NEVADA REALTORS®
Advocacy. Leadership. Excellence.

Nevada REALTORS®
760 Margrave Drive - Reno, NV 89502
775-829-5911 - NevadaRealtors.org

NEWS FOR THE NEVADA REALTOR®

Business Email Compromise

— Think Twice Before Clicking Send —

CHRISTAL PARK KEEGAN, Esq.
NVR Legal Info. Line Attorney

Cybercrimes against real estate transactions are increasing and unsecured email correspondences are a target. Realtors® need to beware that hackers can intercept emails between clients and real estate agents that could enable the thief to steal funds. Further, you can be held liable to the victim for negligent cybersecurity, as was the case where a jury found in favor of the buyer and entered a verdict of $170,000 against the listing agent and broker (Bain v. Platinum Realty, LLC, D. Kan. 2018). It's crucial that all parties involved in the transaction are diligent in their communication and take necessary precautions to protect Personal Identifying Information (PII).

NVR's LIL Attorney Christal offers members some best practices based on Nevada law NRS 603A, along with information provided by the National Association of REALTORS® (NAR), as well as feedback from title companies.

Encrypt email and attachments. In addition to checking your email settings for encryption capabilities, there are numerous companies (such as Virtru and ShareFile) that provide this service. Although an original email may be encrypted, it's important for brokers and their agents to know that when an email is forwarded it is not encrypted.

Do not email unredacted earnest money deposit (EMD) checks. Doing so violates NRS 603A because it includes a client's PII. Take care on who is copied on emails that include EMD checks and only include persons absolutely necessary. Consider letting the title company directly reach out to your clients to get the information they need, which limits your exposure to a potential mishandling of PII claim.

Be patient with log-in issues with encrypted and/or multi-step authentication emails. Understand that requesting the title company to send a PDF of an attachment to bypass multi-step verification processes violates NRS 603A. Call the title company and troubleshoot the issues or seek in-house IT assistance if available.

Check your E&O insurance coverage. Ensure it covers business email compromising events. In light of wire fraud scams, ask about social engineering and impersonation coverage.

Consider the timing of social media postings. Hackers lie in wait, silently monitoring real estate transactions, until the most opportune moment to strike. Consider delaying posts of upcoming and real-time closing signings so as not give the criminals a heads-up.

Do not log in to public WiFi. Hackers, malware and other threats pose security risks. When using your business email ensure you are on a secured network.

Install anti-malware protection and regularly update it. At a very minimum, a computer itself should be protected with basic anti-malware software. Monitor email accounts for unrecognized activity and regularly purge unneeded emails from your account. Check your email settings to ensure your emails aren't being impermissibly copied and forwarded. Never click on links or attachments in unverified emails because they may deploy malware.

Every single agent, staff member, and employee should be trained on best email handling practices. Often data breaches result from negligence on the part of an otherwise well-meaning employee. Make sure everyone on your team is on the same page.

RESOURCES

(Differerent web browsers treat various links in different ways. If a link does not seem to be clickable, try copying and pasting the link directly into your web browser.)

The NAR shares several examples of wire fraud notices used by other REALTOR® associations as an educational and risk management tool to protect real estate professionals from liability related to wire fraud:

- *https://www.nar.realtor/data-privacy-security/wire-fraud-notices*

Numerous federal agencies have issued warnings and tips, including the Consumer Financial Protection Bureau, the Federal Trade Commission (in cooperation with NAR) and the FBI/IC3.

- *https://www.consumerfinance.gov/about-us/blog/mortgage-closing-scams-how-protect-yourself-and-your-closing-funds/*
- *https://www.consumer.ftc.gov/blog/2017/06/protect-your-mortgage-closing-scammers*
- *https://www.ic3.gov/media/2018/180712.aspx*

The National Institute of Standards and Technology offers the "Guide to Protecting the Confidentiality of Personally Identifiable Information."

- *https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf*

The NAR provides a Toolkit which includes information about data security and privacy protection, as well as various helpful checklists on issues to consider when drafting a tailored security program:

- *https://www.nar.realtor/sites/default/files/documents/Data%20Privacy%20and%20Security%20Toolkit_081117_rev.pdf*

Washoe County Sherriff's Office, specifically See Tip #12 Escrow Services Fraud:

- *https://www.washoesheriff.com/sub.php?page=cyber-security-awareness-tips&expand=General%20Information*