GARY R. HERBERT
Governor

SPENCER J. COX
Lieutenant Governor

State of Utah
Department of Commerce
Division of Real Estate

FRANCINE A. GIANI
Executive Director

THOMAS BRADY
Deputy Director

JONATHAN C. STEWART
Real Estate Division Director

May 25, 2016

MEDIA ALERT

Division of Real Estate warns email scam stealing loan proceeds in wire fraud

“Fraudsters sending convincing emails to divert real estate funds to their accounts”

(For immediate release…)

SALT LAKE CITY, Utah – Francine A. Giani, Executive Director of the Utah Department of Commerce, announced today that the Utah Division of Real Estate is warning Utah consumers to be on the alert for a real estate scam that targets property transactions through phony emails to coerce respondents into wiring loan transfers and other high dollar real estate amounts to con artists’ accounts. According to the Federal Trade Commission, this scam has been around since 2012 but has recently resurfaced in some states.

“Similar to IRS scams, these real estate scams may travel state-to-state seeking new victims. Please carefully review any email messages regarding your property transaction and if there is any doubt, contact your real estate agent or mortgage broker to verify before releasing any information or funds,” advised Francine A. Giani.

While Division investigators have not received reports of this fraud occurring in Utah, the National Association of Realtors (NAR) has released media alerts regarding the wiring instruction scam that has caused practitioners and members of the public to lose earnest money, closing costs, down payments, and in some cases, loan proceeds.

“All parties in a real estate transaction should be wary of email communication especially if last minute changes are requested, “stated Jonathan Stewart, Director of the Utah Division of Real Estate, “If criminals have access to your email account, they can make anything sound legitimate.”

According to the NAR, this scam starts with a con artist gaining access to an email account by either hacking or obtaining login credentials through a phishing scheme. Once they have access to an email account, they monitor emails about a pending real estate transaction until the transaction is about to close. Typically within 24 hours of a transaction closing, they will use the email account to send new wiring instructions to the buyer, seller, title or escrow agent, lender, real estate agent or broker, etc. The new wiring instructions often have the money going to a bank account outside of the

UTAH
LIFE ELEVATED

country. By the time the fraud is recognized, the money has already been withdrawn from the fraudulent bank account and it is too late to locate the criminal.

<u>Tips for Real Estate Consumers</u>

1. Be wary of last minute emails with changes to the transaction.
2. Contact email senders by telephone using a phone number you have independently verified.
3. Never send wire transfer information via email. For that matter, never send any sensitive information via email, including banking information, routing numbers, PINS, or any other financial information.
4. Do not email financial information. It's not secure.
5. If you're giving your financial information on the web, make sure the site is secure. Look for a URL that begins with https (the "s" stands for secure). And, instead of clicking a link in an email to go to an organization's site, look up the real URL and type in the web address yourself.
6. Be cautious about opening attachments and downloading files from emails, regardless of who sent them. These files can contain malware that can weaken your computer's security.
7. Keep your operating system, browser, and security software up to date.

<u>Tips for Real Estate Professionals</u>

1. Inform clients from day one about your email and communication practices, and alert them to the possibility of fraudulent activity. Explain that you will never send, or request that they send, sensitive information via email.
2. Prior to wiring any funds, the wirer should contact the intended recipient via a verified telephone number and confirm that the wiring information is accurate. Do not rely on telephone numbers or website addresses provided within an unverified email, as fraudsters often provide their own contact information and set up convincing fake websites in furtherance of their schemes.
3. If a situation arises in which you have no choice but to send information about a transaction via email, make sure to use encrypted email.
4. Security experts often recommend "going with your gut." Tell clients that if an email or a telephone call ever seems suspicious or "off," that they should refrain from taking any action until the communication has been independently verified as legitimate. When it comes to safety and cybersecurity, always err on the side of being overly cautions.

5. If you receive a suspicious email, do not open it. If you have already opened it, do not click on any links contained in the email. Do not open any attachments. Do not call any numbers listed in the email. Do not reply to the email.
6. Clean out your email account on a regular basis. Your emails may establish patterns in your business practice over time that hackers can use against you. In addition, a longstanding backlog of email may contain sensitive information from months or years past. You can always save important emails in a secure location on your internal system or hard drive.
7. Change your usernames and passwords on a regular basis, and make sure your employees and licensees do the same.
8. Never use usernames or passwords that are easy to guess. Never, ever use the password "password."
9. Make sure to implement the most up-to-date firewall and anti-virus technologies in your business.

For more information on real estate fraud and how to avoid becoming a victim, contact the Utah Division of Real Estate by logging on to www.realestate.utah.gov or by calling 801-530-6747.

For media enquiries contact:
Jennifer Bolton
Public Information Officer
Utah Department of Commerce
(801) 530-6646 office
(801) 652-8322 cell
jenniferbolton@utah.gov
Follow us on Twitter @UtahCommerce