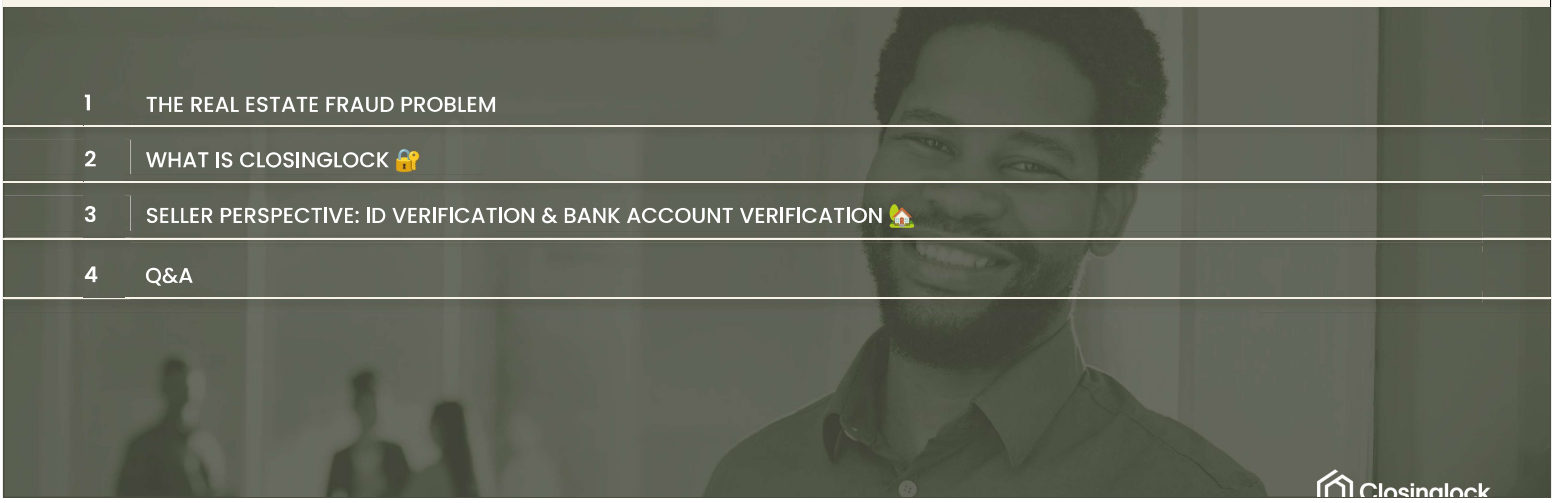
Closinglock | Advocus

Closinglock Overview

Agenda

Closinglock Overview:



1 THE REAL ESTATE FRAUD PROBLEM

2 WHAT IS CLOSINGLOCK 🔐

3 SELLER PERSPECTIVE: ID VERIFICATION & BANK ACCOUNT VERIFICATION 🏡

4 Q&A

Closinglock

KEY TAKEAWAYS

What the 2025 FBI IC3 Report Means for Real Estate

The data is clear, the trend is accelerating, and the stakes for real estate professionals have never been higher.

1

Fraud Is Massive & Growing

$20.9B lost in 2025, a **26%** jump from 2024. Cybercrime is not plateauing. It is accelerating every year.

2

BEC & Wire Fraud Are the #2 Loss Category

$3.05B lost to Business Email Compromise. 86% of those losses moved via wire transfer.

3

Real Estate Is a Prime Target

$275M in real estate-specific fraud. The closing is the single most dangerous and highest-value moment in any transaction.

