Wire fraud: A new nightmare for real estate conveyancers and title companies - by Francis DiSanti

June 16, 2017 - Spotlights

Francis DiSanti, CATIC

As if real estate conveyancers and title insurance companies did not have enough to worry about with tracking down missing assignments/discharges, or determining whether or not a lender has followed the guidelines to perfect its rights of foreclosure, they now face a growing threat that has dire financial consequences. Unfortunately, a disturbing number of conveyancers are becoming victims. According to estimates published by the Wall Street Journal, computer hackers perpetrating wire fraud have accounted for approximately $1 billion in losses from October 2013 to June 2015.(1)

Hackers are acquiring information by infiltrating and monitoring emails of the real estate community. They learn who the parties are to the transaction, the amount of the purchase, the date of the closing, and most importantly, if any of the funds are being wired. Once the information is learned, the hacker generates an identity very similar to one of the parties involved in the transaction. For example, the seller's attorney's correct email address of AttyJones@joneslaw.com is altered slightly to AttyJones@jonelaw.com. The fake email is set up to appear exactly the same as the correct email address, and could even contain the official logo of the seller's attorney. On the day of the transaction, an email is sent from the fake address to the buyer's attorney indicating that there is a change in the wire instructions, and instructing the attorney to wire the seller's proceeds or a payoff to a new address. An unsuspecting conveyancing attorney may look quickly at the email address and not realize that the email transmission was coming from a criminal third party. The wire is sent to the fraudulent address and the funds are forever lost.

This scheme could even affect real estate conveyancers who believe they are protected against

cyber-crime because all of their emails are encrypted. Hackers are targeting not only the real estate conveyancers, but also the real estate agents who are involved in the transaction. The unprotected emails of the realtors are compromised by the hacker. From there, the hackers can monitor the information being exchanged and learn the information they will later need to set up the fake email account. The fact that a real estate conveyancer uses encrypted email to send out information does not protect him or her from an incoming email from a fraudulent third party.

Conveyancers who fall victim to wire fraud and attempt to cover the loss with a claim to their malpractice insurance may be informed by their carrier that they lack coverage. Some malpractice companies are taking the position that the sending out of wire fund is not considered the practice of law; rather it is considered a ministerial task and not a covered risk under the policy. Attorneys are being forced to seek court determination if wire fraud is a covered risk. In Stark & Knoll Co., L.P.A. v. ProAssurance Cas. Co., 2013 WL 1411229 (N.D. Ohio 2013), a malpractice insurer made such an argument; however, the court found in favor of the attorney referring to Nardella Chong v. Medmarc Casualty Ins. Co., 642 F.3d 941, 942 (11th Cir. 2011), which ruled that the insurance policy covered actions which included those of a “trustee” or “similar fiduciary capacity.” While in this instance the attorney was successful in obtaining coverage, the firm still had to incur out of pocket expenses to enforce the provisions of the malpractice policy to cover the wire fraud claim.

From a title insurance perspective, this issue becomes extremely problematic with the wiring of payoffs for mortgages or outstanding municipal taxes. Using the same email scheme, hackers can supply false mortgage payoffs requesting funds be paid to fraudulent accounts. In such a scenario, claims could be made under both the Closing Protection Letter and the title policies for the current transaction because the lien on the property would not be paid or discharged. Considering the size of many mortgage payoffs, the repercussions of these hacker attacks are astronomical.

According to the American Land Title Association, title companies have reported an increase of wire fraud scams in the amount of 480% in 2016 (2). In an effort to combat these hacker attacks, there are a number of measures designed to increase security. Such measures include: avoid web-based email accounts such as yahoo or gmail to transmit business communications;

secure your wireless network; change computer passwords regularly; keep virus and firewall software up to date; and most importantly, in the event there is a change in wire instructions during a transaction, call the receiver of the wire directly and verify the requested change.

Considering the increased reliance on electronic communications and the wiring of funds during transactions, it does not appear that the end of these cyber-attacks is coming anytime soon. In addition to the measures discussed previously, conveyancers and title companies need to be vigilant in keeping up to date with the latest schemes in order to make sure they know what to look for if faced with a similar circumstance. If you unfortunately become a victim of a scheme, contact your local Federal Bureau of Investigation (FBI) office and file a complaint with www.ic3.gov.

Francis DiSanti, Esq. is title counsel in CATIC, Springfield, Mass.

(1) Wall Street Journal, July 29, 2015 https://www.wsj.com/articles/hackers-trick-email-systems-into-wiring-them-large-sums-1438209816

(2) ALTA, May 30, 2017 https://www.alta.org/news/news.cfm?20170509-Title-Companies-Report-480-Increase-In-Wire-Fraud-Attacks