What You Should Know and Do to
Prevent Unsuspecting Buyers and Sellers from being Duped by Fraudsters

By: Matthew Goodwin, Attorney and Legal Resources Committee Member

Over the last few years, wire fraud scams have swept the nation. With no end in sight, the criminal masterminds behind these sophisticated schemes are increasing their effectiveness in siphoning hundreds of thousands of dollars from unsuspecting parties to real estate transactions. This article will provide a quick summary of the fraudulent scheme, some real examples, and useful information as to what you can and should be doing right now to protect yourselves and your customers from becoming victimized.

How Your Email is compromised and Examples of Emails Subject to Being Hacked

Since email is the primary means of orchestrating the fraud, all the fraudsters have to do is a quick Internet search for email addresses of real estate agents, title companies, and attorneys. Indeed, most of these real estate practitioners WANT their contact information to be easily accessible on the Internet so this is a menial task. Once the fraudsters have their email list, they send official looking emails asking recipients to verify their account information, click on links, or open attachments that contain viruses. Once the email account is compromised, all they need to do is monitor email communications. For example:

- The closing agent sends wire instructions from a compromised email account where hacker can read incoming and outgoing emails and obtain information about upcoming transactions;
- The closing agent sends wire instructions from a secure account to an unsecure account. This can occur if the buyer's email address is compromised or if a Realtor who was cc'd on the wire transmittal email has a compromised email account.
- Email containing wire instructions sent in an open, non-password protected PDF or other unsecure format. The hacker's ability to see the original instructions, including the fonts and formatting, is important for the fraud to work.

Statistical Data and Real Examples:

The Federal Bureau of Investigation, Internet Crime Complaint Center (IC3) has reported the following statistics in connection with what is referred to as the Business Email Compromise (BEC) scam. Between January 2015 and June 2016, IC3 identified a 1300% increase in losses due to the BEC scam. As of June 2016 there have been a total reported of 22,143 domestic and International victims with combined losses exceeding $3 billion dollars. Between October 2013 and May 2016, total U.S. victims lost approximately $1 billion dollars.

Below are a few instances of actual losses from the BEC scam:

- July 2015, Stroudsburg, PA - Buyer received email from Realtor the morning of the closing with instructions to wire $36,000 to a Florida account. The scam became apparent only *after* the buyer received *another* email a few hours later from the title company with different instructions for where to wire the payment. This scam originated in South Africa where the fraudster somehow obtained the user name and password of the agent, monitored all of the email transactions between the Realtor, buyer and title company and then, knowing that the buyer would be receiving wiring instructions on the date of closing, sent a bogus email early that morning with his own set of wiring instructions.

- November 2015, Frederick County, MD - $300,000 was minutes away from being diverted to an account set up by hackers operating out of Nigeria when one of the Realtors noticed something odd at the closing. Contrary to instructions from his seller clients, the buyers' title company was about to wire the proceeds of the sale to an unknown bank account rather than sending a check to their relative.

- January 2016, Fernandina Beach, FL - Real estate attorney wired nearly $600,000 to a fraudulent account after receiving an email she believed was from the seller. According to a police report, the

transfer occurred just before the closing of the sale. However, the scam was not discovered until a week later, when the seller informed the attorney he had not received the proceeds.

A similar scam was reported in the Tampa Bay area, where a closing agent received an email from the sales associate's legitimate email address, requesting that $85,000 be sent via a wire transfer to a different account. Fortunately, the closing agent called the sales associate for confirmation and didn't transfer the funds to the fraudulent account.

- January 2017, Cape Coral, FL: A man trying to sell his house in Cape Coral nearly lost $60,000 when a scammer tricked the title company to wire the money to a bogus account. Follow this link for the full story and interview with the seller: http://tinyurl.com/jvnvrdv

Prevention and Protection

Realtors have a lot a stake and are exposed to lawsuits, attorney's fees, litigation expenses, damaged credibility and reputation, restitution judgments, and more. Here are some things you can begin doing right now to prevent yourself from becoming exposed to liability and your clients from losing money:

- At the onset of a transaction, gather verified emails and phone numbers for the buyer, seller, their agents, and the title company or closing attorney; make sure the buyer and seller have the verified contact information of the title agent and vice versa;
- Make it your policy not to send, accept, or request wiring instructions, instead explain to your customers that it is their responsibility to ensure they have the most current information from the title agent;
- Tighten up your email security measures by changing passwords more frequently because if your email is impenetrable, the fraudsters are much less likely to be able to rip off your clients.
- Purge your emails on a regular basis. Your e-mails may establish patterns in your business practice over time that hackers can use against you and if your email is ever penetrated, it will be more difficult to establish a pattern.
- Implement the most up-to-date firewall and anti-virus technologies on your server or computer.
- Use a more "secure" email address for any correspondence about the transaction. Consider using your work email address because there are generally more firewalls and security protocols. Avoid free, internet-based accounts like Yahoo and Gmail.

Make sure your customers are informed by telling them:

- Before wiring funds, contact the escrow agent using a telephone number verified at the outset of the transaction and confirm the wiring information is accurate. Do not rely on telephone numbers or Web site addresses provided within an unverified e-mail.
- Never to send any non-public person information via e-mail, including but not limited to bank routing and account numbers, social security numbers, and identification documents. If you wouldn't share the information on Facebook, don't put it in your email!
- Verify any changes to the settlement agent's contact information or wiring instructions either in person or via the trusted phone number given at the beginning of the transaction.
- If they receive an email changing the timing and/or amounts to be wired to the settlement agent, verify using a trusted phone number or in person.
- Watch out for instructions marked "urgent" or giving a close deadline (e.g. close of business today). Fraudsters want to create a sense of urgency to get you to act without thinking.
- Watch out for offers from the seller or their real estate agent that are "too good to be true." For example, if you are negotiating a repair escrow or credit at closing and receive an offer agreeing to resolution for significantly less money if they are paid the balance "today, by wire transfer," contact your real estate agent or attorney to verify the legitimacy of the offer.
- Never use the phone number given in an email to verify the information contained in the email. Fraudsters often use pre-paid cell phone numbers in these emails and then actually answer the phone when you call, thereby continuing the fraud.

- Be alert for slightly different email addresses from anyone connected with the transaction, for example: john-smith@titleone.com vs. johnsmith.titleone@gmail.com
- If unable to verify the settlement agent's wire instructions via a trusted phone number or in person, wait until they can verify to wire funds.

Many companies have already implemented strict wire transfer protocols, but do not be surprised of future policy changes with your preferred title company or real estate attorney's office, such as mandatory telephone confirmation of wiring instructions prior to disbursement, password verification system for wire instruction or funds disbursement changes, and encrypted emails requiring a user ID and password.

What makes the BEC scam so scary, is that the perpetrators are nearly impossible to identify and it is difficult to blame financial institutions because they generally do not owe a fiduciary duty to non-account holders initiating wire transfers. Therefore, title agents, realtors and their brokers are left to take the blame. The best way for you to avoid liability and customer losses is to make sure you and your customers are educated and taking proactive measures to protect yourselves.

If you or anyone you know is suspicious of fraudulent activity, take note of the following ways to report it:

- Inform local law enforcement or the state attorney general as appropriate
- Report stolen finances or identities and other cyber crimes to the Internet Crime Complaint Center at www.ic3.gov
- Report fraud to the Federal Trade Commission at www.onguardonline.gov/file-complaint
- Report computer or network vulnerabilities to US-CERT via the hotline: 1-888-282-0870 or www.us-cert.gov