E-mail Hacks and Wire Fraud Continue to Impact the Commercial Real Estate Market

By: Michael J. Romer, Esq., Managing Partner, Romer Debbas LLP

Michael J. Romer, Esq.
Romer Debbas LLP
275 Madison Ave, Suite 801
New York, NY 10016
212-888-3100
mromer@romerdebbas.com

For good reason, our office decided to stay ahead of the curve and retained the services of an information security specialist to conduct a thorough audit of our systems and protocols in order to ensure that client information was secure. At the end of the audit, we received an ALTA Best Practices Pillar 3 Certificate, the current gold standard for law firms when it comes to information security.

In the world of legal representation, whether you represent individuals or large institutions, securing confidential client information is crucial. We now live and work in a world where e-mails are hacked and information is stolen on a regular basis. It seems there is a new story concerning email hacks every day. As we have all come to learn, top-secret government emails aren't even truly safe. Sadly, one's personal and financial information has become a commodity of sorts. However, many don't realize that the real estate market is not immune to such hacking, fraud, and information theft.

Over the course of my 17 years of practice, I have been witness to multiple attempted scams ranging from fake official bank checks (that look almost exactly like the real thing) to attempted fraudulent property transfers. This is why it is so crucial to ensure that the banks, title companies, and other business partners are both trusted and experienced. Such attempts at fraud and theft are generally easy to detect and prevent. However, e-mail hacking has taken things to a different level. In many cases, despite the best servers and IT available, we practitioners oftentimes cannot trust the information we are receiving on a daily basis from our own colleagues in the field.

In recent years, we have received multiple emails from practicing lawyers' actual email accounts (or "spoofed" versions thereof) which were later proven to be fraudulent. Besides potentially wanting to obtain personal information from a client for identity theft purposes (which alone is concerning), it seems the individuals behind the hacks are zeroing in on wiring instructions.

Here is the scam in a nutshell. An individual hacks the email server of a real estate lawyer (often a personal one) and actually scans the emails searching for a deal at the wiring money stage (i.e. time of down payment posting or time of closing). Then, the hacker composes an email from the attorney's server and email address providing the wiring instructions for the account to which either the contract down payment, closing proceeds, or otherwise should be sent. The problem is that the account number pertains to a bank account (usually off shore) maintained by a shell company affiliated with the hacker. If the email recipient (generally the attorney on the other side) or its bank does not verbally verify the wiring instructions and then proceeds to send the wire, those funds could very well disappear. Substantial sums of money are at risk on a daily basis and all parties to a deal are forced to be more diligent than ever before.

Our office recently represented a purchaser acquiring a piece of property and was working with an attorney on the other side (who we have worked with before) and the contract had just been finalized and executed by our client. Our client (as many do) wired the down payment proceeds to us as counsel in order for us to forward over to seller's counsel. This particular attorney requested the down payment be wired to his escrow account. Shortly thereafter, we received a second email from the exact same email address stating that the previous instructions were sent in error and that we were to use replacement instructions. As we always do (and I cannot stress the importance of this), our office contacted the other attorney to verbally verify the instructions and were surprised to learn that the second email was indeed fraudulent. Someone had hacked the attorney's email server (which happened to be personal), read the email chain, and sent instructions that matched the initial one's, except both the bank account number and the routing number had been changed. Luckily, a crisis was averted.

With respect to our market, it begs the question as to what measures real estate attorneys, law firms, brokerage houses, banks, and otherwise should have in place to prevent emails from being hacked. A wide majority of banking institutions have even implemented password protected secure email systems requiring an email recipient to create his own login and password to access the bank's secure server.

In this day and age, law firms must be extra vigilant and ensure that their IT systems are secure and their client's personal information and money remain protected. Protecting client information is more important now than ever. The risk is real.