4

AI Is Making Scams Undetectable

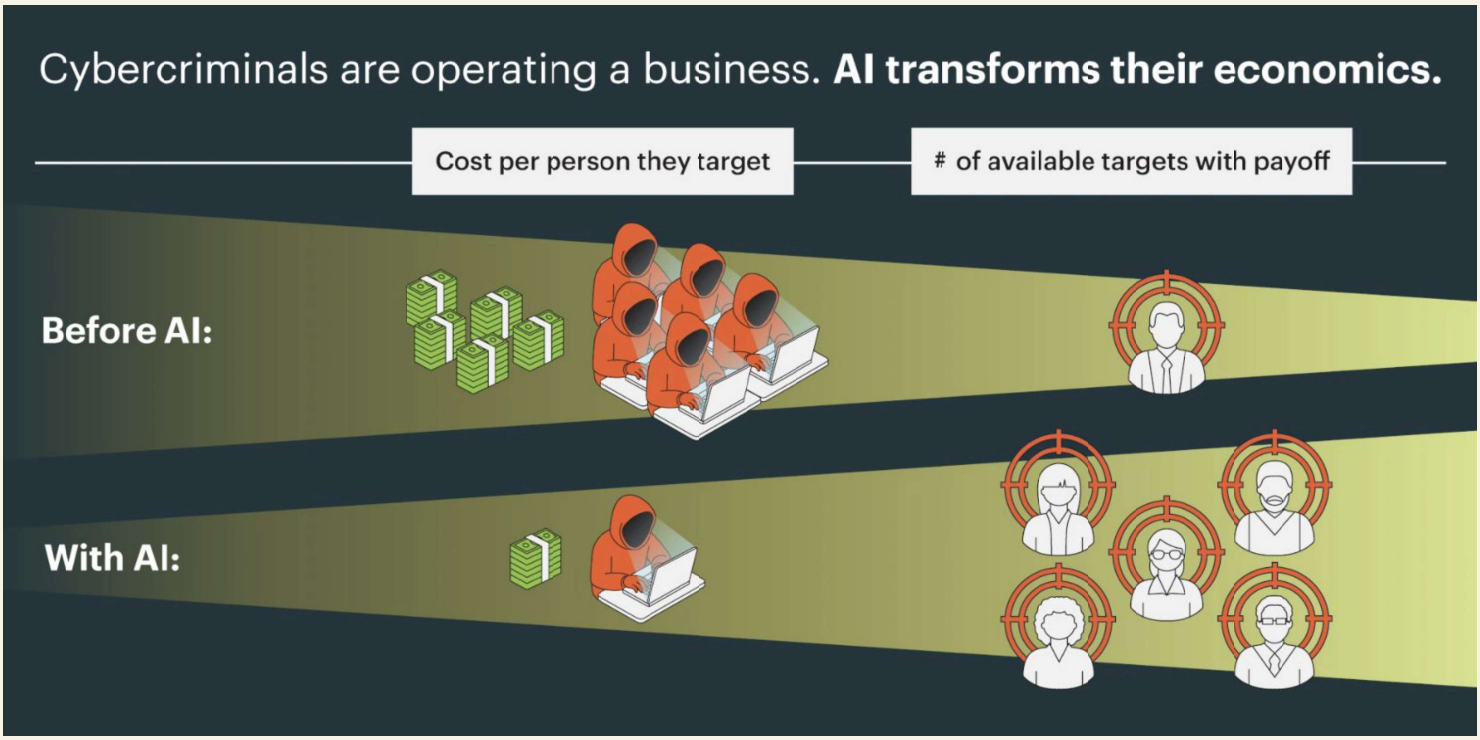
$893M in AI-enabled fraud. Voice cloning and deepfakes are now mainstream threats. Deepfake fraud is up 900% YoY.

5

Prevention Is the Only Reliable Answer

The FBI's best recovery effort succeeds only 58% of the time. Once money is gone, it is usually gone forever.

Source: FBI IC3 2025 Annual Report • closinglock.com



AI-ENABLED FRAUD · FBI IC3 2025

AI Is Supercharging Every Attack

Voice cloning makes the fake bank call undetectable. Deepfakes make the fake closing agent indistinguishable. Synthetic documents make the fake payoff statement perfect.

$893M
AI-enabled losses 2025

900%
Deepfake fraud growth YoY

54%
AI phishing click rate (matches human experts)

53%
How often humans correctly detect AI voices

Voice Cloning
Needs just 30–60 seconds of audio to clone your attorney, lender, or title agent's voice and redirect wires by phone.

Deepfake Video
Fake video calls with spoofed identities posing as legitimate closing agents — increasingly indistinguishable from real.

AI Phishing
Perfect grammar, matched email style, context-aware content. 90% cheaper than hiring skilled criminals.

Synthetic Documents
Fake pay stubs, IDs, checks, and closing documents generated in seconds — impossible to spot by eye.

One Solution. No Usernames. No Passwords.

Direct Wire Fraud Insurance
Protect your business with $5M in direct coverage for all **wire instructions and payments** sent through the system – no confusing exclusions and at no extra cost.

Identity Verification
Verify identities instantly using non-public data sources.

Wire Instruction Exchange
Send and receive verified wire instructions.

SecurePay
Receive earnest money deposits and cash-to-close as good funds.

Payoff Verification
Confirm loan payoff accounts and routing numbers in real-time.

Document Request and Exchange
Conveniently receive and exchange closing documents with your clients.

eSigning and Forms
Closinglock x docusign

Request and receive government-compliant eSignatures and intake forms.

Two-way text messaging
A better way to connect—on both sides of the closing.

Business and Personal Account Verification
Instantly verify business and personal bank accounts to ensure secure and accurate fund transfers before closing.

