BEWARE WIRE TRANSFER FRAUD

Scams that target real estate transactions are on the rise and can be devastating to potential homeowners who fall prey to wire transfer fraud. Licensees are urged to warn consumers about wire fraud schemes when purchasing a home. Obviously, this is quite possible in a world where Equifax, Target, Verizon and Sony can be hacked.

Although it fortunately has a happy ending, the Commission was recently informed by a Maine licensee of a wire transfer fraud scam that almost succeeded. The scammer apparently hacked into the email account of a real estate licensee and learned details about an upcoming closing such as the parties' names, contact information, the title company involved, the closing agent, financial information specific to the transaction and the closing date.

A fraudulent email sent to the buyers made to look like it was sent by their buyer agent and directed them to wire the funds necessary to close (in this case over $70,000) to an account at a local bank. The bank account number was different from the one the buyers were previously provided but it was at the same bank and the email with new wiring instructions appeared to be from a trusted source and looked legitimate. The buyers wired the funds as directed. The fake wiring instructions were to an account controlled by the hacker and once the funds were received, they were to be diverted to an account in Dubai beyond the reach of local authorities.

The next day at the closing the scam was discovered. The real estate licensees involved quickly contacted local police and the FBI, the transfer of the funds to the offshore account was stopped just in time, and the buyers' life savings were no longer in jeopardy.

This story has a happy ending, but many do not and millions of dollars have been lost forever due to wire transfer fraud.

Licensees should alert clients that however convincing an email may appear, if it involves money-moving instructions for the closing, additional steps need to be taken before proceeding to wire funds. Clients should be advised to confirm all money transfer instructions, either in person or through a trusted and independently verified phone number (not a number listed in the fraudulent email). Licensees are reminded that good communication with their clients at the beginning and throughout the transaction will always lead to better outcomes, especially if it prevents cyber hijacking by scammers.

Other tips for licensees for keeping the transaction secure:

1. Add a standard warning to your e-mail signature that you will never discuss or ask for personal financial information via email.

2. At the beginning of the transaction discuss wire fraud scams with your clients and alert them to the dangers.
3. Avoid free Wi-Fi to prevent compromise of transaction information by hackers.
4. Use strong passwords and change them regularly. Advise clients to do the same.
5. Practice secure device management – monitor use of your electronic devices where email or transaction documents can be accessed.
6. Install and update reliable security software on all computer systems.
7. If a wire transfer is involved in a transaction, always confirm with a legitimate and verifiable source before proceeding with the wire transfer.

The threat of wire transfer fraud is real, and vigilance is the best defense.