REALTORS® Warned About Rising Threats From Scams and Identity Theft

FTC and Identity Theft Resource Center share fraud prevention strategies

Real estate professionals increasingly find themselves on the front lines of fraud prevention as scammers target businesses and consumers with sophisticated schemes involving identity theft, wire fraud, phishing attacks and data breaches.

That was the message delivered during a recent Zoom presentation to more than 45 brokers, owners, and managers of local real estate brokerages. The session, presented by the 10,000-member Southland Regional Association of REALTORS®, featured Gema De Las Heras of the Federal Trade Commission and Mona Terry of the Identity Theft Resource Center.

The speakers warned that real estate transactions are especially attractive to criminals because they involve sensitive personal and financial information, including Social Security numbers, bank account details and wire transfer instructions.

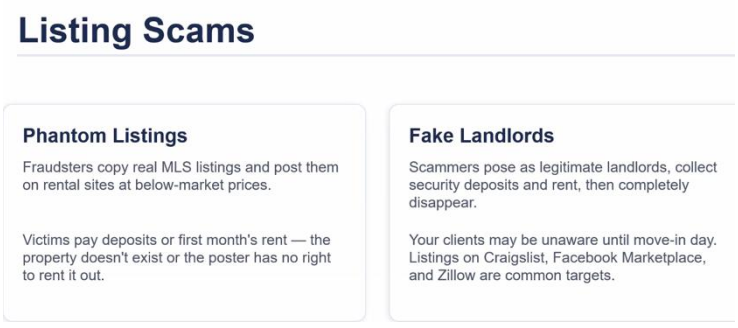
Common Scams Targeting Businesses

De Las Heras said scammers often impersonate trusted organizations to pressure business owners into making payments or sharing confidential information.

Common scams include:

- Utility shut-off threats.
- Fake government notices involving licenses or fines.
- Bogus tech support or website-related warnings.
- Vendor impersonation schemes.
- Phishing emails requesting passwords or account access.

“Scammers create a sense of urgency just to pressure you into paying or giving them information,” De Las Heras said.



She advised REALTORS® and business owners to independently verify unexpected requests and never rely on contact information provided in suspicious emails or text messages.

Fake Invoices and Phishing Attacks

Fraudulent invoices remain a common tactic. Scammers send realistic-looking bills hoping employees will process payments without scrutiny. In some cases, links embedded in invoices install malware that allows criminals to access company networks and client information.

To reduce risk, the speakers recommended:

- Verifying all invoices.
- Establishing vendor approval procedures.
- Researching unfamiliar companies online.
- Training employees to recognize phishing attempts.

Data Breaches Fuel Identity Theft

Terry said identity theft often begins with information exposed through data breaches.

According to ITRC data:

- The U.S. experienced 3,322 publicly reported data compromises in 2025.
- That represents a 79% increase over five years.
- 81% of small businesses reported experiencing a cyberattack or security breach.
- 54% of breach victims later experienced increased phishing attempts.

“Once criminals have information, they just keep using that information to try and get more,” she said.

New Threat: HELOC Fraud

An emerging trend involves fraudsters using stolen personal information to gain access to homeowners’ Home Equity Lines of Credit

Criminals:

- Impersonate homeowners.
- Bypass security checks using stolen personal data.
- Obtain access to credit lines.
- Sell compromised accounts through criminal networks.
- Withdraw funds before victims discover the fraud.

Homeowners with significant equity are increasingly being targeted, Terry said.

HELOC Fraud Takeover Process

Home Equity Line of Credit Takeover. Over $245K+ in credit lines actively sold on Telegram.

1

Data Breach

Criminals obtain your client's PII — including SSN, DOB, and address — often originating from a prior breach or a targeted phishing attack.

2

Identity Takeover

The fraudster poses exactly as the homeowner, bypassing security protocols to request HELOC access directly from a financial institution.

3

Sold on Telegram

The compromised access is listed on dark web channels. It is advertised as "Controlled" or "Spammed" and priced by the credit limit.

4

Funds Drained

A buyer withdraws the available funds rapidly, often completing the theft before the real homeowner notices any change to their account.

ITRC | IDENTITY THEFT RESOURCE CENTER

The HELOC Threat Landscape

Why Realtors Are on the Front Line

Homeowners with significant equity are prime targets. Your clients' transaction records, property data, and personal information are high-value assets to fraudsters.

A HELOC can be opened and drained before the seller even closes on a new home.

Sold Openly Online

- **"Controlled" Accounts:**
  The fraudster already has access to the victim's banking environment (full identity takeover achieved).
- **"Spammed" Accounts:**
  Mass-attempt campaigns launching multiple simultaneous takeover attempts at a massive scale against real homeowners.

