fraudulent wiring instructions to innocent parties. These fraudulent wiring instructions direct innocent parties to deliver funds to the criminals' bank accounts (often to off-shore accounts), rather than to the legitimate bank accounts belonging to the respective service provider. Once innocent parties release their funds to the criminals' bank accounts, there is little chance that such funds will ever be recovered.

Some criminals have even established fraudulent telephone numbers, intended to be called by innocent parties if they attempt to seek verbal confirmation that the fraudulent wiring instructions are accurate. In such cases, innocent parties call the telephone number (mistakenly believing that they are calling the respective service provider), the call is then answered by the criminals, and then the criminals provide confirmation that the fraudulent wiring instructions are in fact accurate. The innocent parties, wrongly believing that they just spoke to, and received confirmation from, the respective service provider, then authorize a transfer of their funds into the criminals' bank accounts under the false impression that they are transferring their funds to the respective service provider. Don't let this be you!

EXP WILL NEVER SEND WIRING INSTRUCTIONS TO YOU REGARDING YOUR TRANSACTION

Be advised of the following:

1. You should obtain the telephone numbers of your service providers at the time that you first engage them.
2. You should never wire funds to your service providers without first calling them (*at the telephone number that you originally obtained from them*), and having them confirm that the wiring instructions you received from them are accurate (including the account number, routing number, and any other codes).
3. You should avoid sending personally identifiable information (such as social security numbers, social insurance numbers, dates of birth, etc…) in emails or text messages. It is best to provide such information in person or over the telephone directly to your intended service provider.
4. You should take steps to secure any electronic systems you are using. For example, ensure that your email account and WiFi service each contain strong passwords, and that you are opting-in to use two-step verification processes, where available.
5. If an email, telephone call, or other communication seems suspicious, follow your instincts and do *not* authorize the release of any funds without first independently confirming that the communication is legitimate. Additional information concerning how to protect yourself from and against wiring fraud may be obtained from the following sources, among others:

    - U.S. Department of Justice (Criminal Division): https://www.justice.gov/criminal/criminal-fraud/report-fraud
    - Federal Bureau of Investigation: https://www.fbi.gov/investigate/white-collar-crime & https://www.fbi.gov/investigate/cyber
    - The National White-Collar Crime Center: https://www.nw3c.org/UI/Index.html
    - On Guard Online: www.onguardonline.gov

Received, reviewed, and understood by each of the undersigned:

_____ _____ _____ _____
Date Date

_____ _____ _____ _____
Date Date

(*For Colorado Residents Only*): This form has not been approved by the Colorado Real Estate Commission.

Created by Kevin Ma with SkySlope® Forms