CHICAGO BULL

(June 11, 2015, Chicago Title NC Blawg)

Where's my money?
Wire schemes and email hacks are on the rise

Theft from closing attorneys and settlement agents across the country is increasing. Now that email is the primary (or sole) mode of communication for closings, and money is routinely wired, hackers are taking advantage of the lack of security by stealing closing funds. How can you protect yourself and your clients?

First, as much as we all find that encrypted email can slow the closing process down, it is certainly one of the most important steps in avoiding theft of closing funds. Hackers can intercept wiring instructions, emails containing HUD-1 settlement statements, or other emails with private information pertinent to the transaction. These interceptions are then used to send fraudulent information to the intended recipient in an effort to redirect the destination of funds. Hackers may also use information obtained to convince someone in your office that they are involved in the transaction and provide fraudulent information by email or phone to redirect funds.

Second, if your office receives payment or wire information from a party to the transaction and it is not encrypted, it is possible that the information was intercepted and you have received fraudulent information. One way to confirm that the information is correct is to make a phone call to a known party to the transaction (not to the phone number listed on the unencrypted email) to verify the information provided. Do not reply to the party that sent the email as the reply email would likely go to the intercepting party.

Third, trust your instincts. Often the signs that something is wrong are small – an email sent from an email address that is one letter off, unusual misspellings in emails (such "authorisation" instead of "authorization"), addresses or other information that don't match up to what you know about the transaction, and/or refusal to give or discuss the changes on the phone. Sometimes there are bigger flags such as requesting at the last minute that proceeds be wired instead of a check (or stop payment on a check after it has been sent). If something doesn't seem right, follow up with a known party to the transaction by phone using a verified phone number.

These schemes are becoming more and more prevalent so diligence in protecting information is key and any red flags warrant further investigation to save you and your client from a potential huge loss.