Real Estate Scams - Impersonations

This is an update to our "Real Estate Scam-Vacant Properties" Advisories (v 1.1) that was issued in the Spring of 2022. This scam has evolved, and the U.S. Secret Service has become aware of an increase of instances where criminals are impersonating title companies to steal real estate transactions (buyers deposits, closing funds, escrow payments, etc.). Now more than ever, it is important for Realtors, Transaction Coordinators, Lenders, Mortgage Brokers, Property Owners, and even Prospective Buyers to validate these financial transactions before they're sent.

Criminals are using similar techniques that continue to be deployed in real estate specific Business Email Compromise (BEC) schemes. Visit the U.S. Secret Service website for guidance on BEC schemes and other cyber-enabled financial crimes.

THE SCHEME

- The criminal impersonates a real property owner to negotiate a contract to sell vacant/unoccupied property to an unsuspecting buyer.
- Once the contract is signed, the criminal directs the realtor(s)/buyer to use the criminal's "preferred" title company to handle the closing (i.e. criminal impersonating a title company).
- The criminal impersonates a real title company by purchasing fake domain(s) similar to a real title company's domain (Ex: www.titlecollc.com vs. www.titleco.com).
- The criminal introduces the realtor(s)/buyer to their preferred title company via email (Ex: me@titlecollc.com vs. me@titleco.com).
- Criminal provides wire instructions for the impersonated title company to the buyer (i.e. criminal's fraudulently created bank account).
- Buyer sends their funds to purchase the property to the fraudulently created bank account.

RED FLAGS

- Communication is primarily by email and commonly contains poor grammar.
- Wiring instructions are sent over standard email instead of a secure email platform.

- Pressuring the buyer to wire money urgently and in advance of the expected closing date.
- The listing is vacant land or a 'second home' where the owners are out of state/country.
- The listing is below market value with the 'seller' looking for a cash buyer or quick closing.
- The 'seller' wants to use their own 'title company' and it's out of the area where the property is located.

PREVENTION

BUYERS & REALTORS

- Conduct an online/independent search of the 'title company'.
- With a known phone number (from a trusted website/previous contact), call and verify name/email address of the title company contact(s) to confirm legitimacy.
- If possible, visit a local physical branch of the 'title company' to confirm validity.
- Contact the bank on the wiring instructions to confirm the name on the account.

REALTOR SPECIIFC

- Obtain a copy of a government issued ID from any 'seller' and evaluate for abnormalities.
- Use credible realtor safety applications to confirm identity.
- Contact the bank on the wiring instructions to confirm the name on the account.
- Consider a form of multi-factor authentication with your clients, for example: Sending an overnight letter to the mailing address on the tax bill asking the property owner to call you with a one-time code embedded within the letter to confirm the sale.

This article is a re-printing of the United States Secret Service - Cybercrime Investigations' article (2024-09) on Real Estate Scams - Impersonation, attached in the Related Files section of this article.