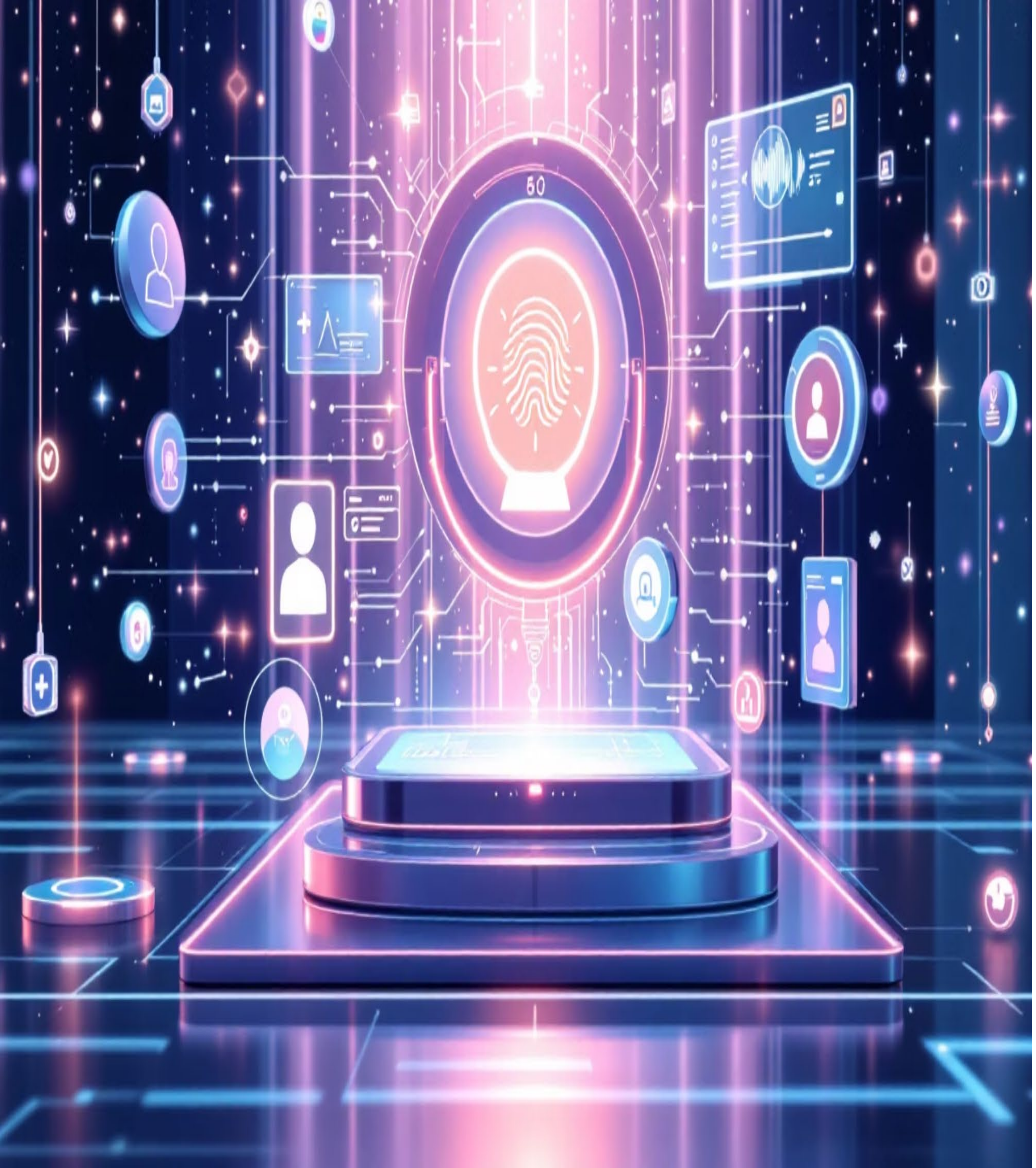


ALTA's New Identity Verification Best Practices for Title Professionals

Where We Have Been

Establishing foundational compliance standards and certification processes that protect all stakeholders in real estate transactions.

Where We Are Going

Evolving toward comprehensive operational excellence with enhanced fraud protection and identity verification protocols.

