

# protect yourself **FROM WIRE FRAUD**

Wire fraud is raging, reaching historic levels in the U.S. and abroad. The FBI has reported an explosive increase in wire related fraud. In 2016, the FBI reported \$19 million in wire fraud associated with the home buying process, but 2017 paled that number, with over \$1 billion in reported losses, and the numbers continue to grow.

Buyers and Sellers must remain aware and proceed with caution.

## **Buyers & Sellers: Take Action!**

Here are some actions consumers can take to help prevent wire fraud from happening in the first place.

- ✓ **Talk to your real estate agent** to learn about the process. Know who you will be working with at the escrow office, and how to reach them.
- ✓ **Follow the security protocols** established by your lender and escrow office. Encrypted email has become a very common tool. It takes an extra moment or two to receive important communications, but they can be better trusted.
- ✓ **Call the recipient of the funds** before you send the wire, using the phone number you have previously verified as correct.
- ✓ **Beware of last-minute changes!** Never trust an email which contains a last-minute change to wiring instructions for your closing. Such a change is extraordinarily rare, and should be met with heightened suspicion. Call the closing office at a trusted phone number, and not the phone number provided in the notice of change.
- ✓ **Never send your sensitive or financial information over a standard email** or enter it in an unknown website – it is not safe.

## **ADDITIONAL SECURITY MEASURES**

**Here are some additional security tips that everyone can use when conducting sensitive financial transactions.**

- Keep a constant check on your email account, especially rules and tools for forwarding emails.
- Enable a two-factor authentication to access your email account (password plus a verification code).
- Practice secure password management. Use different and complex passwords (including letters, numbers and symbols) for different accounts. Otherwise, the compromise of your single password will act as a master key to every account you own. (There are multiple password securing services available to hold the variety of information).
- Do not rush. Read all emails carefully, and trust your instincts if something seems off. Don't log in to websites through links provided in emails sent by others. Go to a website directly if you need to log in to your account. Do not open unexpected attachments, which can contain malware or spyware.

