BEWARE OF BUSINESS EMAIL COMPROMISE - IT COULD COST YOU!

If you are in the real estate industry, you probably know someone who has gotten the call – or unfortunately, you may have gotten the call. Sometimes the homebuyer is the victim; other times it is the sales agent or title company. In any case, the calls always end the same: "Wait what? Are you telling me that they wired $50,000 to some hacker? What do we do now? How do we stop this from happening again?"

Business email compromise scams target companies and industries, like real estate, that regularly transfer funds via wire. To protect yourself and your customers, the FBI recommends increased awareness and understanding.

Some specific recommendations include:

- Avoiding free web-based email accounts- Establish a company domain name and use it to establish company email accounts in lieu of free, web-based accounts
- Considering additional IT and financial security procedures, including the implementation of a two-step verification process
- Immediately reporting and delete unsolicited email (spam) from unknown parties- DO NOT open the spam email, click on links in the email, or open attachments. These often contain malware that will give subjects access to your computer system.
- Being aware of sudden changes in business practices- For example, if a current business contact suddenly asks to be contacted via their personal email address when all previous official correspondence has been through company email, the request could be fraudulent. Always verify via other channels that you are still communicating with your legitimate business partner.
- Confirming requests for transfers of funds- When using phone verification as part of two-factor authentication, use previously known numbers, not the numbers provided in the email request.
- Scrutinizing all email requests for transfers of funds to determine if the requests are out of the ordinary

If you or someone involved in the transaction falls victim to a scam, you need to move quickly, as the longer you wait, the less chance there is to recover the funds. The FBI recommends that you:

- Contact your financial institution immediately upon discovering the fraudulent transfer
- Request that your financial institution contact the corresponding financial institution where the fraudulent transfer was sent
- Contact your local Federal Bureau of Investigation (FBI) office if the wire is recent. The FBI, working with the United States Department of Treasury Financial Crimes Enforcement Network, might be able to help return or freeze the funds
- File a complaint, regardless of dollar loss, at www.IC3.gov

For more tips from the FBI on how to avoid being a victim, and what to do if you get scammed, go to www.justice.gov and look at the publication titled "Best Practices for Victim Response and Reporting of Cyber Incidents."

HELPING YOU SHINE BRIGHT