Closinglock

Seller Experience

Closinglock

Seller Experience

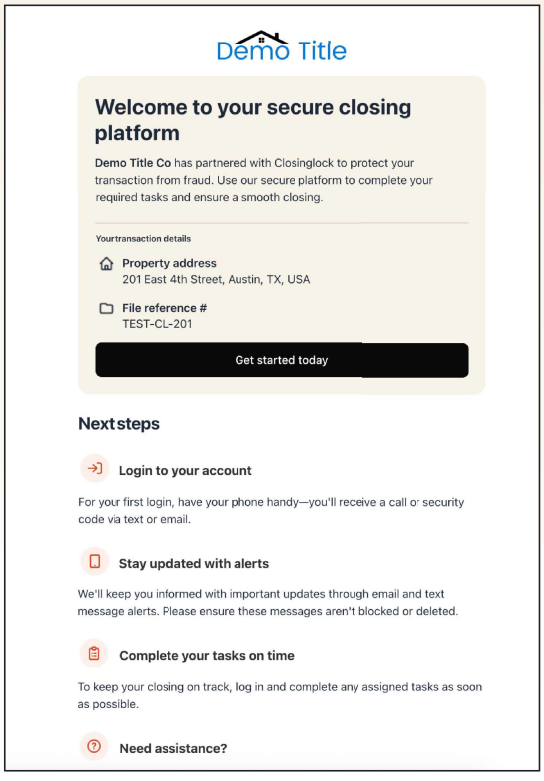
Seller receives the email from **no-reply@closinglock.com** in their inbox.

Property is confirmed.

Tasks assigned from the file will be included in the email body.

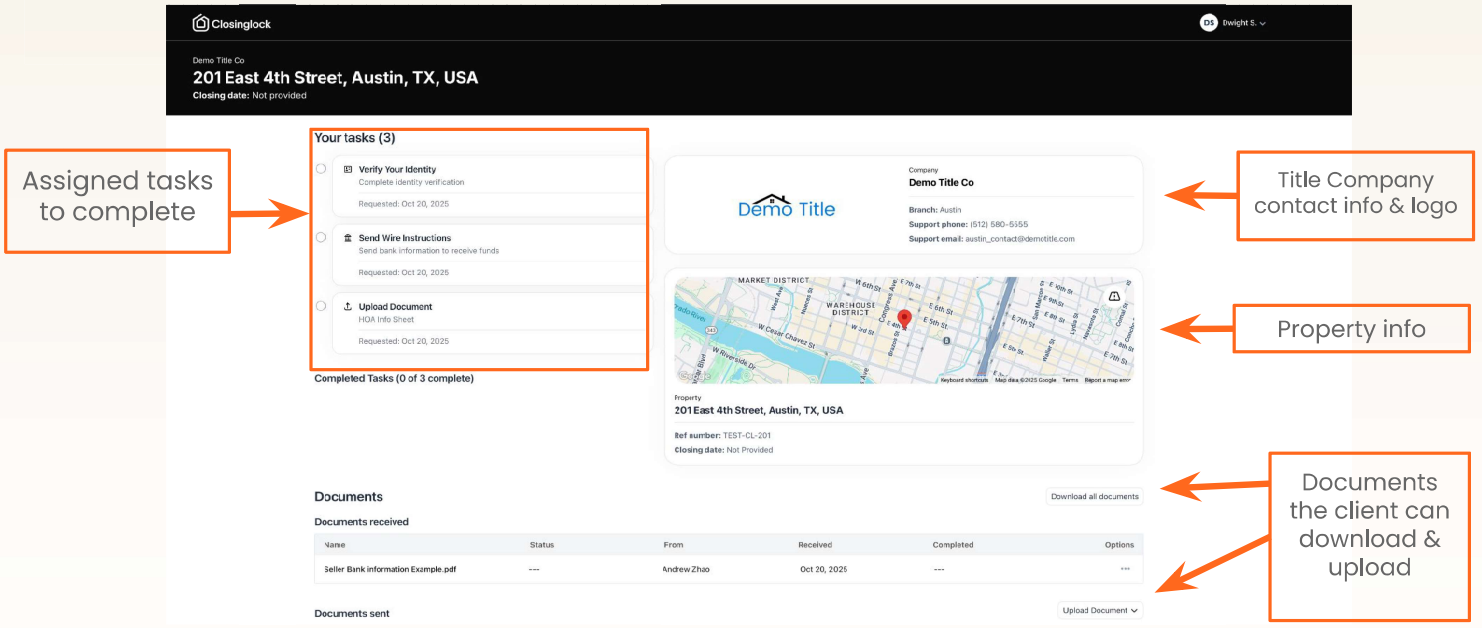
Seller selects "**Complete my open tasks**" to access Closinglock platform.

If no tasks are assigned, it will say "**Get started today**".



