A Deal Disrupted: Scams, Loss, and Recovery

Marcie Anthony
FVP, Senior Claims Counsel and Regional Claims Manager, Old Republic Title

Thomas Cronkright II
Co-Founder and Executive Chairman/ CEO, CertifID

Douglas Pollock
President, IDSnetwork, Inc.

CERTIFID

State of Wire Fraud

2026

Fraud trends and insights for the real estate industry

Table of contents

I. Cybercrime: the threat at large

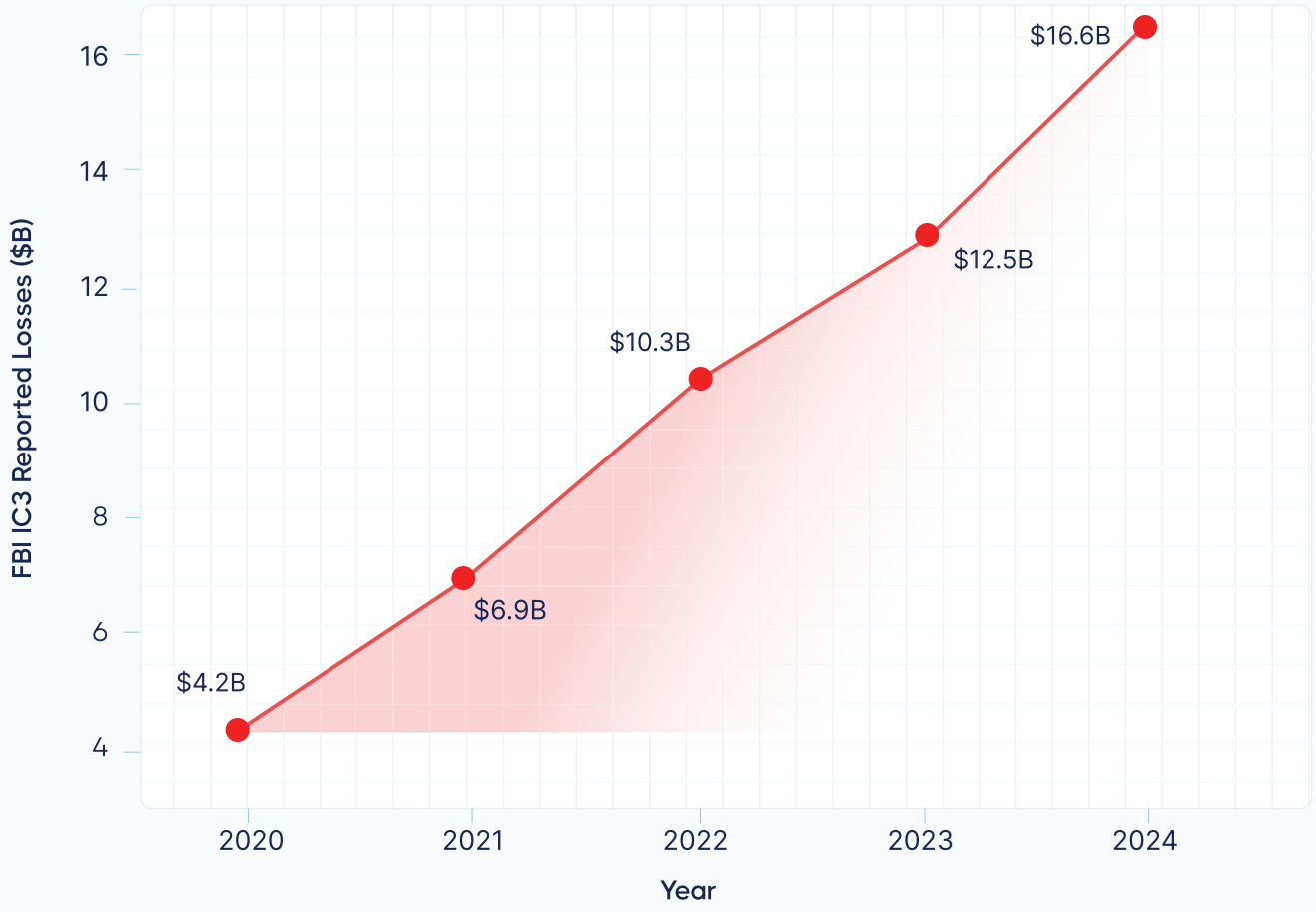
I. Cybercrime: the threat at large

Over the past five years, cybercrime has grown from a distant threat to an epidemic. Last year, the FBI reported Americans lost $16.6 billion to cybercriminals, a staggering 33% increase from the prior year. To put that in perspective, losses have more than tripled since 2020, when the FBI reported $4.2 billion in cybercrime losses.

Business email compromise (BEC) still remains one of the most common and devastating attack vectors, accounting for $2.77 billion in losses across more than 21,000 reported incidents in 2024.

What makes BEC attacks particularly dangerous is exploited trust. When criminals successfully impersonate the people and organizations that victims have every reason to believe, the outcomes are devastating.

Cybercrime losses over time (2020-2024)



Real estate: a prime target in 2026

For an industry like real estate, where processes and transactions rely deeply on trust (and email), cybercrime is an existential threat.

The U.S. real estate industry is facing a growing threat of wire fraud attacks. The sector offers criminals a near-perfect combination of vulnerabilities that make attacks both lucrative and relatively easy to execute. High transaction values and stakes, multiple communicating parties, publicly available information and fragmented security practices all contribute to this risk profile.

- **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.

AI is accelerating the threat

Generative AI is compounding wire fraud threats, and has fundamentally changed the fraud landscape. Criminals now have access to tools that can craft convincing emails, clone voices, and even generate deepfake videos, all at scale and at minimal cost. Last year, fraud analysts estimated 40% of business email compromise phishing emails were AI-generated.