Webinar Sponsor

OLD REPUBLIC TITLE

Speakers

Craig Haskins

Board Governor | American Land Title Association
craig@knightbarry.com

Cheri Hipenbecker

General Counsel | Knight Barry Title Group
cah@knightbarry.com

Why Is Best Practices Important?

By following Best Practices and identifying and remediating any deficiencies, Agents take active steps to protect all parties and processes involved in real estate settlements.

Consumers

Safeguarding homebuyers and sellers throughout the transaction process

Banks

Protecting lending institutions and ensuring regulatory compliance

Title Insurers

Maintaining underwriting standards and risk management protocols

Real Estate Professionals

Supporting brokers and agents in secure transaction processing

Your Business

Protecting your operations, reputation and long-term sustainability

Best Practices Review: Standards and Pillars

The Seven BP Pillars

Areas of compliance that form the foundation of operational excellence:

- **Pillar 1:** Licensure and regulatory compliance
- **Pillar 2:** Procedures and Controls of Escrow operations
- **Pillar 3:** Written Information Security Plan to Protect NPI
- **Pillar 4:** Standard Real Estate Settlement Policies and Procedures
- **Pillar 5:** Title Policy Production and Premium Remittance
- **Pillar 6:** Maintaining Insurance Coverage
- **Pillar 7:** Resolving Consumer Complaints

BP Assessment Process

A comprehensive comparison of BP standards to your current operations, procedures, and documentation to identify deficiencies and develop remediation plans.

Where We Have Been

Best Practices 4.X Development Journey

The evolution of ALTA Best Practices has been driven by regulatory changes, market demands and the continuous need to enhance protection for all stakeholders in real estate transactions. Annual review to make needed updates.

Changes to Best Practices Objectives

1

Prior to 2023: Compliance Focus

Earlier versions concentrated primarily on compliance certification provided to lenders in response to CFPB Bulletin 2012-03 and similar OCC and FRB regulatory bulletins.

2

2023+ Revisions: Expanded Mission

Maintained agent certification to third parties including lenders and title insurers, while introducing a new major focus on continual operational improvement.

3

Three Pillars of Improvement

- **Safety:** Enhanced security protocols and risk management
- **Customer Experience:** Streamlined processes and service quality
- **Efficiency:** Operational optimization and technology integration

Best Practices 4.2 (Published 8/19/25)

Protection Against Buyer/Seller Impersonation: Identity Verification

Fraud and forgery concerns continue to be a growing and persistent challenge in processing financial and property transactions across all industries.

Fraud Reduction

Robust identity verification reduces impersonation fraud, safeguarding from substantial financial losses and emotional distress.

Market Trust

Builds trust in real estate platforms and agencies, fostering a healthier and more secure market environment.

Legal Protection

Provides crucial legal protection for all parties involved, creating a clear audit trail for potential disputes.

Regulatory Compliance

Ensures compliance with increasingly strict regulations aimed at combating money laundering and fraud in real estate transactions.

Best Practices 4.2

Identity Verification: New Pillar 4 Requirements

Take comprehensive steps to confirm that the proper parties are signing documents for settlement transactions.

01

Staff Training

Train staff on fraud in the real estate sector, including buyer, borrower, and seller impersonation fraud detection techniques.

02

Signing Professional Control

Control the selection of signing professionals who will meet with buyers, borrowers, and sellers to execute documents.

03

Employee Training & Tools

Provide training and tools to validate authentic government-issued IDs and verify signer identity matches the presented ID.

04

Third-Party Verification

Confirm third-party signing professionals utilize proper ID validation and identity verification tools and processes.

05

Independent Validation

When parties choose their own signing professionals, independently obtain and validate signer credentials and government-issued ID authenticity.

06

Fraud Response Protocols

Create comprehensive protocols and processes to identify and respond to suspected fraud or impersonation attempts.

Best Practices 4.2

Specific language under Pillar 4 requiring company to create and implement an identity fraud prevention program designed to verify the identity of the parties who are signing documents for a Settlement.

