Title Industry Wire Fraud Alert!

At the request of the CLTA (California Land Title Association) Claims Awareness Committee, we would like to alert all of our clients about a new internet fraud scheme that is causing a number of unsuspecting **home buyers to lose their down payments.** Please read this alert in full so that you will not become a victim of this fraudulent activity.

How the Wire Fraud Scheme works:

1. Hackers identify lenders and real estate agents as potential targets by navigating their websites and copying any personal or business information, including: company logos, employee names, physical addresses, and email addresses of agents, brokers, and lenders. All of this information becomes useful in establishing a false identity in subsequent emails.

2. The hackers then hack directly into the email accounts of the real estate agent and/or broker and identify emails referencing pending real estate deals. From these strings of emails, the hackers pull out specific details about the deal, such as: (a) the parties' names, (b) the title company involved, (c) the escrow officer in charge of the deal, and (d) other information specific to the transaction.

3. The hackers then use any gathered company logos, personal and/or business information, and transaction details to create a fraudulent email that looks legitimate on its face, and then send this fraudulent email directly to the buyer or lender, making it look like it was sent by the real estate agent, mortgage broker, or escrow agent. These fraudulent emails now direct the buyer and/or lender to wire the funds necessary to close escrow directly to a different bank account than provided in the preliminary report or in the escrow instructions. Obviously this new bank account is controlled by the hacker, not the title company or the escrow holder.

4. If the fraudulent email request is not caught by the buyer or lender, then the money is wired to the bogus account controlled by the hacker and is immediately withdrawn. Due to the amounts involved and the complex nature of investigating and prosecuting wire fraud, the odds are that the authorities will do nothing to help in these instances.

This is why we emphasize time after time why it is so important for us to encrypt our email when transmitting such sensitive information to our clients. When you are ready to send your wiring instructions or banking information to us, ask your escrow officer to initiate an encrypted email message and send to you, as the email recipient you can send back your information via a return encrypted email, this will avoid any information being sent in an unsecured, unencrypted message, which dangerously expose yourself to the world of the unknown.

For additional information on how you can better prepare yourself from becoming a fraud victim, CLTA has prepared a document "*Steps you can take to avoid being a target of wire fraud scams*", click here to download. Contact your Escrow Officer or your Sales Executive(s) below if you would like more information on how we can help you protect your non-public information.

CHICAGO TITLE®

STRENGTH | EXPERTISE | SERVICE