The attacks individuals see today are not the poorly written scam emails of the past; they are grammatically perfect, contextually relevant, and increasingly difficult to distinguish from legitimate communications.

1,760% Year-over-year increase in BEC attacks since generative AI tools became widely available

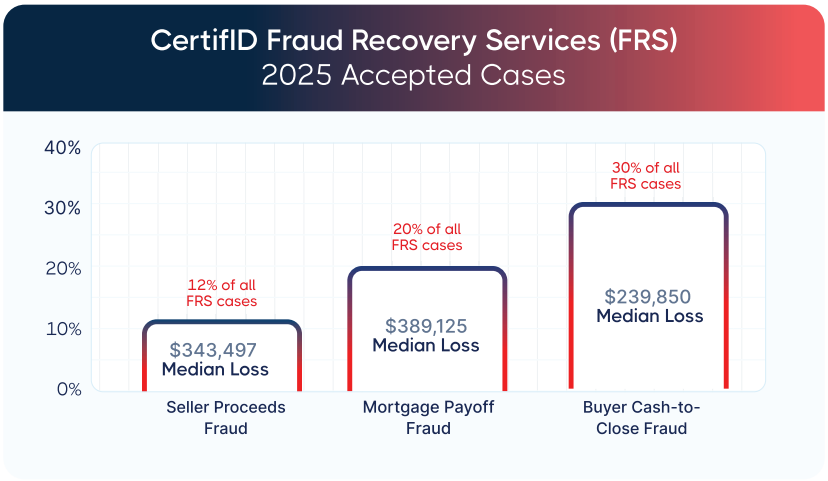
For title professionals on the front lines, they see the change clearly. In our survey of 153 title and escrow professionals, **72.6%** report that fraud attempts are becoming more sophisticated, **60.1%** say fraud attempts are increasing in frequency, and **57.5%** encounter suspicious activity quarterly or more frequently.

60.1% Title professionals who say attempted wire fraud has increased over the past year

The reality is that criminals are getting better, and the industry must keep pace.

Understanding fraud types and their impact

However, not all wire fraud is created equal. CertifID's Fraud Recovery Services data last year revealed three primary categories, each with distinct characteristics and loss profiles that are contributing to the overarching real estate wire fraud problem.



Remaining cases were other forms of payment or unclassified.

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.

How it happens: Criminals impersonate title companies or real estate agents and send fraudulent wire instructions, instructing buyers to act fast or risk losing their home purchase.

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

How it happens: In these scams, criminals intercept or forge payoff statements and redirect mortgage payoff funds to fraudulent accounts. The large dollar amounts and the complexity of verifying payoff instructions make this an attractive target for sophisticated criminal operations.

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

How it occurs: Criminals impersonate sellers and redirect the proceeds of a home sale to their own accounts. These scams exploit the emotional and logistical chaos of moving, when sellers are distracted and communications are frequent.

Victim story: Mortgage payoff fraud

"Like hitting a Mack truck."

Sarah Dombrowski has worked in title for 27 years. In March 2022, she opened her own company, Unique Title and Escrow. She thought she was protected: she had fraud prevention tools in place. Then came the phone call.

On August 7th, 2024, an employee told her a mortgage payoff wire hadn't arrived. $311,785 was missing.

"I felt like I was dying," Sarah recalls. "My chest was tight, my heart was racing. It's like hitting a Mack truck at 60 miles per hour."

Her first concern was her clients. Then came the terrifying realization: her business, her livelihood, her team—everything was in jeopardy. She barely slept for weeks. Insurance companies and attorneys offered no guidance.

The product she had trusted? They told her to call her bank.

CertifID FRS eventually helped return most of the stolen funds, but the experience left a permanent mark. Sarah now operates differently with verified processes in place for every wire.

"I can close my eyes at night knowing I will not experience wire fraud again," she says. "I don't want to be in cybersecurity. I want to focus on title."

Hear Sarah in her own words.

