TitleNews Online Archive

Wire Fraud Advisory: Vacant Property Fraud

January 24, 2023

Real estate transactions have been a prime target of cybercrime over the past decade, and there is little sign of change in this focus, even as the housing market slows. Instead, fraudsters continue to evolve their scam and money laundering tactics to avoid detection.

The latest trend involves vacant lots or unencumbered properties. These scams involve bad actors posing as owners of these vacant lots or properties. CertifID has worked recently with federal law enforcement on numerous of these cases.

This trend began to emerge before the winter holidays. A title agency in North Carolina reported to us a loss of $33,000 from a vacant lot transaction. The title agency and the real estate agent were scammed by an imposter seller. Luckily, it was reported quickly, and we were able to work with the U.S. Secret Service to freeze and return the funds.

According to the National Association of Realtors (NAR), **home sales continued to fall** for the 10th month consecutively in November. As a result, cybercrime rings have turned to new tactics to make up for the lower housing market transaction volume that they can target. Here's how these new vacant property scams work:

- Public records are searched to identify real estate that is free of mortgage or other liens. These often include vacant lots or rental properties. The identity of the landowner is also obtained through this public records search.
- Posing as the property owner, the scammer contacts a real estate agent to list the property for sale. All communications are through email and digital means and not in person.
- The listing price of the property is typically below the current market value to generate immediate interest in the property.
- The scammer quickly accepts the offer, with a preference for cash sales.
- At the time of closing, the scammer refuses to sign documents in person and requests a remote notary signing. The scammer impersonates the notary and returns falsified documents to the title company or closing attorney involved in the transaction.
- The title company or closing attorney transfers the closing proceeds to the scammer. The fraud is typically not discovered until the time of recording of transferring documents with the applicable county.

Another recent case with one of our title company customers in Ohio followed this playbook almost perfectly. The "seller" of a vacant lot contacted the real estate agent online, with no previous connection. The "seller" was very pushy about transferring money and the amount they'd make. They claimed to owe

more than the $30,000 sale value and were anxious to receive the funds. There were many other markers of fraud identified during the CertifID verification process. Luckily, due to all of these red flags, the fraud was detected and stopped in time.

All title companies should protect themselves and their clients from this latest scam by doing the following:

- Independently search for the identity and a recent picture of the seller.
- Request an in-person or virtual meeting to see their government issued identification.
- Be on alert with a seller accepting an offer price below market value in exchange for the buyer paying cash and closing quickly.
- Never allow a seller to arrange their notary closing. Use a trusted title company or closing attorney to coordinate the exchange of closing documents and funds.

Another title company customer in Florida avoided a sizable $110,000 fraud loss due to these clues. A "seller" living in Vermont contacted a real estate agent online to list a vacant lot. The listing came from a real estate agent that the title company knew and trusted. However, red flags were identified by the CertifID verification process. And the "seller" asked to use their own notary due to being out of state. Luckily, this too, was detected and prevented in time.

The best way to limit your exposure is to supplement your teams' efforts with a solution that can verify wire instructions before any funds are sent. The human eye will not catch every spoofed email address or web domain. Having a solution that reduces your risk by using a combination of software, services, and insurance is a more comprehensive approach.

CertifID's **Fraud Recovery Services** are available to help if you or your client have been hit. The team provides a single point of contact, so you don't have to be alone in navigating across the multiple parties, including banks and law enforcement, who need to work together during a recovery process.

Tom Cronkright, CEO of Sun Title and executive chairman of CertifID, can be reached at ***tcronkright@certifid.com****.*

ALTA Resources

- **ALTA Wire Fraud Video:** This 2-minute video provides four tips on how consumers can protect their money and offers advice on what to do if they have been targeted by a scam. Link to this video from your website, include in your email or share on social media.
- **ALTA Wire Fraud Infographic**: ALTA has produced this Rack Card explaining Wire Fraud. ALTA members can brand the infographic with their own information **here**.

Contact ALTA at 202-296-3671 or ***communications@alta.org****.*