Research: Prof. David Maimon, Georgia State University

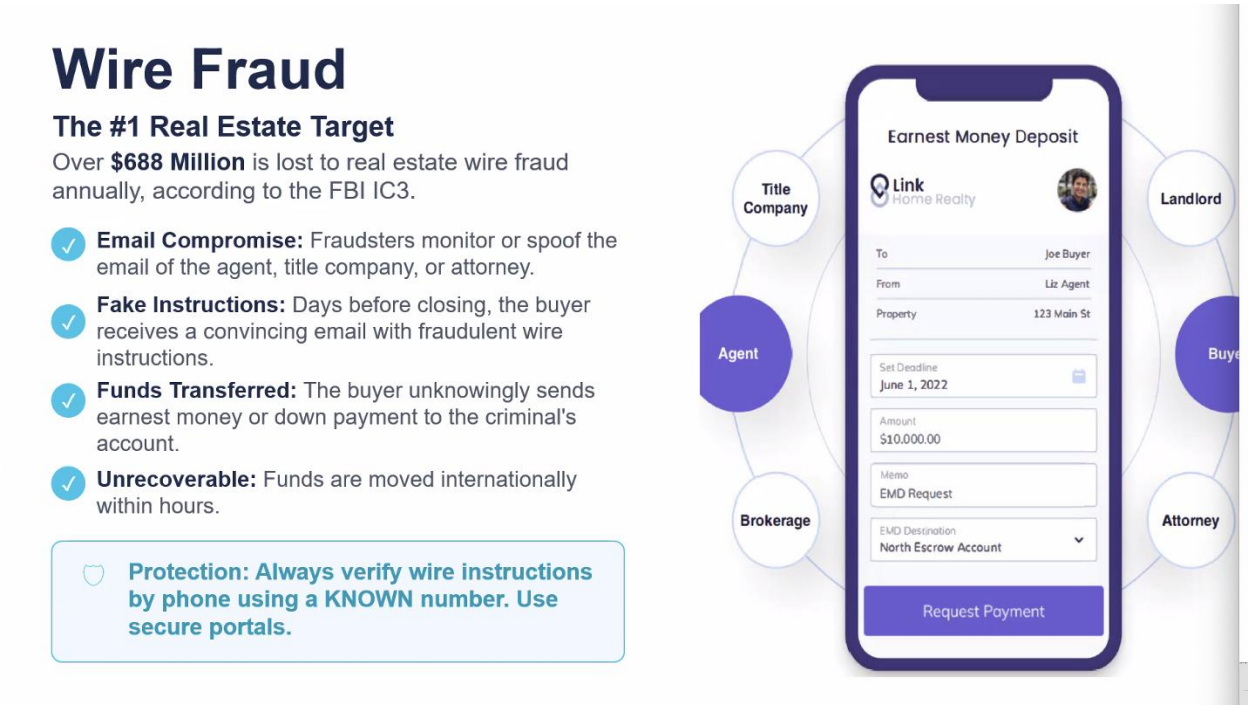
ITRC | IDENTITY THEFT RESOURCE CENTER

Real Estate Wire Fraud Continues

Wire fraud remains one of the costliest scams affecting real estate transactions. According to FBI data cited during the presentation more than $688 million is lost annually to real estate wire fraud. The scheme often occurs shortly before closing when criminals send buyers fake wire instructions that appear to come from agents, attorneys or title companies.

To prevent losses, experts recommend:

- Verifying wire instructions by phone.
- Using trusted contact information.
- Confirming any last-minute changes independently.
- Using secure communication portals whenever possible.



Emotional Toll Often Overlooked

Terry emphasized that identity theft affects more than finances.

ITRC research found:

- 36% of victims lose more than $10,000.
- 60% experience severe anxiety after a data breach.
- 67% of identity theft victims reported considering self-harm while navigating recovery alone.

“They feel isolated, they feel shame, and they don't want to tell someone they're going through these scams,” Terry said.

Realtors Share Real-World Experiences

Several attendees described fraud incidents they have encountered, including:

- A tenant allegedly using another person's Social Security number to secure housing.
- Fraudulent rental listings created using photos copied from legitimate real estate advertisements.
- Difficulties obtaining law enforcement assistance in identity fraud investigations.

The discussion highlighted the growing role Realtors play in identifying and reporting fraud.

Resources Available

Both organizations encouraged Realtors and consumers to report fraud and seek assistance.

Key resources include:

- ReportFraud.ftc.gov for scam reporting.
- IdentityTheft.gov for recovery plans and identity theft reporting.
- The Identity Theft Resource Center's free victim assistance services.
- FTC small-business cybersecurity and fraud-prevention resources.

The presenters emphasized that awareness, verification and prompt reporting remain the best defenses against increasingly sophisticated scams.

As cybercriminals continue to evolve their tactics, Realtors are being called upon not only to protect their businesses, but also to help clients navigate one of the most vulnerable aspects of any real estate transaction: the protection of personal and financial information.

– David R. Walker

If you paid a scammer

You paid by	Contact
Credit card	Your card issuer
Wire transfer	Wire transfer company
Gift card	Company that issued the gift card
Money transfer app	Company behind the money transfer app
Cryptocurrency	Company you used to send the crypto

If you gave a scammer your personal information

- Did someone use your information?
  - Yes? IdentityTheft.gov
  - No? IdentityTheft.gov/DataBreach

Get your free credit report at
AnnualCreditReport.com