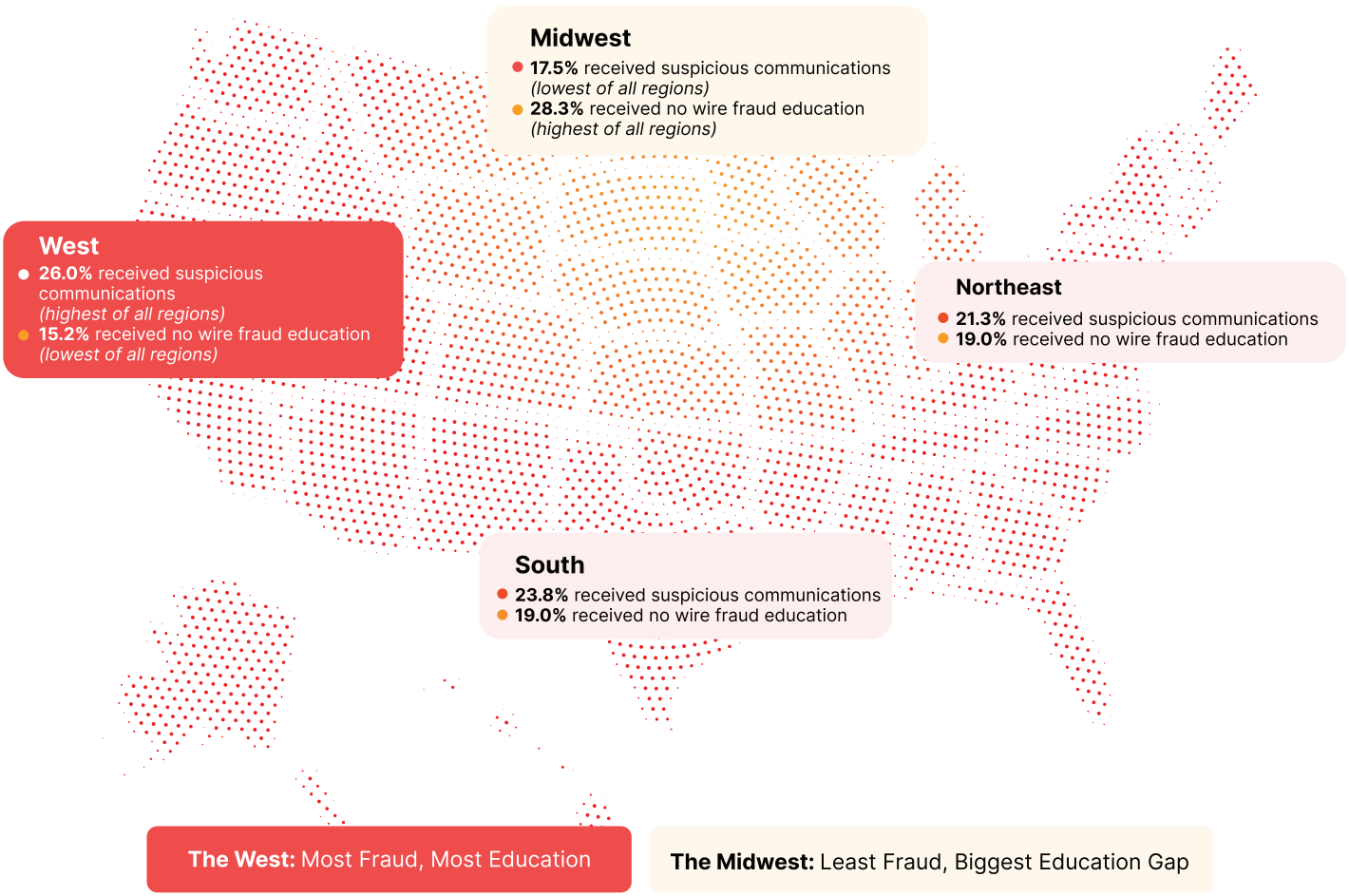
It's important to note that these numbers reflected cases that were reported to us directly. As stated earlier, many cases go unreported due to fear or shame. Understanding these patterns—and that human context—can help businesses identify where they are most vulnerable and where prevention and education efforts should focus.

Geographic risk patterns

Analysis of CertifID platform data also reveals some interesting geographic variation in fraud risk. Florida and Nevada emerged as two of the highest-risk states in 2025, with elevated rates of high-risk transaction markers.*

Consumer survey data shows similar patterns. The Western region reports the highest rate of suspicious communications at 26% of respondents, while the Midwest reports the lowest at 17.5%. Notably, the West also has the lowest rate of consumers receiving no wire fraud education at 15.2%, suggesting that higher threat exposure may be driving greater awareness efforts in those markets.

Fraud Risk & Education Levels Across the U.S.



*These patterns may reflect differences in transaction volumes, property values, regulatory environments, or the concentration of criminal targeting efforts.

II. Consumers are aware and demanding protection

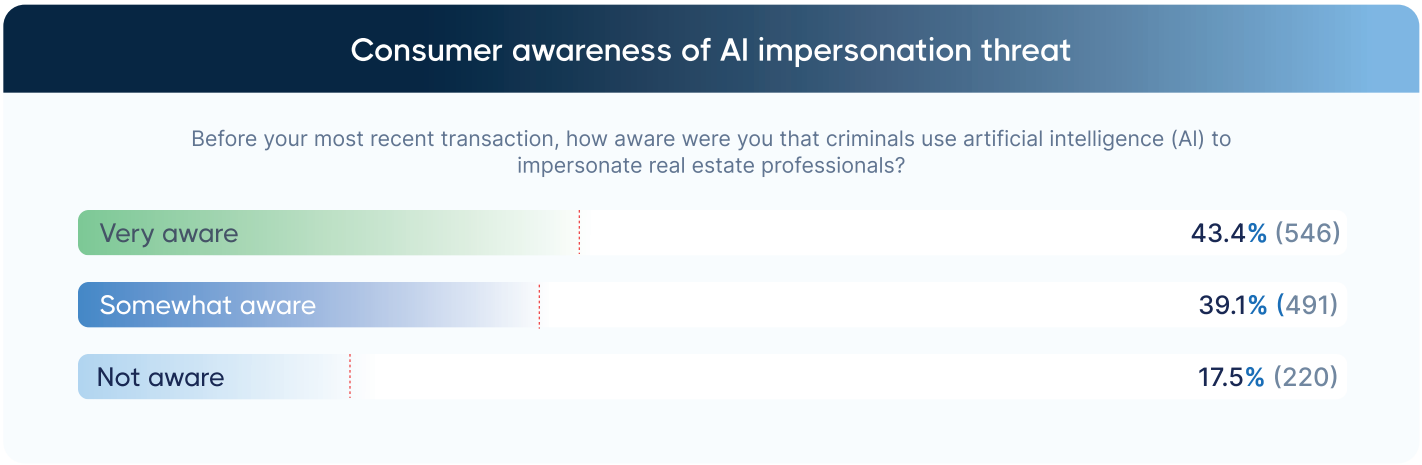
II. Consumers are aware and demanding protection

The days of consumer ignorance about wire fraud are over. Our survey of 1,260 recent home buyers and sellers reveals that awareness has reached a tipping point, and expectations have shifted accordingly. Consumers are no longer asking what wire fraud is. They are asking how you are protecting them from it, and they are making decisions based on the answers they receive.

