Best Practices for Preventing Real Estate Wire Fraud

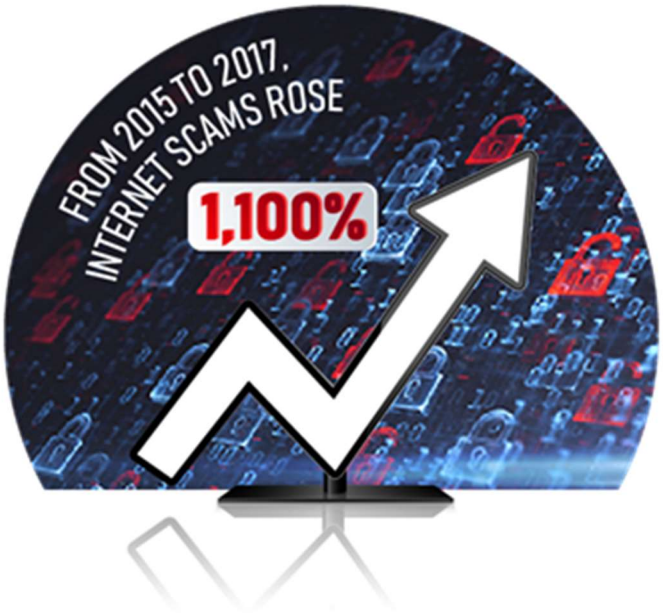
October, 2021

Imagine saving for years to buy a home. After a long search, you find the perfect property, make an offer and it's accepted. As closing day draws near, you receive an urgent email from someone who purports to be your closing agent/attorney containing pre-closing instructions. You open an attachment to see the address of the home, the name of your title insurance company, the exact dollar amount due from you at closing and detailed wire instructions – all signed by the individual on company letterhead. Someone who claims to be their assistant even calls to make sure you received the message. So you have your bank wire the funds due to the account listed in the wire instructions. When you show up at closing, however, you find you were duped out of your five-figure down payment and your closing on that dream home is cancelled.

Scenarios like this are playing out across the globe at an alarming rate.

According to the Federal Bureau of Investigation (FBI), over **13,638 victims lost $213 million** to real estate wire fraud in 2020. The scheme, called **business email compromise**, involves fraudsters who use deceptive techniques to hack the email account of one or more of the parties involved in the real estate transaction. The cybercriminal then monitors the email traffic and gathers transaction details and graphics to send spoofed communications that look real, but direct buyers to wire funds into the fraudster's account. Too often, unsuspecting victims don't realize their money is gone until it's too late to get it back.

It's easy to be fooled by cybercriminals if you let your guard down, but with knowledge and preparation, you can avoid becoming a victim.



Tips for Preventing Wire Fraud

- **Secure your devices and accounts.** Securing your computer, phone and mobile devices, and practicing good email and password hygiene can make you less vulnerable to any cybercrime.
  Click **here** for best practices.
- **Be vigilant.** All parties to a real estate transaction are potential targets. However, cybercriminals tend to prey on older buyers who they believe may have limited knowledge of cybersecurity or wire transfer protocols.
- **Consider using cashier's checks instead of wiring funds.** Your title company can verify checks with the bank prior to funding, which satisfies Good Funds requirements and eliminates your risk of wire fraud.
- **Learn your title company's process for wiring funds.** Many companies have policies against emailing wiring instructions. Ask your closing agent for a list of approved contacts and wiring instructions at the beginning of your transaction. Keep them handy to use as a reference.
- **Slow down.** Fraudsters work hard to lull buyers into a false sense of security, so they don't take the time to scrutinize requests. Always check the sender's email address for irregularities. When responding to an email, use "forward" instead of "reply." Typing in a trusted email address lowers your chance of accidentally replying to the cybercriminal that sent you a spoofed email.
- **Be suspicious of any changes to wiring instructions, especially on Fridays or before holidays.** Changes to wiring instructions are rare and should only come from your closing agent. Since it takes 72 hours to wire money, fraudsters often request wire changes on a Friday or just before a holiday, so the funds are

gone by the time anyone notices. There is little your financial institution can do to recover funds once they are wired into a new account.

For more tips and resources for preventing wire fraud, visit **https://stopwirefraud.org/**.

If You Think You Might Be a Victim of Wire Fraud

If you recently complied with a request to change wiring instructions without calling a trusted source to verify the request, you could be a victim of wire fraud and need to act immediately. **Click here to learn more.**