hi@solanasis.com
303-900-8969
solanasis.com

Wire Fraud Prevention Guide for Title Companies

Why title companies are the #1 target and what to do about it

$500M+ IN WIRE FRAUD LOSSES ANNUALLY. 95% REPORT ATTACKS INCREASING.

Why Title Companies Are the #1 Target

Title companies sit at the intersection of large wire transfers, sensitive personal information, and multiple parties who trust each other. Every closing involves Social Security numbers, financial records, government IDs, and wire instructions — often coordinated over email. Attackers know this. Business Email Compromise (BEC) targeting title companies is the fastest-growing category of wire fraud in real estate.

The math is simple: compromise one email account at a title company, and you can redirect wire transfers worth hundreds of thousands of dollars. Only 19% of victims recover all their funds.

The Numbers

95%

of title professionals report wire fraud attacks have increased or held steady (Qualia 2025)

60%+

of title companies were targeted in the past 12 months

75%+

still rely on manual fraud prevention processes

22%

use digital or automated fraud detection tools

It Happened to Them

Efficient Services Escrow — $1.5M, Bankrupt

Remote access trojan led to three fraudulent wires totaling $1.5M over 45 days. The company — 20 years in business — went bankrupt. All staff laid off.

Chicago Title — $4.1M

Hacker accessed parties' computers and sent fraudulent wire instructions the day before closing. January 2026. Lawsuit pending.

Denver Homebuyers — $30K

Fraudulent wire instructions appearing to come from the title company. Right here in Colorado. Funds not recovered.

The Regulatory Landscape

Two frameworks govern how title companies must handle security. Both are tightening.

ALTA Best Practices 4.2 (Updated August 2025)

The American Land Title Association's seven operational standards. Version 4.2 added identity verification programs, mandatory independent channel verification for wire instructions, vendor security documentation requirements (SOC 2 Type II preferred), and notarization oversight. Underwriters and lenders increasingly require ALTA certification.

Key pillars for wire fraud:

- **Pillar 2 — Escrow Trust Account Controls:** Wire procedures, daily reconciliation, authorization documentation, independent channel verification
- **Pillar 3 — Information Security & Privacy:** Written ISP (WISP), MFA, vendor vetting, identity verification program
- **Pillar 6 — Professional Liability Insurance:** E&O, cyber insurance, crime/fidelity coverage

FTC Safeguards Rule

Title companies providing settlement and escrow services are covered by the FTC Safeguards Rule as "financial institutions" under the Gramm-Leach-Bliley Act. State regulators enforce equivalent requirements for the title insurance side.

Key requirements:

- Designate a Qualified Individual to oversee the security program
- Develop and maintain a Written Information Security Program (WISP)
- Conduct annual risk assessments
- Implement MFA for all systems accessing customer data
- Encrypt customer data in transit and at rest
- Develop a documented incident response plan
- Assess service provider security

Penalties: Up to $100,000 per violation for companies, $50,120/violation/day for consent order violations.

What Most Title Companies Are Missing

Wire verification is verbal, not documented

Most companies verify wires by phone callback, but there's no log, no documented procedure, no evidence trail. When an underwriter or auditor asks for proof, there's nothing to show.

WISP doesn't exist or is outdated

A Written Information Security Program is required by both ALTA and the FTC Safeguards Rule. Most shops under 20 people have no written policy at all, or have one that was written once and never updated.

Vendors are trusted by default

Your TPS vendor, cloud platforms, and document management tools all handle PII and financial data. ALTA 4.2 requires documented vendor assessments. Most title companies have never asked their vendors for security documentation.

Recovery has never been tested

Having backups and being able to recover are different things. If your systems went down today, how long would it take to get back to processing closings? Most companies don't know.

A Practical Prevention Checklist

Use this as a starting point for assessing your wire fraud prevention posture.

Wire Transfer Controls

- ✓ Written wire transfer procedures documented and current
- ✓ Independent channel verification for all wire instructions (callback on known number)
- ✓ Authorization chain documented with named approvers
- ✓ Daily escrow account reconciliation with documented evidence
- ✓ Staff trained on BEC identification within the last 12 months

Email & Access Security

- ✓ Multi-factor authentication enabled on all email accounts
- ✓ SPF, DKIM, and DMARC configured for your domain
- ✓ Anti-phishing controls active (advanced threat protection)
- ✓ Access controls reviewed quarterly (who can initiate wires?)
- ✓ Former employee access revoked within 24 hours of departure

Vendor & Insurance

- ✓ Complete vendor inventory with data access levels documented
- ✓ SOC 2 Type II or equivalent documentation requested from key vendors
- ✓ Cyber insurance policy in place (separate from E&O)
- ✓ Insurance coverage reviewed for wire fraud and social engineering
- ✓ Crime/fidelity bond includes computer fraud and funds transfer coverage

Documentation & Response

- ✓ Written Information Security Program (WISP) exists and is current
- ✓ Incident response plan documented with named roles
- ✓ Incident response tested within the last 12 months (tabletop exercise)
- ✓ Consumer complaint procedure documented per ALTA Pillar 7
- ✓ Designated Qualified Individual per FTC Safeguards Rule

Timeline for Getting Secure

If your company is starting from a typical baseline (some security controls in place, no formal documentation), here's a realistic timeline:

TIMEFRAME	FOCUS AREA	KEY ACTIONS
Weeks 1-2	Assessment	Gap analysis against ALTA 4.2 and FTC Safeguards requirements. Identify what exists, what's missing, what needs updating.
Weeks 3-4	Wire Controls	Document wire procedures, implement independent channel verification, establish daily reconciliation evidence trail.
Weeks 5-6	Documentation	Create or update WISP, incident response plan, vendor inventory. Designate Qualified Individual.
Weeks 7-8	Vendor & Insurance	Request vendor security documentation. Review insurance coverage for cyber, wire fraud, social engineering gaps.
Weeks 9-10	Testing	Tabletop exercise. Disaster recovery test. Staff training. Verify the whole program works.
Ongoing	Maintenance	Quarterly reviews. Annual ALTA reassessment. Vendor contract renewals with updated security language.

How Solanasis Can Help

Our 10-day Compliance Readiness Assessment covers every item on the checklist above. We test what others only check on paper — including a real disaster recovery restore — and we map every finding to ALTA Best Practices, the FTC Safeguards Rule, and NIST CSF.

After the assessment, you can execute the roadmap independently, bring us in for a remediation sprint, or engage us as an ongoing Fractional CSIO — no lock-in at any stage.

Book a 30-minute conversation: go.solanasis.com/intro

Download the title company compliance checklist: go.solanasis.com/title-checklist

BOOK A CALL