Awareness has reached critical mass

82% of consumers are aware that AI can be used to impersonate trusted parties during real estate transactions

This datapoint represents a dramatic shift in public consciousness. Consumers understand that the threat is real, technologically advanced, and personally relevant. In addition, more than 1 in 5 consumers (22%) reported receiving suspicious or fraudulent communications during their recent closing process, and 81.8% have either personally experienced fraud or know someone who has. Wire fraud has entered the mainstream consciousness in a way that demands a response from the industry.



Source: CertifID Consumer Survey. October 2025. n=1,260

For businesses still wondering whether to invest in fraud protection, the math is simple: **the vast majority of clients will pay for it, and many will pay more than businesses typically charge.**

Awareness varies by demographics

Despite some overarching trends in awareness, education is still not standard across the real estate industry. These variations should inform how businesses approach different client segments. The data reveals important demographic patterns that have practical implications for client communication and education strategies.

Age matters: Consumers aged 30-39 show the highest AI threat awareness at 88%, while those 60 and older have significantly lower awareness at 66%, a 22-point gap. If you often work with older consumers, they may need more proactive education and reassurance.

Experience matters: Counterintuitively, experienced buyers are more likely to receive suspicious communications (27.5%) than first-timers (16.9%), yet they receive less early education (26.5% vs 33.6%). The industry may be under-serving repeat clients who assume familiarity equals safety.

Region matters: The Midwest has the highest rate of consumers receiving no wire fraud education at 28.3%, while the Northeast leads in early agent education at 34.6%. Regional differences in practice create uneven consumer protection.

The anxiety is real and it is damaging

What is made most clear from the data is that today's consumers rely on real estate professionals for clear guidance through the transaction. Real estate transactions are already among the most stressful experiences in American life. Wire fraud fear is making them worse, creating anxiety that affects client experience and transaction efficiency. This anxiety is not irrational, but a logical response to a genuine threat that consumers increasingly understand.

Consumer anxiety during transactions

61%

felt funds could be at risk during transaction

46%

delayed sending funds due to security concerns

Source: CertifID Consumer Survey. October 2025. n=1,260 (315 per region)

Consider what these numbers mean in practice. Nearly half of all consumers are so worried about fraud that they hesitate to complete their wire transfer. They second-guess legitimate instructions. They call to verify and often get voicemail. They lie awake at night wondering if they just sent their life savings to a criminal. This anxiety creates friction in every transaction and damages the client experience even when nothing goes wrong.

This anxiety also reveals a critical insight. **Consumers do not just want protection. They want to know how they are being protected.**

Proactive communication about security measures can eliminate this anxiety entirely. When clients understand that wire instructions are being verified through a secure platform, that identities are being confirmed, and that insurance backs every transaction, the stress evaporates. Security becomes a selling point, not just a backend process.

Consumers will pay for protection

According to our survey, **85% of consumers are willing to pay extra for wire fraud protection.** This is not reluctant acceptance, but an active demand that represents a clear market opportunity for businesses willing to meet it. Even more telling: the willingness spans income levels and demographics, indicating broad-based recognition that security has value.

Consumer willingness to pay for protection

How much more would you be willing to pay as a one-time security or processing fee to work with a real estate business that prioritizes protecting your money from wire fraud?

Source: CertifID Consumer Survey. October 2025. n=1,260

The numbers tell a clear story. 71% would pay $51 or more, and 43% would pay $101 or more. Only 14% said they would not pay anything additional.

For businesses still wondering whether to invest in fraud protection, the math is simple: **the vast majority of clients will pay for it, and many will pay more than businesses typically charge.**

Consumer voice: The anxiety of uncertainty

"I felt like a ghost."

Jason and his wife went to wire their down payment on a Tuesday. Something felt off; the instructions were missing information. They reached out to their loan officer, title company, and real estate agent to confirm. No one responded.

They sent the wire anyway, figuring someone would flag it if something was wrong. They emailed to confirm receipt. Still nothing. Friday morning, Jason finally got the loan officer on the phone. He said he hadn't sent the instructions, but no alarm bells went off. He promised to check with his team.

Hours later, pushing harder, the truth finally landed: they were victims of wire fraud.

