ALERT – Fund Transfer Frauds Escalate and Not Just Via Email Compromises

CATIC has received an increasing number of reports from businesses affected in one way or another by a fund transfer fraud. As you already know, the criminals have educated themselves on all the players involved in the real estate transaction, their respective roles, and the different requests that may be made regarding payments. Using this information, they will, for example, tailor a spoof request to a participant in the transaction so that deposits, payoffs, proceeds, *you name it*, are directed to the criminal.

Making matters worse is that the criminals communicate with us by all different means, like, for example, email, e-fax, regular fax, telephone, text, regular mail – *again, you name it!*

Of course, we have heard of numerous scams using fraudulent emails, tricking one into sending funds to the criminal. But we have also heard of cases where reliance was made on fund transfer instructions received in other ways. For example, a CATIC agent advised us of the receipt of a fake mortgage payoff instruction by regular fax; another received an instruction by e-fax. **It is imperative to discuss the concept of fraudulent faxes. Often, we are misled into believing that faxes are secure and the best form of communication, especially when wiring instructions become part of this equation. However, fax machines are incredibly insecure.** The reality is that faxes, when connected to a network, for example, use technologies that have gone unchanged for nearly three decades. Fax data is typically sent with no cryptographic protections. When we think of these types of protections, we are referring to assurances that the transit of this data is kept confidential and is not subject to alteration.

Standard fax machines lack encryption and firewall defenses; e-faxes have made better progressions in terms of security by at least using TLS encryption, *but this method can still be hacked*. For example, if criminals are aware of your fax number, they can send a document with a malicious attachment. If that document is opened, hidden and malicious codes can execute on your machine. In another light, if your email is already compromised and you are working on an upcoming real estate transaction, a bad guy can send you bogus wiring instructions via your e-fax number, and people will likely not expect something fraudulent coming from a fax number.

Even telephone calls are made to convince you that you are speaking to the legitimate party in order to get you to divert funds to the criminal.

This is why it is so important to educate and plan accordingly, implement risk management initiatives, and maintain proper insurance coverages. For example, and by no means all-inclusive, consider:

1. *implementing a process to securely communicate upfront with all participants, at the beginning of each transaction*, warning them about what is transpiring in the industry, and have everyone agree then as to how to handle communications and transfers of funds securely; and

2. *independently verifying and confirming any instructions you receive* by using independent, confirmed, known contact information for the proper party you need to verify and confirm with; *do not rely on or use contact information on the potentially fraudulent instruction communication that you received.*

Plan with your experts. And then remember also to continually review and update your processes and plans with your experts – attacks change, security initiatives and resources change, etc. – so we all have to stay on top of this and modify accordingly. If you have questions on this alert, please contact Colleen M. Capossela, Esq., President of CATICPro, at (860) 513-3131.