Closinglock

Seller Experience

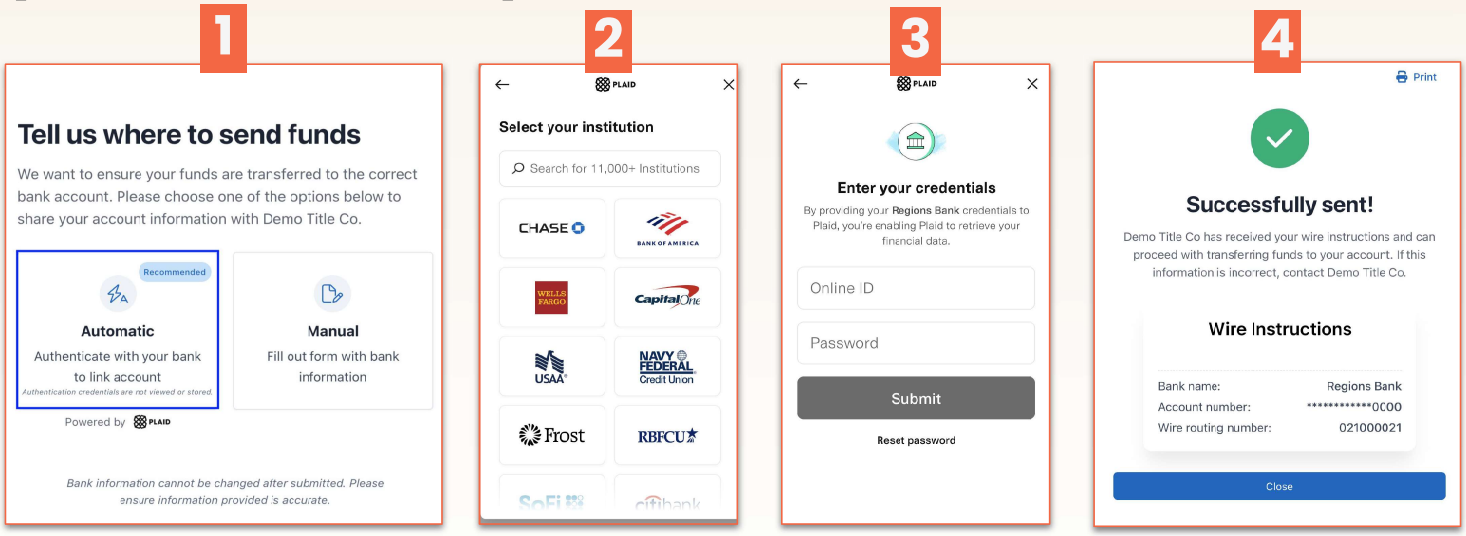


Closinglock

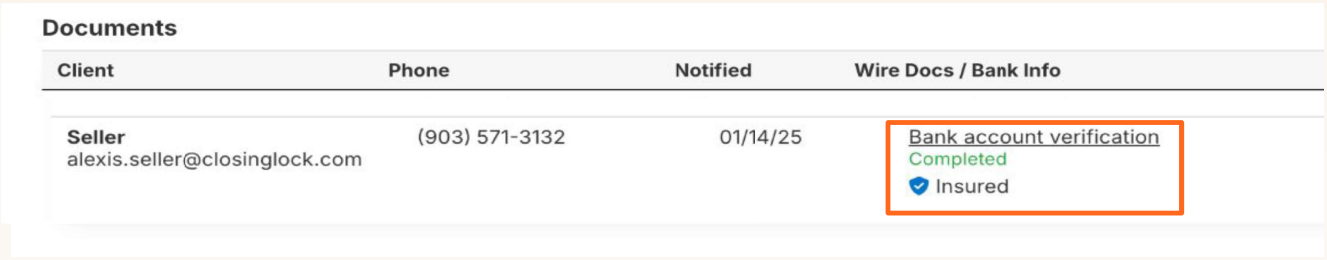
How Sellers Upload Wire Instructions

Closinglock

Automatic Wire Instructions Option (Recommended)

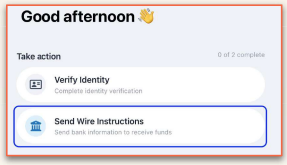


Wire Instructions (Automatic Workflow)

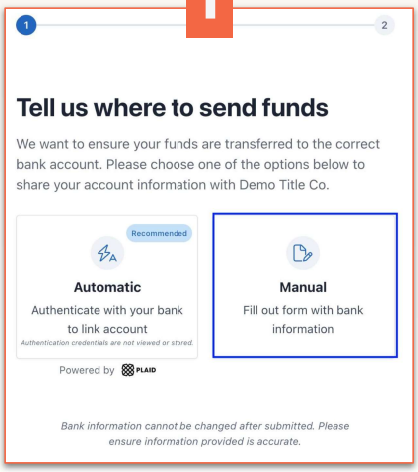


- When a client automatically provides bank information, it will show that **it is insured.** No additional actions are required.
- Click the link to view the associated certificate.