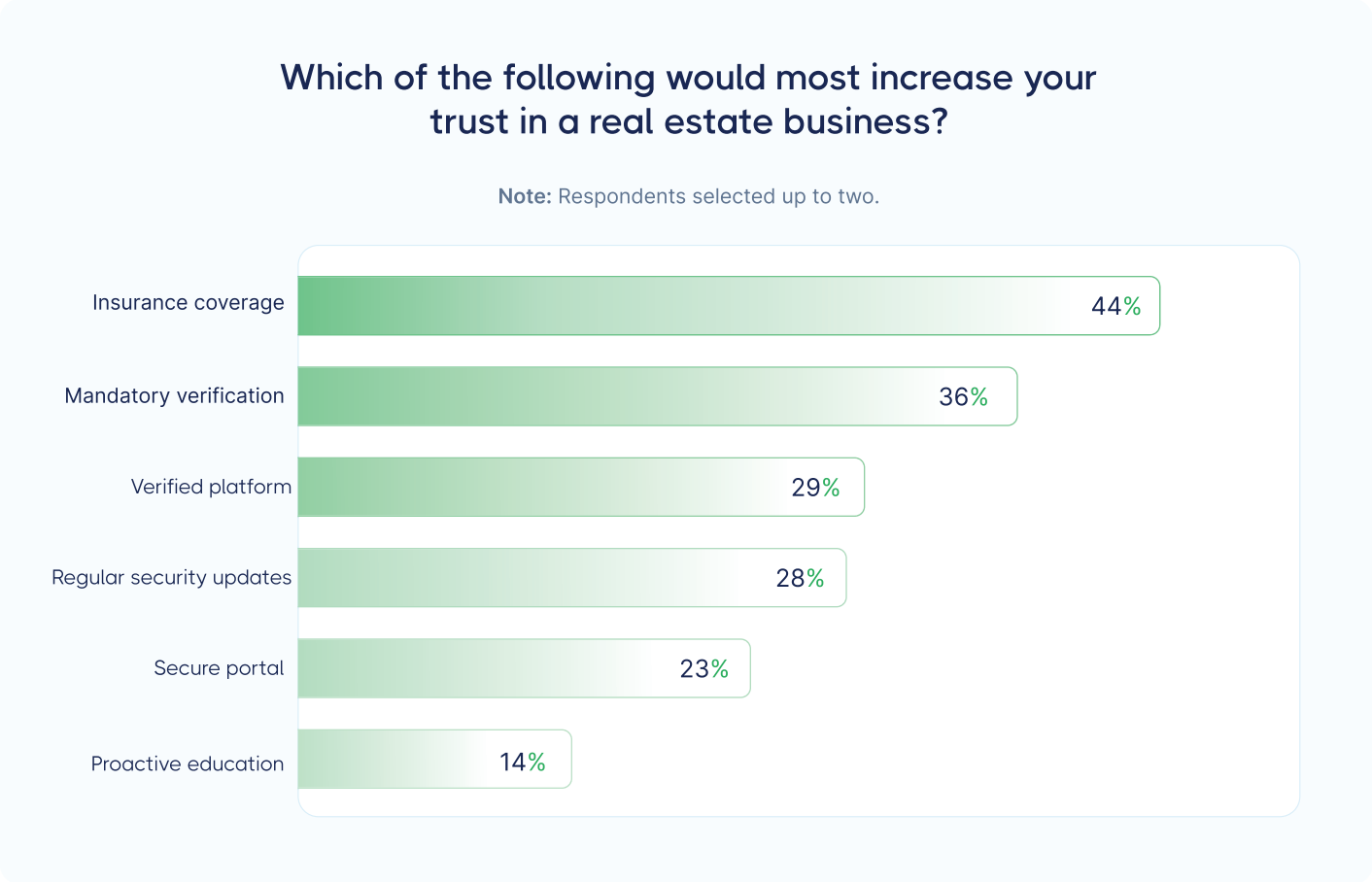
"That's when everything drops out of you," Jason says. "You turn into a ghost."

The days of silence, the missed calls, the unanswered emails—all while their money was gone. This is what the anxiety of wire fraud looks like when no one is watching.

Hear Jason in his own words:

What builds trust: accountability + education

When we asked consumers what would increase their trust in a real estate business, the results were unambiguous. Accountability measures ranked far above educational efforts, indicating that consumers want tangible protection with real consequences, not just information about risks.



Source: CertifID Consumer Survey. October 2025. n=1,260

Consumers prioritize accountability over education. They want to know that if something goes wrong, they are covered. Insurance and guarantees, not just awareness, are what drive trust. This does not mean education is worthless, but it does mean that education alone is not enough. Consumers want tangible protection with real accountability attached.

The real estate firms that are most equipped for the fraud risks ahead apply a layered approach to the security: regular education (to both clients and their internal teams) and software and insurance to limit their exposure and risk.

III. Recovery is possible, but not a business strategy

III. Recovery is possible, but not a business strategy

When wire fraud occurs, recovery is possible. CertifID's Fraud Recovery Services (FRS) has proven this hundreds of times, helping victims navigate the complex process of reclaiming stolen funds. But recovery should never be the plan. **The risk is simply too high, and the consequences extend far beyond the immediate financial loss.**

Recovery works, when it works

FRS has helped hundreds of victims navigate the aftermath of wire fraud. The results demonstrate that recovery is achievable when victims act quickly and have the right support. Speed matters enormously in these situations, as funds that have not yet been moved through multiple accounts or converted to cryptocurrency can often be frozen and returned.

CertifID Fraud Recovery Services Results (Total through March 2026)

773
victims supported

69%
recovery rate

$118.4M
stolen funds recovered

These numbers represent real families who got their money back, real closings that were saved, and real futures that were restored.

The FBI's Recovery Asset Team (RAT) has achieved similar results at scale, successfully freezing 66% of fraudulent wire transfers they pursue. When fraud is reported within 24 hours, recovery rates are significantly higher because the funds have not yet disappeared into the criminal financial system.

Recovery success story:
Seller proceeds fraud

A Florida title company wired $648,815 to what appeared to be the seller's attorney—same name, same firm address, same official letterhead. Only the routing numbers were different. By the time the listing agent called to say the seller hadn't received funds, nearly an hour had passed.

The company acted fast: initiating a recall and filing an FBI IC3 report the same day. But the receiving bank warned recovery could take 90+ days with no guarantees.

After being referred through their insurer, they engaged CertifID Fraud Recovery Services on December 4. The FRS team escalated through its U.S. Secret Service partnership, reached the receiving bank directly, and guided the company through issuing a Letter of Indemnity (a step many victims miss).

Two weeks later, on December 18, nearly 100% of the funds were returned.

The owner, working from home with a two-month-old, described screaming with relief when she saw the confirmation. What could have been a business-ending loss became proof that expert guidance changes outcomes.

Time to recovery:
14 days

Amount recovered:
$648,795 (99.99%)

But recovery should not be your plan

A 69% recovery rate sounds encouraging until you consider what it means for the other 31%. For those families, the outcome is devastating: lost down payments, derailed retirements, shattered dreams of homeownership. And even when recovery succeeds, it comes at tremendous cost in time, stress, resources, and uncertainty that affects everyone involved.

