Proof

Identity Fraud Prevention Readiness Checklist for Title Agencies

Align your closing workflow to ALTA Best Practices Framework 4.2

ALTA's updated Best Practices Framework (v4.2) calls for a formal Identity Fraud Prevention Program built on layered verification. This checklist helps break those expectations down into six practical workflow considerations for title teams.

1. Establish a formal identity fraud prevention program

Identity fraud prevention should act as a documented, repeatable program rather than a situational control.

- [ ] Document identity verification policies
- [ ] Standardize verification procedures across transactions
- [ ] Define onboarding protocols for buyers and sellers
- [ ] Train teams to recognize identity risk indicators

Where Proof fits

Proof embeds identity verification directly into transaction intake workflows, helping agencies operationalize fraud prevention policies inside day-to-day operations.

2. Implement layered identity verification

Single-factor identity checks are insufficient. Agencies should apply multiple verification methods.

- [ ] Perform government ID credential analysis
- [ ] Validate participant data against authoritative databases
- [ ] Incorporate biometric or liveness checks
- [ ] Retain verification evidence for auditability

Where Proof fits

Proof supports layered identity verification that combines credential analysis, database validation, and biometric confirmation, creating a stronger participant assurance record tied to the transaction.

3. Verify participants at transaction intake

Identity verification should occur at the start of the transaction, not solely at notarization.

- [ ] Verify buyers at escrow opening
- [ ] Verify sellers before document preparation
- [ ] Confirm borrowers prior to funding coordination
- [ ] Complete verification before issuing wiring instructions

Where Proof fits

Proof enables agencies to verify participants as they enter escrow, establishing confirmed identity before sensitive transaction steps occur.

4. Maintain identity continuity through execution

Verified identity should remain connected to participants as documents move.

- [ ] Send disclosures to verified participants
- [ ] Execute ancillary documents through verified sessions
- [ ] Link eSignature activity to identity records
- [ ] Preserve audit trails for document execution

Where Proof fits

Proof maintains continuity between verified participants and document execution, keeping sign-ahead activity tied to established identity records. For in-person interactions, agencies can use secure verification links to confirm identity on-site before documents are executed.

5. Verify identity for notarization events

Notarization should occur within environments where identity verification is consistent and controlled.

- [ ] Verify identity before curative notarizations
- [ ] Confirm participant credentials at closing
- [ ] Record notarial sessions where applicable
- [ ] Standardize notarization verification practices

Where Proof fits

Proof enables notarization within a controlled digital environment where identity verification and document execution stay visible and standardized.

6. Create an auditable identity record

Identity verification must be demonstrable and reviewable.

- [ ] Document verification steps
- [ ] Retain credential validation results
- [ ] Store notarization session artifacts
- [ ] Connect identity records to transaction events

Where Proof fits

Proof generates a tamper-evident audit trail that connects verified identity to signing and notarization activity, supporting both internal reviews and external compliance needs.

About Proof

Proof connects trusted identity to high-stakes digital actions. Organizations use Proof to verify identity, authorize actions like signing and notarization, and preserve defensible records they can stand behind. Proof operates the Notarize Network, the largest on-demand network of trusted notaries available 24/7. Learn more at proof.com.