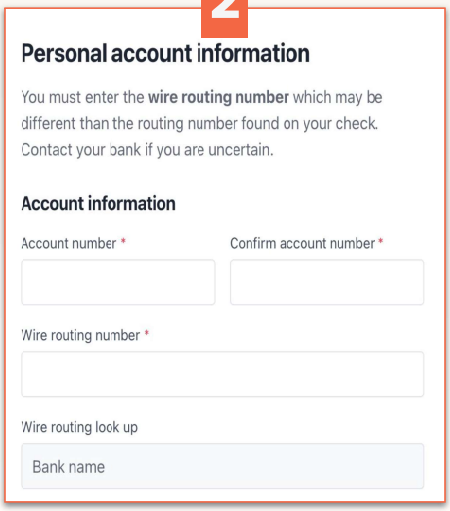
Manual Wire Instructions Option



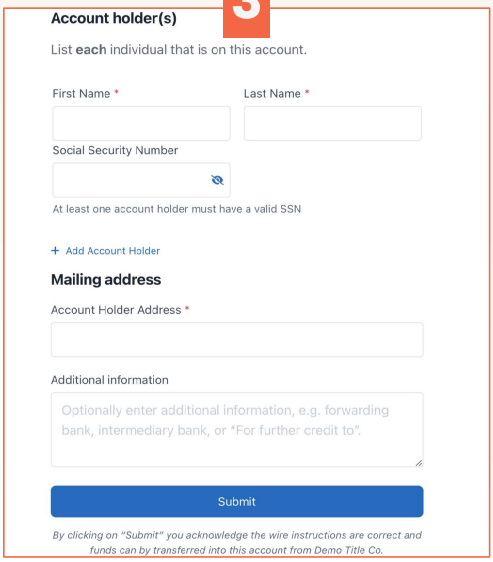
1



2

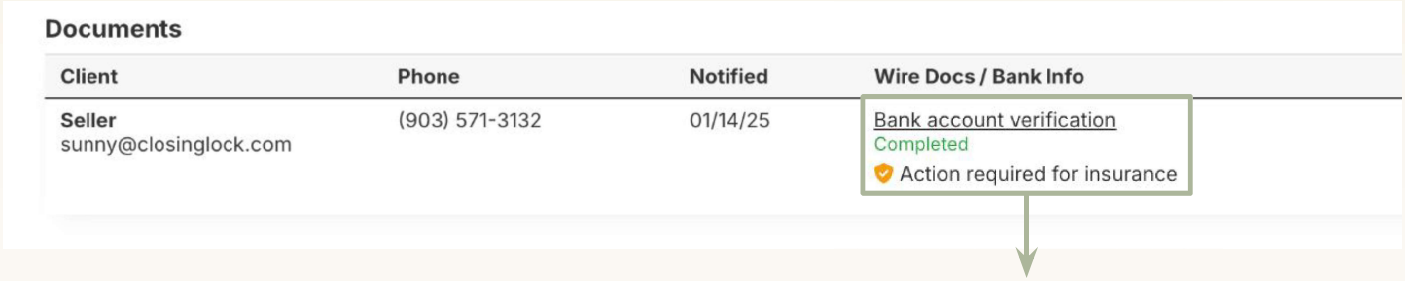


3



Closinglock

Wire Instructions (Manual Workflow)



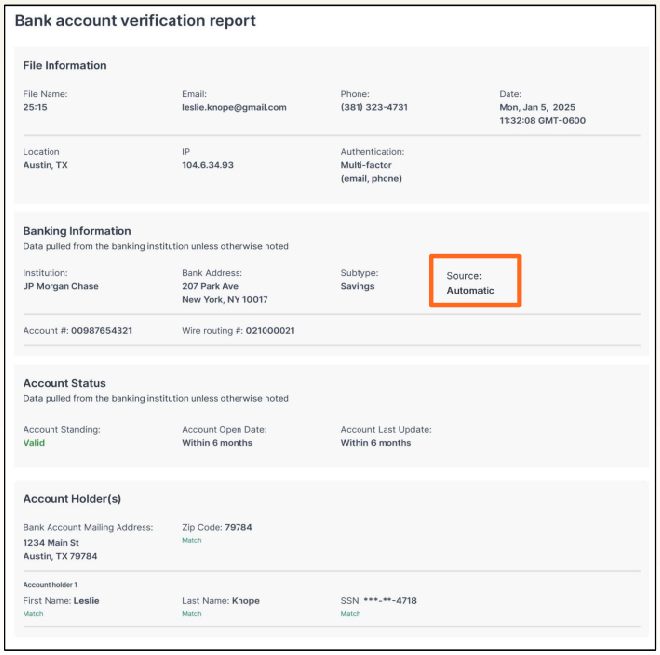
- When client manually entered bank information, it will show that there is an action required for insurance coverage.
- **Your client** will need to **complete and pass the Identity Verification request** in order for insurance to cover this action.
- Click the link to view certificate.

Closinglock

Bank Account Verification Report

This report is created by Closinglock when a seller completes a wire instruction request.

Source: shows which method the client used to submit their bank information.



Bank account verification report

File Information

File Name: 25:15
Email: leslie.knope@gmail.com
Phone: (381) 323-4731
Date: Mon, Jan 5, 2025 11:32:08 GMT-0600

Location: Austin, TX
IP: 104.6.34.93
Authentication: Multi-factor (email, phone)

Banking Information

Data pulled from the banking institution unless otherwise noted

Institution: JP Morgan Chase
Bank Address: 207 Park Ave New York, NY 10017
Subtype: Savings
Source: Automatic

Account #: 00987654321
Wire routing #: 021000021

Account Status

Data pulled from the banking institution unless otherwise noted

Account Standing: Valid
Account Open Date: Within 6 months
Account Last Update: Within 6 months

Account Holder(s)

Bank Account Mailing Address: 1234 Main St Austin, TX 79784
Zip Code: 79784 Match

Accountholder 1

First Name: Leslie Match
Last Name: Knope Match
SSN ***-**-4718 Match

Closinglock

Q&A

Any questions?

