RISK INSIGHTS

TPG
THE PLATINUM GROUP
Delivering More!

Wire Fraud in Real Estate

No industry is exempt from cyber crime, and the real estate industry has become a common target. As hackers devise plans to obtain sensitive information about real estate transactions, real estate professionals need to take particular interest in cyber security to protect their clients and themselves from wire fraud.

What is Wire Fraud?

In instances of wire fraud, a common ploy involves hackers breaking into a real estate agent's email account to obtain details about upcoming transactions. Once the hackers have all the information they need, they send an email to the buyer, pretending to be the agent or a representative of the title company.

In an email to the buyer, the hackers state that there has been a change in the closing instructions and that the buyer needs to follow new wire instructions listed in the email. If a buyer falls victim to the scam and wires money to the fraudulent account, they're unlikely to see the money again.

Red Flags

A potential indicator of wire fraud is an email that makes any reference to a Society for Worldwide Interbank Financial Telecommunication (SWIFT) wire transfer, which is sent via the SWIFT international payment network and indicates an overseas destination for the funds.

However, since the emails tend to include detailed information pertaining to the transaction—due to the perpetrator having access to the agent's email account—many people make the mistake of assuming the email is from a legitimate source. The email addresses often appear to be legitimate, either because the hacker has managed to create a fake email account using the name of the real estate company or because they've hacked the agent's actual email account.

How to Avoid It

Wire fraud is one of many types of online fraud targeting real estate professionals and their clients. To prevent cyber crime from occurring, every party involved in a real estate transaction needs to implement and follow a series of security measures that include the following:

- Never send wire transfer information, or any type of sensitive information, via email. This includes all types of financial information, not just wire instructions.
- If you're a real estate professional, inform clients about your email and communication practices, and explain that you will never expect them to send sensitive information via email.
- If wiring funds, first contact the recipient using a verified phone number to confirm that the wiring information is accurate. The phone number should

> A number of unsuspecting homebuyers are losing large sums of money due to a wire fraud scheme targeting the real estate industry.

be obtained by a reliable source—email is not one of them.

- If email is the only method available for sending information about a transaction, make sure it is encrypted.
- Delete old emails regularly, as they may reveal information that hackers can use.
- Change usernames and passwords on a regular basis, and make sure that they're difficult to guess.
- Make sure anti-virus technology is up to date, and that firewalls are installed and working.
- Never open suspicious emails. If the email has already been opened, never click on any links in the email, open any attachments or reply to the email.

If You've Been Hacked

Take the following steps if you suspect that your email, or any type of account, has been hacked:

- Immediately change all usernames and passwords associated with any account that may have been compromised.
- Contact anyone who may have been exposed to the attack so they too can change their usernames and passwords. Remind them to avoid complying with any requests for financial information that come from an unverified source.
- Report fraudulent activity to the FBI via the Internet Crime Complaint Center at www.ic3.gov/default.aspx. Also contact the state or local realtor association, which will alert others to the suspicious activity.

Contact TPG Insurance Services today for more information on avoiding real estate fraud and other types of cyber crime.