- **Time:** Recovery efforts can take weeks or months, during which funds are frozen and transactions are in limbo.
- **Stress:** Victims describe the experience as traumatic, even when funds are eventually recovered.
- **Resources:** Recovery requires significant effort from your team, diverting attention from other clients.
- **Uncertainty:** Until funds are recovered, no one knows the outcome, creating prolonged anxiety for everyone involved.

The reputational damage is permanent

Even when funds are recovered, the damage to your business may be irreversible. Trust, once broken, is extraordinarily difficult to rebuild, and the data shows that most consumers will not give you the chance to try.

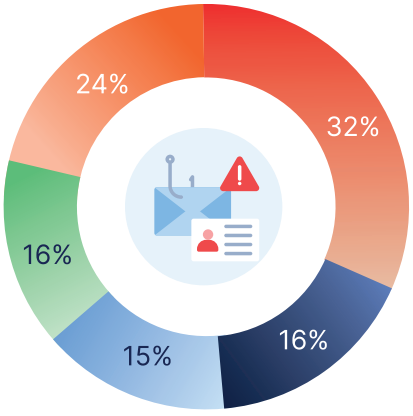
56% of consumers say they would be unlikely to work with a company again after a fraud incident—even if all their funds were recovered

More than half of your clients would walk away forever, even in the best-case recovery scenario. Consider also the 32% who are "very unlikely" to return are not just dissatisfied. They are likely telling everyone they know about their experience. In an industry built on referrals and reputation, a single fraud incident can cascade into years of lost business. Recovery fixes the immediate financial loss, but it does not fix the trust that has been broken.

Would you work with the company again after a fraud incident?

If a fraud incident occurred with a company - even if your funds were recovered - how likely would you be to work with them again?

- Very unlikely
- Somewhat unlikely
- Very likely
- Somewhat likely
- Neither likely nor unlikely



Awareness alone is not enough

The data also reveals a troubling gap between awareness and action. Many consumers recognize suspicious activity but do not know how to respond effectively, leaving them vulnerable even when they sense something is wrong.

33% of consumers who received suspicious communications either ignored them or took no action at all

These are not uninformed people. They knew something was wrong. But without clear protocols and automated protection, they froze. They did not know who to call, what to do, or how to verify whether the communication was legitimate.

This is why **automated protection matters more than awareness.** You cannot rely on consumers, or even trained employees, to catch every sophisticated fraud attempt. When AI can generate perfect impersonation emails and clone voices convincingly, human judgment alone is not sufficient. Technology must be the first line of defense.

The only answer: prevention

Recovery is a safety net. Prevention is the strategy. When you prevent fraud from occurring in the first place, you protect both the funds and your reputation. You eliminate the anxiety your clients feel. You avoid the operational chaos of a recovery effort. You never have to explain to a client why their life savings ended up in a criminal's account. Prevention is not just better than recovery; it is the only approach that fully protects your business and your clients.

IV. The value of protection

IV. The value of protection

Wire fraud is preventable. The technology exists, it is proven, and it works at scale. Businesses that implement comprehensive protection measures see dramatic reductions in successful fraud attempts, and the data from 2025 demonstrates just how effective these tools can be.

In 2025, CertifID completed and verified over 1.46 million wire transfers, further demonstrating the value of systematic fraud prevention.

$283M

Approximate value of financial loss prevented in 2025 by CertifID

1,018

Blocked transactions in 2025 by CertifID

Each of those 1,018 blocked attempts represents a family that did not lose their down payment, a seller who received their proceeds, and a business that did not have to explain a catastrophic failure to their client. The $283 million in protected funds represents life savings, retirement accounts, and the financial futures of American families that remained secure because technology caught what humans might have missed.

How prevention works

Prevention works because it removes the human vulnerability that fraudsters exploit. As a core principle, that means **verify everything through a secure channel that criminals cannot compromise**. When verification happens through secure platforms rather than email or phone calls that can be intercepted or spoofed, the attack surface shrinks dramatically.

So what does a "secure platform" mean in 2026? Effective wire fraud prevention includes several integrated components that work together to create comprehensive protection.

- **Identity verification:** Confirming that the person requesting or receiving funds is who they claim to be, using methods that cannot be easily spoofed.
- **Account ownership verification:** Confirming that bank accounts belong to the verified parties, not criminals using similar names.
- **Secure communication channels:** Transmitting wire instructions through encrypted platforms, not email that can be intercepted or spoofed.
- **Risk scoring:** Analyzing transactions for indicators of fraud and flagging high-risk situations for additional review.
- **Insurance backing:** Providing financial protection if fraud does occur despite prevention measures.

The industry recognizes the threat

Title professionals today understand the stakes. They encounter fraud attempts regularly and have watched the sophistication of these attacks increase dramatically in recent years. Their perspective from the front lines confirms what the data shows: prevention is not optional.

57%
encounter suspicious activity on a quarterly basis or more

73%
say fraud attempts are becoming more sophisticated

60%
report that fraud attempts are increasing in frequency

They see the threat every day. They know that manual verification processes cannot keep pace with AI-powered attacks. And they know that prevention is the only sustainable answer to a threat that continues to evolve.

V. Wire fraud prevention is now a must-have

V. Wire fraud prevention is now a must-have

The convergence of escalating threats, consumer awareness, and proven protection technology has fundamentally changed the methodology for real estate businesses. Wire fraud prevention has crossed from "nice-to-have" to "must-have," and the businesses that recognize this shift will thrive while those that do not will face increasingly serious consequences.

The landscape has shifted

Consider the factors that now make prevention essential. Each factor alone would be significant. Together, they represent a fundamental change in the operating environment for real estate businesses.