Closinglock

Thank you!

Advocus National Title Insurance Company
Webinar Resource Materials
Wire Fraud and Identity Theft Protection with ClosingLock
May 18, 2026

From a title insurance claims perspective, the biggest fraud targets right now are not random residential resale deals. The industry is seeing very specific transaction profiles getting hit over and over.

Here's what is showing up most frequently across the market right now:

1. Vacant Land Transactions (by far the biggest target)

This is the #1 fraud category nationally right now. Most of these are seller impersonation frauds.
The typical setup:

- Vacant lot
- Out-of-state owner
- Property owned free and clear
- Seller only communicates by email/text
- Wants a quick cash closing
- Refuses in-person meeting or video verification
- Pushes for remote/mobile notary
- Wants proceeds wired immediately

The scammer pulls ownership info from public records, creates fake IDs, lists the property with an unsuspecting agent, and tries to close before anyone notices. Industry surveys are showing roughly 60%+ of reported title fraud incidents now involve vacant land.

This is especially common in:

- Florida
- Texas
- Arizona
- Tennessee
- Carolinas
- Rural recreational land markets

From a claims perspective, these become:

- Forged deed claims
- Lack of title claims
- Forgery/impersonation losses
- Litigation over invalid conveyances

2. Mortgage-Free Homes / Elderly-Owned Property

Fraudsters love properties with:

- no mortgage,
- elderly owners,
- absentee owners,
- inherited property,
- or long-time ownership.

Why? Because no lender is monitoring the title.

A lot of the current deed theft activity involves:

- forged deeds,
- fake POAs,
- fake HELOCs,
- fraudulent refinance transactions,
- or foreclosure rescue scams.

These cases are exploding in urban areas with rapidly appreciating property values.

3. Refinance Transactions

This surprises a lot of people.
Recent industry studies are showing refinance fraud/forgery claims are now an enormous loss category for title underwriters — reportedly over 40% of title insurer fraud losses in some studies.

Common refinance fraud patterns:

- Identity theft
- Forged payoff statements
- Fake borrowers
- HELOC fraud
- Fraudulent satisfactions/releases
- Straw borrower activity
- Wire diversion during payoff

The losses are severe because:

- loan amounts are high,
- lenders fund quickly,
- and the fraud is often discovered after disbursement.

4. Remote Online Notarization / Remote Closings
Remote closings themselves are not the problem — weak identity verification is.

Claims teams are seeing fraudsters exploit:

- remote notaries,
- fake IDs,
- AI-generated documents,
- deepfake video calls,
- and spoofed credentials.

The “seller” insisting on:

- no in-person interaction,
- overseas travel,
- bad camera,
- “can’t video today,”
  is now one of the biggest red-flag combinations in title operations.

5. Wire Fraud / Business Email Compromise

This remains a constant problem.
The fraud may not always become a covered title claim, but title companies are absorbing huge operational losses and cyber exposure from:

- altered wiring instructions,
- hacked email chains,
- spoofed realtor/lender/title domains,
- and social engineering.

Funding Shield data showed almost half of reviewed transactions had at least one fraud-risk indicator recently.
The most vulnerable files are:

- fast closings,
- all-cash deals,
- vacant property deals,
- and files where communication suddenly changes near funding.

6. Estate / Probate / Heirship Transactions

These are getting hit more often because scammers monitor:

- obituaries,
- probate filings,
- tax records,
- and vacant inherited homes.

Common fraud patterns:

- forged heirship affidavits,
- fake family members,

- fake POAs,
- impersonated executors,
- fraudulent deed transfers after death.

There's also increasing use of AI-generated identity materials tied to deceased owners.

7. Investor / LLC-Owned Properties

Especially:

- single-purpose LLCs,
- non-local investors,
- rental portfolios,
- and distressed properties.

Fraudsters know these owners:

- often never visit the property,
- may have outdated contact info,
- and rely heavily on email-only communication.

Vacant rentals and investment land are prime targets.

Biggest Operational Red Flags Title Companies Are Watching

Across the industry, the same patterns keep appearing:

- Seller pushes urgency
- Cash transaction
- No mortgage payoff
- Seller won't meet in person
- Seller insists on remote notary
- Foreign phone number
- Newly changed mailing address
- Property is vacant
- Owner is out-of-state
- Under-market pricing
- Proceeds going to unrelated account
- Email-only communication
- Different signatures across docs
- Unknown/mobile notary
- Seller knows surprisingly little about property

The Most Dangerous Combination Right Now

If you asked most claims counsel or underwriting attorneys today, the highest-risk file is probably:

Vacant land + free and clear + out-of-state seller + remote closing + cash buyer.
That combination is generating a huge percentage of current fraud alerts and claims activity.

