

# SHARE THIS CONSUMER ALERT: BEWARE OF WIRE FRAUD SCHEMES WHEN BUYING A HOME

Buying a home is an exciting time. You've saved, found the perfect home and planned the move. Now, the closing day for your home is just around the corner.

The American Land Title Association wants to make sure your home purchase doesn't get derailed by a dangerous threat that could keep you from getting the keys, painting walls and decorating. Criminals have stolen money meant for the purchase of homes through malicious wire fraud schemes targeting consumers across the country.

Criminals begin the wire fraud process way before the attempted theft occurs. Most often, they begin with a common social engineering technique called phishing. This can take the form of email messages, website forms or phone calls to fraudulently obtain private information.

Through seemingly harmless communication, criminals trick users into inputting their information or clicking a link that allows hackers to steal login and password information.

Once hackers gain access to an email account, they will monitor messages to find someone in the process of buying a home. Hacks can come from various parties involved in a transaction, including real estate agents, title companies, attorneys or consumers. Criminals then use the stolen information to email fraudulent wire transfer instructions disguised to appear as if they came from a professional you're working with to purchase a home. If you receive an email with wiring instructions, don't respond. Email is not a secure way to send financial information. If you take the bait, your money could be gone in minutes.

"Attorneys and title companies have taken many steps to combat this problem, such as putting consumer warnings on websites and communications, securing email communications and sending notices to consumers and real estate agents informing them of the scams," said Michelle Korsmo, chief executive officer of the American Land Title Association. "But the criminals are smart and constantly alter their tactics to steal information and money.

"Everyone involved in real estate transactions must also be aware of the potential losses as criminals phish for information and stalk home closings, hoping someone makes a mistake. If someone does mess up, it could cost your savings or retirement."

## HERE ARE FIVE TIPS TO PROTECT AGAINST WIRE FRAUD:

1. Call, don't email: Confirm all wiring instructions by phone before transferring funds. **Use the phone number from the title company's website or a business card.**
2. Be suspicious: title companies DO NOT CHANGE wiring instructions and payment info
3. Confirm it all: Ask your bank to confirm not just the account number but also the name on the account before sending a wire.
4. Verify immediately: You should call the title company or escrow to validate that the funds were received. Fraud can all happen within a matter of a few hours - be vigilant and contact your title company IMMEDIATELY to verify funds were received. **Use the phone number from the title company's website or a business card.**
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 make it easier to discover if a fraudster is after you. **DO NOT ACCEPT, REPLY OR FORWARD OPEN PLATFORM EMAILS. i.e. gmail, yahoo, cox, etc.**

**Customer Service** cs@caltitle.com | 844.544.2752

**Los Angeles** 100 N. First Street, Suite 404 | Burbank | 818.382.9889

**Orange County** 28202 Cabot Road, Suite 625 | Laguna Niguel | 949.582.8709

**San Diego** 2355 Northside Drive, Suite 310 | San Diego | 619.516.5227



*Protecting Your Property Rights*



[WWW.CALTITLE.COM](http://WWW.CALTITLE.COM)

The information contained herein is deemed to be reliable, but it is not guaranteed. California Title Company assumes no responsibility for errors or omissions. Images may be subject to copyright. A ©2018 California Title Company.