1. **The threat is escalating.** AI-powered fraud is up 1,760% year-over-year. Criminals are more sophisticated than ever, and they are specifically targeting real estate because of its vulnerabilities.
2. **Consumers are aware.** 82% know about AI impersonation threats. They are asking questions about security before they sign with you, and they are comparing your answer to what competitors offer.
3. **Consumers are demanding protection.** 85% will pay for it. 68% say guaranteed fraud protection would strongly influence their choice of provider. This is not a niche concern but a mainstream expectation.
4. **The reputational stakes are existential.** 56% will not come back after a fraud incident, even with full recovery. One incident can damage your business for years through lost referrals and damaged reputation.
5. **Have a recovery plan.** Prevention is the strategy, but recovery is the safety net. Know who to call and what to do if the worst happens. Speed matters, and having a plan in place before you need it can make the difference between recovery and permanent loss.

Businesses that do not offer wire fraud prevention will lose clients to competitors who do. Businesses that experience fraud without protection will face reputational damage that takes years to recover from, if they recover at all.

The path forward: an implementation checklist

Every real estate business should take these steps to protect their clients, their reputation, and their future. Implementation does not need to be complicated, but it does need to be comprehensive.

Wire Fraud Prevention Implementation Checklist

Turn prevention into a competitive advantage.

- [ ] **Implement verification technology**
  Automate secure payment verification processes.
- [ ] **Communicate proactively with clients**
  Set clear expectations around payment instructions.
- [ ] **Train your team regularly**
  Keep awareness high as threats evolve.
- [ ] **Have a recovery plan ready**
  Respond fast if an incident occurs.

1. **Implement verification technology.** Do not rely on email or phone calls to confirm wire instructions. Use a secure platform that verifies identities and account ownership through methods that criminals cannot easily compromise. The technology exists and is readily available.
2. **Communicate proactively.** Tell your clients how you are protecting them. Explain your security measures at the first meeting, not the day before closing. Remember that 61% of consumers feel anxious about their funds during transactions. Proactive communication eliminates that anxiety and builds trust.
3. **Offer insurance and guarantees.** Consumers trust accountability. It is their number one factor for building trust. Back your processes with coverage that protects them if something goes wrong, demonstrating that you stand behind your security measures.
4. **Train your team.** Technology is the first line of defense, but humans need to know the protocols. Regular training keeps everyone alert to evolving threats and ensures consistent execution of security procedures across your organization.
5. **Have a recovery plan.** Prevention is the strategy, but recovery is the safety net. Know who to call and what to do if the worst happens. Speed matters, and having a plan in place before you need it can make the difference between recovery and permanent loss.

The real estate industry handles trillions of dollars annually. It is time to protect it like the critical infrastructure it is.

About the study

Consumer survey

The consumer data in this report is from an October 2025 online survey of 1,260 individuals in the U.S. who had purchased or sold a property within the prior three years. The survey was administered through the Attest professional survey platform with stratified sampling across four U.S. regions (Midwest, Northeast, South, and West). All respondents were verified to have completed a real estate transaction within the qualifying period.

Title professional survey

The title professional data is from a separate survey of 153 title and escrow professionals conducted in late 2025 through Typeform. Respondents represented a cross-section of the industry including independent title agents, title company employees, and escrow officers from various regions and company sizes.

Proprietary data

The proprietary data in this report is based on all CertifID services and software usage in 2025. Findings on fraud recoveries come from cases reported to CertifID Fraud Recovery Services. Findings on fraud prevention come from transactions processed by the CertifID platform. All data has been anonymized and aggregated to protect client confidentiality.

External sources

External data sources include the FBI Internet Crime Complaint Center (IC3) 2024 Annual Report, American Land Title Association (ALTA) surveys, and industry research as cited in the Sources section. All external data was current as of the publication date of this report.

Sources

1. Federal Bureau of Investigation. Internet Crime Report 2024. FBI Internet Crime Complaint Center, 2025. https://www.ic3.gov/AnnualReport

2. Federal Bureau of Investigation. "Business Email Compromise: The $50 Billion Scam." Public Service Announcement I-060923-PSA, June 9, 2023. https://www.ic3.gov/PSA/2023/psa230609

3. American Land Title Association. ALTA Critical Issues Study: Cybercrime & Wire Fraud, 2025." https://www.alta.org/news/2025-cybercrime-survey

4. Hoxhunt. "Business Email Compromise Statistics 2025." Hoxhunt Blog, 2025. https://hoxhunt.com/blog/business-email-compromise-statistics

5. National Association of REALTORS. "Highlights From the Profile of Home Buyers and Sellers." 2024. https://www.nar.realtor/research-and-statistics/research-reports/highlights-from-the-profile-of-home-buyers-and-sellers

6. Redfin. U.S. Housing Market Data, December 2025. https://www.redfin.com/us-housing-market

7. CertifID. State of Wire Fraud Consumer Survey. Attest Platform, October 2025. n=1,260

8. CertifID. Title Professional Survey. Typeform, 2025. n=153.

9. CertifID. Proprietary Platform Data, January-December 2025.

10. CertifID. Fraud Recovery Services Case Data, 2025.

About CERTIFID

CertifID is a leader in fraud protection for the real estate industry. The company safeguards billions of dollars every month with advanced software, digital payments, direct insurance, and proven recovery services. Trusted by title companies, law firms, lenders, realtors, and home buyers and sellers, CertifID provides further peace of mind with up to $5M in coverage on every wire transfer it protects. The company's comprehensive approach combines prevention technology, insurance backing, and recovery services to address every aspect of the wire fraud threat.

