Third Quarter 2018

Wire Fraud Is Becoming Increasingly Common, *Particularly in Real Estate Transactions*

When it comes to moving money and even making payments, caution is essential! One of the latest frauds involves wire transfers, in particular, wire transfers made to title companies to close on real estate transactions.

Wire fraud has become the fastest-growing form of real estate cybercrime in the United States. Hackers access the title companies' computers and records of upcoming home closing or intercept outgoing emails and then email fraudulent wire transfer instructions to buyers. The email references the title company employees the buyers have been working with and even includes phone numbers (direct to the hacker) to verify instructions. Even the email address may appear to be from the title company. Once the money is wired, there is little the buyers can do to retrieve their funds. The purchase collapses and the buyers lose not only their down payments but also potentially earnest money and the upfront expenses they have incurred as part of the purchase.

Ironically, wiring money is often required in the home buying process because cashier's checks have become subject to fraud. Using a mobile banking app, unscrupulous buyers can re-deposit a check into their own accounts just before handing it over to the title officer. The title company may not be notified of the bad check for days or even weeks.

Given the title company requires a wire transfer, how do you protect yourself?

(1) Do not assume that the email you receive with instructions is legitimate. Call the title company – using phone numbers you have obtained in person or on verified paperwork - to verify that the wire instructions you've received are correct.

(2) Consult your real estate agent. They deal with the title companies and closing requirements on a regular basis and may be able to arrange acceptance of a cashier's check or assure wire transfer instructions are correct. It is in their best interest that your real estate purchase is successful.

IF YOU MAKE A FRAUDULENT WIRE TRANSFER, in some cases, particularly, if the bank still holds the transfer amount, you can attempt to reverse it. If the money has transferred, it is gone. You have no recourse, no recovery options.

Businesses are also targets for wire fraud. A common tactic is to gain access to legitimate email communications and then mimic familiar business transactions. Individuals who use free, web-based email accounts - which are more susceptible to being hacked - for business transactions are more vulnerable to wire fraud. Telephone solicitations for payment via wire transfer should always be considered suspect.

General precautions to follow include:

- Verify changes in vendor payment location and confirm requests for transfer of funds.
- Obtain wire transfer instructions directly from the business and DO NOT assume email instructions are legitimate.
- Call a number you know is legitimate and confirm before making payments.
- Be suspicious of requests for secrecy or pressure to take action quickly.

Like it or not, YOU ARE A TARGET for increasingly sophisticated scammers and thieves. Protecting your money and your assets is up to you. Any time you are asked to make an instantaneous transfer of funds – whether through wire transfer, by providing your checking account information, a cashier's check or cash – the odds are very high that you are about to be scammed.

Brian R. Carruthers, CFP, CMT

BCA
BRIAN CARRUTHERS & ASSOCIATES

Your Conservative Advisory Firm Since 1990
301 Forest Avenue
Laguna Beach, California 92651-2115 USA
Telephone: 1-949-464-1900
www.gobcafunds.com
brian@gobcafunds.com