OLD REPUBLIC TITLE

A Deal Disrupted: Scams, Loss, and Recovery

A Panel Presentation

Thomas Cronkright, CertifID; **Doug Pollock**, IDSnetwork, Inc.; **Marcie Anthony**, FVP, Senior Claims Counsel & Regional Claims Manager

1

Introductions

2

Introduction to our Panelists

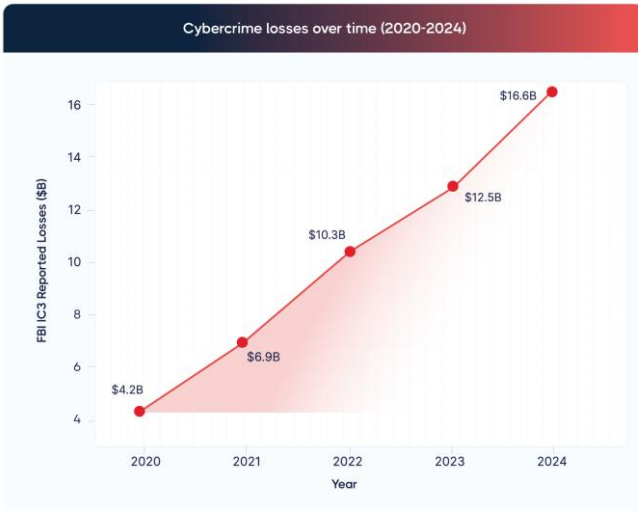
- **Tom Cronkright –**
  - Co-Founder & Executive Chairman/CEO of CertifID
  - CEO of Sun Title
  - Attorney, Real Estate Broker, Title Insurance Producer, and Expert
- **Doug Pollock**
  - President & Founder, IDSnetwork, Inc.
  - Investigator into white collar crime, cyber crime, employee theft, defalcations, real estate and mortgage fraud
  - Certified Fraud Examiner

3

Fraud Trends

4

Can you tell me about the state of fraud in 2026?



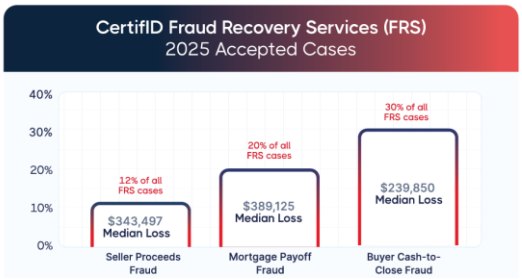
5

What makes Real Estate a Prime Target?

- **High-value transactions:** The median U.S. home price in 2025 exceeds $400,000, and commercial transactions can reach into the millions.
- **Time pressure:** Closings operate on tight deadlines, creating urgency that criminals exploit.
- **Multiple parties:** Buyers, sellers, agents, lenders, title companies, and attorneys all communicate, creating numerous impersonation opportunities.
- **Public information:** Property records, listings, and transaction details are often publicly accessible, giving criminals the intelligence they need.
- **Fragmented security:** Unlike banking or other highly regulated sectors, real estate lacks unified cybersecurity standards, with practices varying widely by state and company.

6

What fraud types are you seeing?



Buyer cash-to-close fraud was the most common fraud type in 2025, representing 30% of cases with a median loss of $239,850. This fraud type often preys on first-time homebuyers who are unfamiliar with the process and eager to complete their purchase.

Mortgage payoff fraud was the most damaging category last year, representing 20% of all FRS cases with a median loss of $389,125.

Seller net proceeds theft accounted for 12% of cases with a median loss of $343,497.

Account Takeovers, ACH Fraud, and Wire Transfers: The Growing Threat Behind the Screen

Account takeover (ATO) fraud and unauthorized ACH and wire transfers continue to rise at an alarming pace. What we are seeing across recent investigations is not just isolated incidents, but organized, repeatable playbooks executed by sophisticated threat actors targeting individuals, businesses, and financial institutions alike.

7

What is Account Takeover Fraud?

How the Fraud Typically Unfolds

In many recent cases, threat actors first infiltrate an online banking account through credential compromise, malware, phishing, or device compromise. After gaining access, they initiate outbound ACH transfers or wires to accounts under their control.

But the fraud doesn't stop there.

Instead, funds are quickly moved again — often within minutes or hours — through second- and third-hop accounts. This layered movement serves one purpose: **to complicate recovery and frustrate tracing efforts.**

The Critical Linchpin: Multi-Factor Authentication (MFA)

Despite the sophistication of these schemes, one common denominator continues to emerge: **compromise of multi-factor authentication (MFA).**

8

What to do about Account Takeover Fraud?

Practical Steps to Protect Yourself

While the tactics continue to evolve, several defensive measures remain highly effective:

1. Monitor Accounts Closely

Frequent review of banking activity can help identify unauthorized transactions early — when recovery chances are highest.

2. Never Share MFA Codes

Banks will **not** ask for MFA codes over the phone. Treat any request for an authentication code as a red flag.

3. Be Skeptical of Incoming Bank Calls

9

What to do about Account Takeover Fraud?

What to Do if You Suspect Fraud

Speed is critical. If suspicious activity is detected:

Immediately contact your bank

Document the activity

Report the incident to the FBI's IC3 (Internet Crime Complaint Center)

Engage experienced investigators early to assist with tracing and recovery

10

Are we still seeing seller impersonations?

YES

11

What are some prevention tips to avoid fraud?

1. Securing Communications
2. Identity Verification
3. Controlling the Notarization
4. Education & Security Awareness
5. Incident Response Plan

12

13