New England Regional Midweek Update
6/21/2023

Dear Stewart Partners,

Thank you for joining us again this week. We hope you enjoyed this past long weekend and took some time out of what is turning out to be a very busy June to spend time with family and friends.

In this week's update, we have included a notable case involving a lawsuit by a buyer who was spoofed and, as a result, sent a purchase money wire to fraudsters, and a short article regarding email scams involving obscured and obfuscated links. We're also passing along some information on Stewart's Virtual Underwriter website. Finally, in case you missed it, there's a link to a recent economic forecast webinar featuring Stewart's Chief Economist, Dr. Ted Jones.

Evolving Law - Hacked escrow agent can be sued by spoofed homebuyer

Although outside the jurisdiction of the New England states, we are highlighting this case to show the importance of having established wire transfer protocols, including providing your clients with clear warnings and instructions about sending wires, and following them.

An Ohio appeals court overturned a lower court dismissal on summary judgment finding there were genuine issues of material fact on several issues including "who bears the responsibility for the escrow fraud that took place in the case." *Conor Hoffman v. Atlas Title Solutions LTD* (Court of Appeals of Ohio, Third Appellate District, Union County, No. 14-23-04). Link to the full opinion here: Hoffman v. Atlas Title Solutions, Ltd. (ohio.gov). The plaintiffs claim a of breach of contract and breach of fiduciary duty in an implied agreement for escrow services. The case involves a 2021 cash purchase where the plaintiffs wired approximately $290,000 to a fraudster. The facts are somewhat common in that there were emails between the real estate agent, buyers and the title company; one party's email was hacked, fraudsters sent altered wire instructions to the buyer and the buyer wired funds to the fraudsters. In this case, certain emails from the broker stated that the title company would provide wire instructions and the buyers should contact the title company to confirm the amount of the wire and the instructions before wiring any money. Prior to closing the buyers received an email with wire instructions, called the number in the email to verify the instructions, and sent the wire. These instructions, however, were sent by a fraudster. Unfortunately, the real wire instructions, which were sent by unencrypted email, were directed to the buyers' spam folder and never received. The misdirection of funds was not detected for three days, and the funds were not recovered. Notably, in this case, evidence was presented that the title company was hacked at some point earlier in 2021 by the same fraudster, but that no information was compromised.

Subsequently, the buyers filed a lawsuit alleging negligence, breach of contract and breach of fiduciary duty. The trial court allowed summary judgment in favor of the title company finding no privity of contract or fiduciary duty and the plaintiffs appealed. The plaintiff contended that the lower court erred in dismissing the case because genuine issues of material fact exist as to whether there was an implied contract between the parties and whether there was a breach of fiduciary duties by the title company. The negligence count was also dismissed by the trial court. The buyers appealed.

The appellate court did not agree that summary judgment was appropriate. The appellate court reversed stating, "[i]mportantly, we agree that triable issues remain as to whether (at the very least) [the title company] implemented "proper" security measures to prevent [the plaintiffs'] personal information from being "phished" to precipitate the "spoofed" email or whether [the plaintiffs] should have recognized that the email was "spoofed," Id. at 2, in part based on testimony by a witness for the plaintiffs who asserted that the title company "did not have an adequate compliance program to safeguard their customers' information... [and] did not follow its own policy or the [American Land Title Association ("ALTA")] Best Practices," which "fell well below the industry standards…."

This case is just one example of how the law in this area is evolving and how the courts are examining the duties and responsibilities of the settlement or escrow agent in a transaction. We featured this case today to highlight the risk of handling funds in general and, more specifically, the risk of not actively making sure clients and others who may be sending funds to your organization don't get tricked into sending funds to a fraudster. It also stresses the importance of having established protocols, including providing clear warnings and instructions about sending wires, and following them. Communication and education early and often with all the parties in the transaction are critical and helps avoid losses.

Stewart's Virtual Underwriter Website

We hope by now you're all aware of Stewart's Virtual Underwriter website, www.virtualunderwriter.com. It's a one-stop site for Stewart's underwriting bulletins, endorsement guidelines, and state-by-state real estate practices. We wanted to alert you that in the coming months, the Virtual Underwriter site will require a login and password to access. Don't worry – you will be hearing from Stewart with details, so that your access will continue. Keep an eye on your inbox for more information!

Scam of the Week: Obscured, Obfuscated Links – By KnowBe4

KnowBe4 recently circulated the following “Scam of the Week” regarding obscured and obfuscated links:

Recently, researchers at Avanan discovered another technique that cybercriminals use to try to steal your information. In this technique, fraudsters use obfuscated links to show IP addresses instead of websites. Obfuscated links are URLs that have been modified to hide the real location of a website.

In this scam, cybercriminals send an urgent email that appears to come from a legitimate source and prompts you to click on a link. The link seems legitimate, but hovering over it shows an IP address instead of a URL. Without a URL, it’s nearly impossible to verify if the link is legitimate. If you open the link in your browser, cybercriminals can download malware onto your device or redirect you to a malicious website.

Follow the tips below to stay safe from similar scams:

- When you receive an email, stop and look for red flags. For example, watch out for emails with different reply-to and sender addresses.
- Before you click a link, hover your cursor over it. If it shows an IP address, it could be a phishing link.
- Be cautious of urgent requests. Cyberattacks are designed to catch you off guard and trigger you to click links impulsively.

For free tools and other resources offered by KnowBe4, visit KnowBe4.com.

In Case You Missed It – Economic Forecast Series Featuring Dr. Ted Jones

In case you missed it you can listen to the recent Economic Forecast Series by Dr. Ted Jones, Stewart’s Chief Economist. A recording of the series is available in the webinar library at TheLegalDescription.com or by clicking this link: www.thelegaldescription.com

Meet Our Team | Stewart Connecticut

Meet Our Team | Stewart Maine

Meet Our Team | Stewart Massachusetts

Meet Our Team | Stewart New Hampshire

Meet Our Team | Stewart Rhode Island

Meet Our Team | Stewart Vermont

1-800-STEWART

www.stewart.com

This email was sent to your address because your email preferences are set to receive our updates.

unsubscribe