WIRE FRAUD ADVISORY

Public Service Announcement Information from the FBI
(Alert Number I-050417-PSA)

The following is an excerpt from a Public Service Announcement (PSA) released by the Federal Bureau of Investigation on May 4, 2017 regarding Business E-mail and Public E-mail Compromise Scam. The full PSA can be located at www.ic3.gov.

The Business E-mail Compromise (BEC)/E-mail Account Compromise (EAC) scam targets all participants in real estate transactions, including buyers, sellers, agents, and lawyers. The IC3 saw a 480% increase in the number of complaints in 2016 filed by title companies that were the primary target of scams. The perpetrators were able to monitor the real estate proceeding and time the fraudulent request for a change in payment type (frequently from check to wire transfer) or a change from one account to a different account under their controls.

The problem is defined as a sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments. The email component targets individuals that perform wire transfer payments.

The scam is carried out when a subject compromises legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.

Most victims report using wire transfers as a common method of transferring funds for business purposes; however, some victims report using checks as a common method of payment. The fraudsters will use the method most commonly associated with their victim's normal business practices.

The following are some, but not all, ways to avoid becoming a victim of wire fraud.

- Obtain full name and phone number of the Escrow Officer.
- Do not ever wire funds prior to calling your Escrow Officer to confirm wire instructions. Only use a phone number you were provided previously. Do not use any different phone number included in the emailed wire transfer instructions. Confirm the bank routing number, account numbers and other codes before taking steps to transfer funds.
- Avoid sending personal information in emails or texts. Provide such information in person or over the telephone directly to the Escrow Officer.
- Be suspicious of requests for secrecy or pressure to take action quickly
- Immediately report and delete unsolicited e-mail (spam) from unknown parties. DO NOT open spam e-mail, click on links in the e-mail or open attachments. These often contain malware that will give subject access to your computer system.
- Take steps to secure the system you are using with your email account. These steps include creating strong passwords, using secure WiFi, and not using free services.

If you believe you have received questionable or suspicious wire instructions, immediately notify your bank, the Escrow Holder and your real estate licensee. The following is a list of resources for more information regarding wire fraud.

Federal Bureau of Investigation:	www.fbi.gov
Internet Crime Complaint Center:	www.ic3.gov
National White Collar Crime Center:	www.nw3c.org

By signing below, parties acknowledge that they have read, understand, and received a copy of this Wire Fraud Advisory.

CLIENT _____ Date _____

CLIENT _____ Date _____

CLIENT _____ Date _____