Homebuyers

Beware of Wire Fraud and Other Cyber Crimes

VETERAN
Loan #: **UAT.72-107407A**
MIN: **100057400002127514**

DATE: **OCTOBER 5, 2018**
LENDER: **PULTE MORTGAGE LLC**
BORROWER NAME: **JACIE TEST VETERAN**
PROPERTY ADDRESS: **478 GREENWAY CIR**
ALAMO, CA 94507

Buying a home is an exciting time so it is important to be careful not to let cyber criminals turn your dream experience into a nightmare.

We have all seen headlines about cybercrime and companies and individuals who have been hacked. Like many industries, the real estate industry has seen a significant increase in cybercrime. The risk is growing as criminals find new ways to obtain information pertaining to real property transactions in an effort to divert and steal funds through malicious wire fraud schemes.

Cyber criminals typically begin their fraudulent schemes long before the attempted theft occurs. They often begin with a common technique called "phishing". This can take the form of email messages, fake websites or phone calls to fraudulently obtain your private information. Through a seemingly harmless communication, criminals trick people into inputting their information or clicking a link that allows hackers to steal computer or email logins and passwords.

Once hackers gain access to an email account, they will monitor messages to find someone in the process of buying a home. The hackers may be experts in real estate transactions. The criminals may hack various parties involved in the home buying transaction, including homebuyers, real estate agents, lenders, title companies or attorneys. Then, around the time the homebuyer is supposed to wire funds for their home purchase, the homebuyer receives what seems like a perfectly normal email apparently from a professional associated with the transaction. This email will include wiring instructions for wiring funds to a fraudulent account. If you take the bait and wire funds to a fraudulent account, your money could be stolen.

Please take precautions so you won't become a victim of cybercrime. Be careful to protect your personal information and passwords. Do not send sensitive information using unsecure email. Do not click on links or attachments in unsolicited emails.

Here are some tips from the Federal Bureau of Investigation (FBI) to protect against wire fraud and other cybercrimes:

1. **Call, don't email:** Confirm by phone all wiring instructions you receive before transferring funds. Use a phone number for the title company that you obtain from a trusted source.
2. **Be suspicious:** Carefully scrutinize all email requests for information or transfers of funds to determine if the emails appear out of the ordinary. It's not common for title companies to change wiring instructions and payment information.
3. **Confirm everything:** Ask your bank to confirm not just the account number but also the name on the account before sending a wire transfer.
4. **Verify immediately:** You should call the title company or your real estate agent to verify your funds were received by the title company or other proper party. Detecting that you sent money to a wrong account within 24 hours may give you the best chance of recovering your money.
5. **Forward, don't reply:** When responding to an email, hit forward instead of reply and then start typing in the person's email address. Criminals use email addresses that are very similar to the real one for a company. By typing in email addresses, you will ensure the intended recipient's correct email address is used.

If you discover that you have been a victim of wire fraud or another cybercrime, immediately contact your financial institution and notify the FBI or other law enforcement authorities. If the fraud or crime involves a real estate transaction, be sure to contact the title company, settlement agent, escrow agent or attorney handling the transaction.