Fund Transfer Scams Continue Even During COVID-19: Stop, Look Up & Confirm!

Unfortunately, even during these trying times in a pandemic, criminals do not stop their criminal tactics. They continue to take advantage of us.

As you know and are all too familiar with, criminals are posing as participants in real estate transactions, transmitting instructions directing the recipients to send funds right into the hands of the criminals. We had two firms contact us in the past couple of weeks who have been affected in some way, one with a criminal posing as a participant in a transaction and trying to scam the firm, and one where the firm's identity was used to try to dupe clients. It happens more often than we might think. CATIC® and CATICPro, Inc. have been regularly alerting you about these types of activities. We frequently hear from CATIC agents regarding these types of frauds and the variety of ways the criminals are taking advantage of all of us, and, unfortunately, these scams are continuing.

These criminals have educated themselves on all of the players involved in the transaction, their respective roles, and the different requests that may be made regarding payments. They understand the details of documents and processes. Using this information, they will tailor a spoof request, with the recipient thinking the communication is from the involved attorney, paralegal, title company, lender, mortgage broker, real estate agent, etc., so that deposits, payoffs, proceeds, *you name it*, are directed to the criminal. They use different forms of communication, including, but not limited to, email, text, fax, telephone, even mail. The criminals understand what is involved in the transaction, what the documents look like, and what requests will be made, and they use this information to steal funds.

Given the sophistication of what these criminals are able to do and the fact that they are constantly changing their tactics based on all they have learned about a real estate closing matter, it is crucial that you continually educate your staff, your customers, and all of the players involved in your transactions about what is happening and the need to be alert as well as cautious. You need to plan in advance for how your business will handle communications and transfers of funds, and identify other risk management initiatives for implementation to protect your business and customers. You also need to plan for how you will respond if you or your customers fall victim. (For example, when receiving instructions to transfer funds, stop, look up the known contact using reliable contact information that you already have, and take the time to verify and confirm the authenticity of what is received - especially if it concerns any type of payment or funds transfer request.) Stop, look up, and confirm, for example, by calling the known reputable source at the number obtained from a verified, independent source (not from the documentation or information received), and verify the information. Also, be sure your customers understand that they need to plan and implement risk management initiatives as well.

Minimize risks by increasing awareness and proper planning and implementation. Also, be sure to continually review plans with your privacy/security experts (like your attorney and technical support, etc.) for how you will mitigate the risk, and also for how you will respond if you or your customers are victimized – criminals change tactics so your efforts may need to be modified along the way. It is important that you work with your support experts to establish measures in this area, review the measures regularly, and modify when necessary. Criminals will change their tactics, so testing, assessing, reviewing, and modifying your initiatives is important. If you have questions on this article, please contact **Colleen M. Capossela, Esq.**, President of CATICPro, at (860) 513-3131.