Real Estate Wire Fraud Statistics

FBI IC3 2025 Report
The FBI's Internet Crime Complaint Center (IC3) reported:

- **12,368 real estate fraud complaints** in 2025
- **$275.1 million in reported losses**
- Losses increased substantially from:
    - **$173 million in 2024**
    - **$145 million in 2023**
- 2022 remains the peak year at approximately **$397 million in losses**

The FBI classifies these incidents broadly as:

- wire fraud,
- business email compromise (BEC),
- fraudulent closings,
- rental scams,
- title/deed fraud,
- and real estate investment fraud.

Business Email Compromise (BEC) Impact
BEC remains one of the highest-loss cybercrime categories nationwide.

According to the FBI:

- BEC schemes caused more than **$3 billion in losses** across industries in 2025.

Real estate transactions are especially vulnerable because:

- large-dollar wires move quickly,
- transactions rely heavily on email,
- and closings involve multiple parties exchanging wiring instructions.

Real Estate Wire Fraud Recovery Challenges
The FBI highlighted multiple real estate cases involving:

- fraudulent wire instructions,
- spoofed attorney/title company emails,
- and six-figure closing losses.

One cited 2025 case involved:

- a fraudulent home-closing wire of more than **$449,000** that was only recovered because the FBI's Financial Fraud Kill Chain (FFKC) intervened quickly.

Industry experts consistently say:

- recovery odds decline dramatically after the first 24–72 hours,
- and many victims never fully recover funds.

AI's Growing Role in Wire Fraud
The FBI specifically warned that AI is accelerating fraud sophistication through:

- voice cloning,
- fake documents,
- deepfake video,
- synthetic identities,
- and highly convincing phishing emails.

This is becoming particularly dangerous for:

- remote closings,
- remote online notarization,
- and email-only transactions.

Seller Impersonation Fraud Statistics
ALTA / NDP Analytics Study
One of the most important datasets comes from the American Land Title Association (ALTA).
Their industry study found:

- **28% of title insurance companies experienced at least one seller impersonation fraud attempt in 2023**
- **19% experienced an attempt in April 2024 alone**

That statistic shocked a lot of underwriters because it confirmed these are no longer isolated incidents.

Most Common Seller Impersonation Targets
According to ALTA and multiple fraud investigations, the most targeted properties are:

- Vacant land
- Mortgage-free homes
- Investment properties
- Inherited property
- Out-of-state owner properties
- Elderly-owned properties

The most dangerous profile continues to be:
Vacant land + remote seller + cash deal + no mortgage payoff.

Deed Theft / Title Theft Trends
National deed theft incidents are rising rapidly.
Recent reporting noted:

- deed theft complaints in some jurisdictions have **tripled between 2023 and 2025**
- more than **58,000 victims nationwide reported $1.3 billion in real-estate-related fraud losses from 2019–2023**

Why Seller Impersonation Is Increasing
Industry experts cite several reasons:
1. Public Records Access

Fraudsters can easily obtain:

- ownership data,
- signatures,
- LLC information,
- tax records,
- and mailing addresses.

2. AI & Deepfake Technology

Fraudsters now use:

- AI-generated IDs,
- deepfake Zoom calls,
- cloned voices,
- and synthetic documents.

One reported case involved a fraudster attempting to sell vacant land using a looping AI-generated video identity during a verification call.

3. Remote Closings

The increase in:

- remote notarization,
- remote seller signings,
- and fully digital closings

  has materially increased exposure.

Current Operational Risk Indicators

Title companies are now treating these as major red flags:

- Seller refuses in-person meeting
- Email-only communication
- Sudden urgency
- Vacant property
- Free-and-clear title
- Foreign phone numbers
- New mailing address
- Remote/mobile notary requests
- Wire proceeds to unrelated account
- Seller lacks property knowledge
- Deepfake-looking video calls
- ID inconsistencies

What Underwriters Are Most Concerned About Right Now

Most title claims counsel and cyber-risk teams would probably identify these as the highest-risk current trends:

1. Seller impersonation on vacant land
2. Business email compromise/wire diversion

3. AI-assisted identity fraud
4. Fake POAs and forged deeds
5. Remote notarization vulnerabilities
6. Fraud involving elderly or deceased owners

The combination of AI tools plus remote transaction workflows is what has claims and underwriting departments especially concerned in 2026.

Best Practices to Prevent Wire Fraud

1. Never Email Wiring Instructions Without Verification Protocols

This is still the single most important rule.

Best practice:

- Provide wiring instructions:
  - through secure portals,
  - encrypted delivery,
  - or verified PDF delivery only.
- Include a standing written warning:

"Our wiring instructions will never change by email."

Many firms now:

- prohibit wiring instructions in the body of emails entirely,
- and require verbal confirmation through a known phone number.

2. Require Live Verbal Verification for All Wires

Before ANY disbursement:

- independently verify wiring instructions by phone,
- using a previously known and trusted number,
- not a number from the latest email.

This applies to:

- buyer funds,
- seller proceeds,
- mortgage payoffs,
- commissions,
- and vendor wires.

