Fraud Greater Concern Than Ever During the Pandemic

Description

The exploding real estate market, which has coincided with a once-in-a-century pandemic has increased the likelihood of fraud.

Mortgage â??phishingâ?•, in which a party receives an email with a fraudulent link is becoming ever more common. This is how it works: An emailed link is sent to a borrower or real estate agent requesting personal information such as bank account information, or requesting a change in wire instructions while indicating that transaction funds should be wired to a different account, which turns out to not be owned by any of the parties participating in the real estate transaction. Responding to this type of phishing email can result in identity theft, misappropriation of funds from bank accounts, or loss of funds through wire fraud. Real estate related wire fraud as recently as 2018 had increased 166% versus 2017, with 11,300 reported victims in the United States losing $149 Million. Moreover, it is estimated that only 12-15% of all wire fraud is reported (FBI Data). Additionally, various law enforcement data suggest phishing scams will increase by over 1000% in the coming years.

Global organizations and corporations are experiencing various types of phishing attacks at an exponentially increased rate and are having to spend more time and resources defending themselves and educating their employees and systems users.

Cyber criminals are becoming more sophisticated in methods of penetrating the real estate market, utilizing various types of phishing related emails. The goal of these types of activities is generally to create an entry point to observe the home buying process and intercept information along the way. Hackers often â??followâ?• email traffic relating to a particular real estate transaction, waiting until a file is ready to fund. At that point, they insert fraudulent wire instructions into the communication stream. By collecting pertinent information such as the name of the title company, real estate agent, transaction partiesâ?? names, addresses, personal information, and lenders, fraudsters can effectively and convincingly mimic the various parties and effectively manipulate individuals to wire funds to fraudulent accounts.

Naturally all real estate transactions are at risk for this type of fraud, however first-time homebuyers are often most vulnerable to these schemes. Although real estate professionals are becoming more cognizant of these scams and are more vigilant in detecting phishing emails, the threat remains. During this current period of high transaction volume real estate professionals prove to be just as vulnerable as their clients, as they are often working on files at the last minute, and lose the ability to thoughtfully and carefully review changes to wire instructions. This â??last minuteâ?• culture within the real estate industry increases the risk of becoming a victim of wire fraud.

For example, it is not uncommon to see a senior managerâ??s email account hacked and fraudulent account information provided in an email between the senior manager and his/her assistant who is working directly with the escrow agent during the final stages of a transaction. This is very difficult to detect, as the assistant is acting in good faith by verifying the account information for the escrow account holder.

Finally, it is important to remember that the â??theftâ?• is only a part of the total loss potentially incurred from a fraudulent transaction. There may be additional losses due to legal expenses, time spent investigating the fraud, and it can be financially devastating to businesses and reputations. Fraudsters are always actively looking to take advantage of opportunities and vulnerabilities, and it is important to identify those risks within your agency and take steps to protect yourself and your customers from the risk of wire fraud.

Tips:

- Contact businesses involved in the transaction in person or use a known or independently verified phone number.
- Always independently verify links. Never click on unfamiliar links in emails, texts or websites. Fraudsters attempt to lure victims to websites to download malicious software, which gives them access to personal information.
- Be cautious of new business opportunities coming to your office seemingly out of nowhere.
- Protect your company and customers with compliant, secure technology.
- Be suspicious of unsolicited phone calls or emails claiming to be associated with your bank, servicer, or mortgage company, even when they appear to come from a trusted source.
- Inform your customers to be on the lookout for fraudsters who may attempt to replace valid wire instructions with false instructions and documentation.
- Reduce risk by always using secure email and following established security procedures and protocols.
- Utilize secure disbursement practices to help avoid misappropriation and theft of escrow funds.

More information:

Business email compromise fraud has resulted in $26 billion in losses since July 2016, according to research released by the FBI, making it one of the costliest cybercrimes against businesses. Read More at: https://www.cnbc.com/2019/09/11/email-wire- fraud-cost-26-billion-since-2016-says-fbi.html

$221M Lost to Wire Transfer Fraud in 2019â?? According to the FBI, incidents and losses due to real estate wire fraud continue to increase, and only 15 percent of all wire fraud incidents are reported. The FBI reported the Internet Crime Complaint Center (IC3) received 467,361 complaints in 2019â??an average of nearly 1,300 every dayâ??and recorded more than $3.5 billion in losses to individual and business victims. Read More at: https://www.alta.org/news/news.cfm?20200218-WTF-221M-Lost-to-Wire-Transfer-Fraud-in-2019

Download a copy of the FBI 2019 Internet Crime Report: https://pdf.ic3.gov/2019_IC3Report.pdf

Kenneth N. Smolar
Esq., President, PCN Network
Courtesy of Safe Escrow and TitleExpress

Category

1. Cybersecurity
2. Uncategorized

Date Created
2020/12/03
Author
vltaexaminer