If you or someone you know falls victim to real estate fraud, **please call us immediately at (616) 202-6612.**

CERTIFID

To download a copy of the
State of Wire Fraud 2026 report, go to: certifid.com/sowf

Specializing in the investigation and prevention of financial crimes

5717 Red Bug Lake Road, Suite 348, Winter Springs, Florida 32708
Mobile: (407) 595-3022

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.

Once attackers gain access to a victim's online banking environment, the clock starts ticking — and funds can disappear rapidly through a series of carefully structured transactions designed to obscure the money trail.

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.**

A notable trend investigators are seeing is transaction structuring:

1. Individual transfers often kept **under $50,000**
2. High transaction volume (20, 30, 40 — sometimes 80–90 transfers)
3. Rapid dispersal across multiple financial institutions

This fragmentation allows fraudsters to avoid triggering automated bank controls while simultaneously accelerating fund laundering.

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).**

Threat actors are obtaining MFA codes through two primary methods:

1. Phone Takeovers (SIM Swaps or Device Compromise)

Attackers hijack a victim's phone number via SIM swap or mobile-account compromise. Once successful, MFA codes intended to protect the account are delivered directly to the fraudster.

2. Social Engineering the Victim

Equally common — and often more effective — is direct manipulation of the account holder.

Fraudsters spoof bank phone numbers and impersonate financial-institution personnel, convincing victims that suspicious activity is occurring. In the urgency of the moment, victims are persuaded to verbally provide MFA codes, unknowingly granting full account access.

This remains one of the most damaging and preventable entry points.

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

Fraudsters can spoof legitimate bank phone numbers. If you receive a call claiming to be from your bank:

Hang up

Locate the official customer-service number from your debit card or bank website

Call back directly

This simple step can stop many attacks in their tracks.

4. Strengthen Mobile-Carrier Security

Adding PINs and port-out protections to mobile accounts can reduce SIM-swap risk.

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

---

Final Thoughts

Account takeover fraud is no longer a niche cybercrime — it is a mainstream financial threat impacting individuals and organizations daily. The combination of social engineering, MFA compromise, and rapid multi-hop fund movement has created a challenging recovery environment.

However, awareness, vigilance, and rapid response remain powerful defenses.

If something feels off with your account, trust that instinct. Acting quickly can mean the difference between recovery and permanent loss.

Fraud groups figured out long ago how to operate at scale. What many people still underestimate is just how structured these operations have become. While they may not always be labeled as traditional "organized crime," their methodologies often fit that definition perfectly.

These groups operate with defined roles, infrastructure, and repeatable processes with phishing teams, account access specialists, money mule coordinators, cryptocurrency off-ramps, and laundering networks that move funds across jurisdictions within minutes. It's not random. It's a business model.

Understanding fraud as an organized operational ecosystem rather than isolated incidents is key to combating it effectively. Prevention, investigation, and recovery strategies must evolve to address the scale, coordination, and sophistication these groups now bring to the table.

Thanks to Stephen Dougherty, USSS (Retired) for his assistance in preparing this handout.

Doug Pollock, CFE
March 12, 2026

Four Policy Buckets Every Title Agency Should Implement in 2026

Wire fraud and impersonation scams continue to target real estate transactions. These four policy buckets provide a framework that managers can use to guide team awareness, internal procedures, and fraud prevention strategies.

I. Securing Communications

Many fraud attempts begin with compromised email accounts or intercepted communications. Title agencies should implement strong communication security policies.

Recommended policies:

- ☐ Use email security platforms such as Mimecast, Barracuda Email Security Gateway, or Microsoft Defender for Office 365.
- ☐ Review email filter reports weekly and share examples of blocked phishing attempts with staff.
- ☐ Require Multi-Factor Authentication (MFA) for email, title production systems, and banking tools.
- ☐ Require re-authentication at least every 12 hours.
- ☐ Provide employees with a one-click phishing reporting tool.
- ☐ Require secondary verification before any wiring instruction changes.

These steps help prevent business email compromise and manipulation of wire instructions.

II. Identity Verification

Identity verification is critical to preventing impersonation fraud in real estate transactions.

Recommended policies:

- ☐ Verify seller identity at order entry for purchase transactions.
- ☐ Reconfirm seller identity and bank credentials before closing.
- ☐ Reverify identity if parties, contact information, or bank instructions change.
- ☐ Apply enhanced verification for higher-risk transactions such as vacant land or non-owner-occupied sellers.
- ☐ For refinance transactions, verify borrower identity at order entry and reconfirm identity and bank information before distributing proceeds.

Proper verification procedures help prevent impersonation fraud and unauthorized changes to wire instructions.

III. Education & Security Awareness

Technology alone cannot prevent fraud. Staff must be trained to recognize common fraud attempts and suspicious activity.

Recommended policies:

- [ ] Provide ongoing staff training on phishing, smishing, and vishing scams.
- [ ] Run internal simulated phishing campaigns to test employee awareness.
- [ ] Share real phishing examples received by the organization during weekly team meetings.
- [ ] Educate staff about malware threats, including keystroke logging and screen capture attacks.
- [ ] Educate referral partners and clients about the secure wire and funding process.

Regular education helps teams recognize threats early and respond appropriately.

IV. Incident Response Plan

Even with strong preventative measures, organizations must be prepared to respond quickly if fraud occurs. Every title agency should maintain an incident response plan aligned with ALTA guidance.

Recommended policies:

- [ ] Define procedures for responding to wire fraud, business email compromise, and cyber incidents.
- [ ] Assign internal ownership for incident response responsibilities.
- [ ] Identify external parties that must be notified, including banks, underwriters, and law enforcement.
- [ ] Ensure employees understand escalation procedures before an incident occurs.

An incident should never be the moment an organization decides how to respond.

Questions? Contact us.

More resources available at www.certifid.com.