TRAINING TIP OF THE WEEK

REALTOR SAFETY:

Avoiding Cyber Liability

Benjamin and Joyce Fox were eager to move to a home near family and settle into retirement. In 2017, after a three-month house hunt, they found a three-bedroom townhouse in Lafayette, N.J.

The townhouse was a foreclosure, owned by JPMorgan Chase. The Foxes agreed to pay cash for the $91,500 listing. They withdrew the money from a home equity line of credit on their current house. On Aug. 29, 2017, Joyce received wire transfer instructions via her Yahoo email account. An email from her real estate attorney had told her to expect such instructions. She wired the $91,500.

On closing day, Sept. 1, 2017, the couple's homebuying dream turned into a nightmare. The closing representative scrutinized the wire transfer receipt: "That's not our bank, and that's not our account number."

The Foxes had fallen victim to an elaborate wire fraud scam that has become all too familiar to anyone who works in real estate sales—a scam that involves infiltrating email accounts and sending fraudulent wire transfer instructions. In this case, the scammers had sent fictitious emails to the Foxes, impersonating both their real estate attorney and real estate agent, for weeks leading up to closing.
Today, more than two years later, the couple is still paying the $91,500 for a home they've never owned. They've filed suit, seeking to hold their attorney, agent, and others accountable for not warning them of the dangers of such scams.

Could You Be Held Liable?

Real estate mortgage closing scams are one of the top five wire fraud schemes, according to the FBI's Internet Crime Complaint Center, accounting for $150 million in losses in 2018 alone.

As cyberfraud scams grow more sophisticated, real estate pros are finding themselves more at the center of such lawsuits. In one case from 2018 (Bain v. Platinum Realty LLC), a Kansas court found a real estate agent and her brokerage liable after fraudulent wire instructions that the agent allegedly forwarded to the buyer resulted in the buyer losing $196,622. The agent denied sending the email. A jury found the agent and her brokerage 85% liable and ordered them to pay the buyer $167,129 in lost funds. A federal court upheld the verdict.

Protect Yourself—and Your Clients

The Foxes accused their agent of using an unencrypted, personal email account to send contracts that the couple argues put their personal information at risk. Upon further investigation of what went wrong, the Foxes had received all incoming and outgoing messages from Joyce Fox's
Yahoo account leading up to the wire transfer.

(continued…)

CACHE VALLEY ASSOCIATION OF REALTORS®

REALTOR SAFETY: Avoiding Cyber Liability

The actual transfer instructions from their attorney's office came in just seven minutes prior to the fraudulent instructions; the scammer had taken control of Joyce Fox's account, deleted the attorney's message, and replaced it with fake instructions. The fake message was sent from an email address that omitted just one "l" from the attorney's email address.

"The best practice to prevent liability is to not let your clients become a victim in the first place, and that means educating them up front—and often—and especially as money is exchanging hands," says Lesley Muchow, deputy general counsel at the National Association of REALTORS®.

NAR is working with the FBI and other real estate industry groups to help warn consumers and arm real estate professionals with tools to educate consumers about the dangers of wire fraud scams. There are videos, pamphlets, and checklists for brokerages to use, urging agents to:

- Have face-to-face conversations with clients to clearly explain the risks. Urge them to always call and verify all wiring instructions they receive by calling a known person through a trusted phone number, not the phone number provided in the email with the wire instructions. Calling a number in the email could result in connecting directly with the scammer, who will confirm the false wire instructions. "A real estate professional has the opportunity to sit down, look the client in the eye, and say, 'This is a problem,' " says Bruce Phillips, chief information security officer at West, a technology subsidiary of Willston Financial Group. There's a customizable brochure available from NAR that agents can use to guide these conversations.
- Add a disclosure form as a risk management tool for your brokerage. Several state associations and brokerages have developed a wire fraud disclosure form that real estate pros can use to warn clients about cybercrime risks. Utah uses a form called the "Wire Fraud Disclosure Form."
- Consider insurance to reduce your liability.
- Adopt greater security precautions to safeguard your transactions. NAR has developed a cybersecurity checklist, available to download at nar.realtor.

It includes tips such as:

- Use encrypted email, a transaction management platform, and a document-sharing program when sharing sensitive information.
- Use two-factor authentication.
- Avoid using unsecured Wi-Fi connections when conducting business.
- Use complex passwords.
- Keep software, firewalls, and operating systems up-to-date with the latest patches.
- Urge clients to confirm all instructions in person or over the phone with a trusted representative and never simply follow emailed instructions.