Beware of Real Estate Wire Transfer Scams

District consumers should beware of real estate wire transfer scams, warns the District of Columbia Department of Insurance, Securities and Banking (the Department).

The following is an example of the scam. District homebuyers John and Catherine were eagerly awaiting closing on the purchase of their dream home. They believed they were one step closer to making their dream a reality when they received an email from their title company instructing them to immediately wire $400,000—the balance of their purchase price—to the title company's account number. When John and Catherine arrived at the offices of the title company for their scheduled closing five days later, an attorney for the title company told them that the funds they thought they had wired to the title company's account were never received. Sadly, John and Catherine soon discovered that their $400,000 wire transfer ended up in a hacker's U.S. bank account. The hacker immediately wired the funds from his account to an offshore bank, never to be recovered.

Unfortunately, this scenario has become all too common as title companies and real estate professionals increasingly rely on electronic mail to provide real estate purchasers and sellers with wire transfer instructions in advance of their closings. The real estate wire transfer scam is carried out by sophisticated hackers who send phishing emails containing malware to employees of title companies and real estate professionals. When the employees click on the links provided in those emails, it gives the hacker access to email accounts. Once inside the compromised system, the hacker obtains information about upcoming real estate transactions. After determining the closing dates, the hacker poses as the real estate professional or the title company representative and sends an email to the purchaser. The phony email advises that there has been a last-minute change to the wiring instructions and directs

Issued: *August 12, 2019*

the buyer to wire the balance of the closing costs to a different account (i.e., the hacker's account).

The Federal Trade Commission and the National Association of Realtors® have warned home buyers about the email and wire transfer scam. If you are buying a home and get an email with money-wiring instructions, **STOP**. Email is not a secure way to send financial information, and your real estate professional or title company should know that.

To avoid wire transfer scams:

- Do not email financial information. Email is not secure. Also, never follow wire instructions sent to you by email.
- Meet in person with your trusted real estate professional or title company representative to discuss financial information and to verify the account name and number where your money should be wired. Be suspicious of any email, text message, or telephone call advising you of a last-minute change to the account number that was provided to you by the title company for your wire transfer.
- Be cautious before opening attachments, clicking on email links, or downloading files from emails, regardless of who appears to have sent them. These files may contain malware that can weaken or compromise your computer's security.
- Keep your operating system, browser, and antivirus software up to date.
- If you suspect that you unknowingly wired money to a scammer, contact your financial institution immediately and request a wire recall.
- For additional tips, visit IdentityTheft.gov.

If you believe you have been a victim of a financial scam or have questions, please contact the Enforcement and Consumer Protection Division of the District of Columbia Department of Insurance, Securities and Banking at 202-727-8000.