Tips to Steer Away from Wire Fraud!

Within the real estate sector, we have almost become numb to the frequent, troubling stories we hear, and sometimes experience, when it comes to wire fraud. We know that wire fraud's presence in any closing transaction will usually not result in a pleasant outcome. The truth is that 76% of title agents reported wire fraud attempts, and a startling 71% of stolen funds in fraudulent dealings were not fully recovered. Feeling wire fraud's fury, or losing one's life savings in a bogus transaction, are both daunting realities that we must try to change, in efforts to get one step ahead of these threat actors. To avoid becoming another statistic under wire fraud's reign, it is important to educate yourself, your clients, and all other parties involved in any type of closing transaction. When you incorporate an educational piece into this mix, you are allowing yourself to be in a better security position, especially when it comes to detecting a potentially fraudulent email in the first place.

As we are aware, threat actors seeking to divert funds from a transaction can strike quickly, as their goals are dependent upon catching someone off guard in this deal. To break this cycle of falling victim to a threat actor's mischievous plans, it can benefit you if you understand these common red flags to be on the lookout for when it comes to suspicious messages:

- A sudden change in wiring instructions. This is what we like to call "Rule 101," as ***any change***, whether it relates to the payoff amount or bank, can indicate that something is amiss with this deal.

- Senses of urgency. Standards like "I need this ASAP," or "move quickly to avoid closing delays," are typically featured in wire fraud cases. We see this hurrying nature, because when people are in a rush or simply not thinking, irrational behaviors can form.

- Check for misspellings, odd sentence structure, punctuation issues, etc. Sometimes the sender's language can simply be "off" in the email.

- Remain watchful when it comes to spoofing.
    - For example, the attorney's legitimate email is JSmithattorney@smithlawctllc.com, but you receive an email from Jsmithattorneyct@gmail.com. These slight changes to the email address are repeatedly realized when it is too late.

Statistics were derived from blog.alta.org.

Please contact CATICITSecurity@catic.com if you have any questions.