The most sophisticated frauds today involve:

- spoofed email domains,
- hacked email threads,
- and perfectly timed last-minute "updated wiring instructions."

3. Use Multi-Factor Authentication Everywhere

Require MFA for:

- email accounts,
- document systems,
- wire platforms,
- escrow software,

- and remote access.

A shocking percentage of successful wire fraud claims still begin with:

- compromised Microsoft 365 accounts,
- weak passwords,
- or reused credentials.

4. Implement Mandatory "Wire Hold" Procedures

Many law firms and title companies now use:

- same-day wire freezes,
- supervisory approval thresholds,
- or delayed disbursement policies.

Example:

- no wire changes within 48 hours of closing,
- no first-time recipient wires without partner approval,
- no international wires without secondary verification.

5. Train Staff to Recognize Social Engineering

Fraudsters rarely "hack" systems directly anymore.
They manipulate people.
Your staff should be trained to spot:

- urgency,
- secrecy,
- emotional pressure,
-
- last-minute changes,
- altered email domains,
- grammatical inconsistencies,
- and unusual communication behavior.

One of the most effective controls is simply:
"Slow the transaction down when something feels off."

6. Use Secure Transaction Platforms

Firms increasingly use:

- secure client portals,
- encrypted messaging,
- identity-authenticated signing systems,
- and transaction-management platforms with audit trails.

Examples include:

- Qualia
- SoftPro
- CertifID
- ClosingLock

Many claims teams now view unsecured email-only transactions as an avoidable risk exposure.

Best Practices to Prevent Seller Impersonation Fraud

7. Independently Verify Seller Identity

This is now essential, especially for:

- vacant land,
- remote sellers,
- free-and-clear properties,
- LLC-owned property,
- and estate transactions.

Best practices include:

- government ID verification,
- biometric verification,
- live video verification,
- knowledge-based authentication,
- and cross-checking public records.

Do NOT rely solely on:

- emailed IDs,
- DocuSign identity checks,
- or mobile notaries.

8. Require Live Video Calls With Sellers

A short live video meeting is becoming standard in higher-risk files.
Ask questions only the real owner should know:

- purchase history,
- neighborhood details,
- tax history,
- mortgage history,
- local landmarks,
- property condition.

Fraudsters often know surprisingly little beyond what appears in public records.

9. Scrutinize Vacant Land Transactions Aggressively

Vacant land is currently the #1 seller impersonation target.
Enhanced controls should include:

- direct outreach to owner via independently sourced contact info,
- mailed verification letters,
- notarization scrutiny,
- title history review,
- and heightened escrow review.

Many underwriters now require escalation procedures specifically for:
vacant land + remote seller + cash transaction.

10. Verify the Notary

Fraudulent notarizations are increasing dramatically.
Best practices:

- independently verify notary commissions,
- review seals/signatures carefully,
- avoid unknown mobile notaries when possible,
- and scrutinize remote online notarization sessions.

Red flags:

- blurry seals,
- inconsistent signatures,
- rushed notarizations,
- or foreign-location signings.

11. Review Behavioral Red Flags — Not Just Documents

Experienced fraud investigators say behavioral indicators matter as much as paperwork.
Major warning signs:

- seller wants quick close,
- refuses video call,
- email-only communication,
- insists on remote signing,
- foreign phone number,
- unwilling to provide additional documentation,
- proceeds going to unrelated account,
- seller "too cooperative."

A legitimate seller usually tolerates verification.
Fraudsters resist it.

12. Independently Confirm Entity Authority

For LLCs, trusts, or estates:

- verify formation docs,
- operating agreements,
- trust certificates,
- probate authority,
- and signer authority independently.

Fraud involving fake managers, trustees, and executors is increasing.

Law Firm Operational Best Practices

13. Create Written Fraud Escalation Protocols
Every firm should have:

- defined fraud escalation procedures,

- mandatory reporting chains,
- and documented hold authority.

Staff should know:

- who can stop a closing,
- when to escalate,
- and when to involve underwriters or law enforcement.

14. Carry Cyber Liability Insurance

Traditional malpractice coverage often does NOT fully protect against:

- cyber events,
- BEC losses,
- ransomware,
- or fraudulent wire exposure.

Cyber coverage should include:

- social engineering fraud,
- funds transfer fraud,
- breach response,
- and wire loss coverage.

15. Coordinate Closely With the Title Underwriter

Many attorneys wait too long to notify underwriters.
The best practice is:
Escalate suspicious files early.
Underwriters increasingly provide:

- fraud review teams,
- identity-verification tools,
- and transaction-risk guidance.

What the Best Real Estate Attorneys Are Doing Right Now
The firms with the fewest fraud losses generally:

- distrust email,
- slow down unusual transactions,
- independently verify identities,
- require verbal confirmation,
- and treat vacant land files as high-risk by default.

The biggest mindset shift in the industry is this:
Fraud prevention is no longer just an IT issue — it is now a core closing and title practice issue.