1. Train staff on fraud in the real estate sector, including buyer, borrower, and seller impersonation fraud.
2. Control the selection of the signing professional who the buyer(s), borrower(s), and seller(s) will meet with to sign the documents.
3. For signing professionals employed by the Company, provide training and tools to: (i) attempt to validate that the government issued ID (both foreign and domestic) presented by the signer is an authentic ID, and (ii) attempt to verify that the signer presenting the ID is the person on the ID.
4. For third party signing professionals retained by the Company, confirm that the signing professional is utilizing training and tools to: (i) attempt to validate that the government issued ID (both foreign and domestic) presented by the signer is an authentic ID, and (ii) attempt to verify that the signer presenting the ID is the person on the ID.
5. If Company receives a document that was notarized by a buyer, borrower, or seller's selected signing professional of their choosing, treat the document as being at risk for fraud. Regarding such a document, Company should independently obtain the signer's credentials to attempt to validate the signer's government issued ID is authentic and attempt to verify that the signer is the person on the ID.
6. Create protocols and processes to identify and respond to suspected fraud or impersonation attempts.

Best Practices 4.2: ID Verification Methods

Various Methods of Identify Verification

1. Verification of government ID provided by a signer
2. Database verification of personal information provided by the signer
3. Personal contacts and references received from the signer
4. Biometric verification for the signer
5. Use of open-source personal information to verify signer

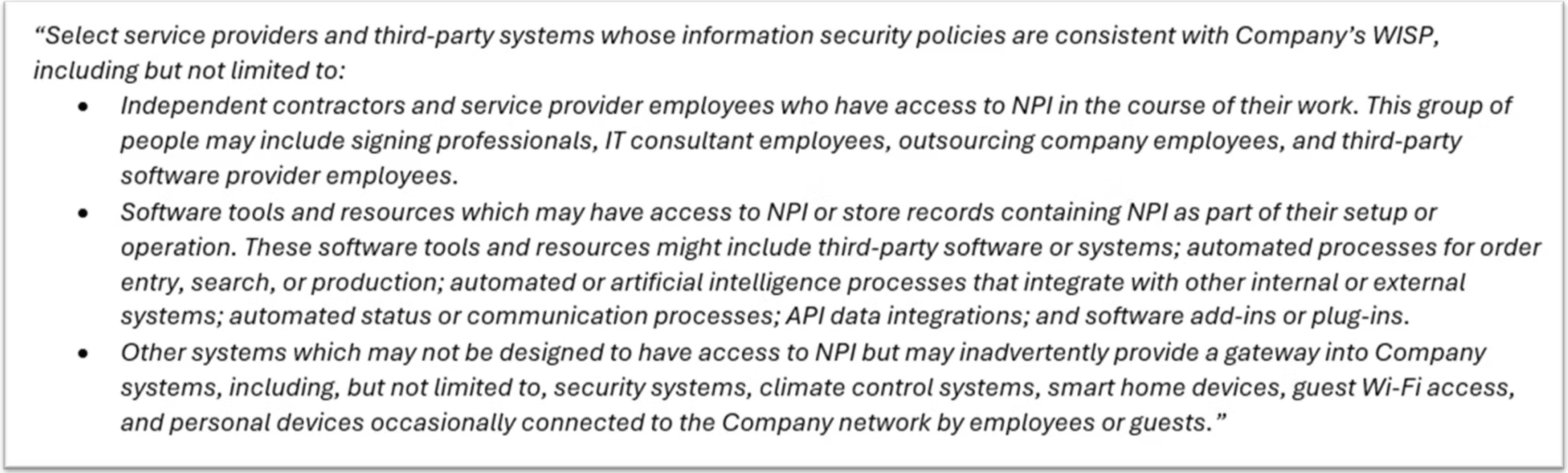
General Recommendations

1. Use a layered approach that does not rely on one factor
2. Common fraud indicators
3. Common transactions targeted by impersonators
4. Employee training
5. Escalation procedures

ALTA’s Guidance on Vetting a Vendor

Vendor selection has become increasingly critical to the success of agent operations and overall security posture. Proper vendor management directly impacts compliance and operational efficiency.

The following existing section from Pillar 3 addresses the critical need for aligning vendor risks to your company's Written Information Security Plan (WISP):



“Select service providers and third-party systems whose information security policies are consistent with Company’s WISP, including but not limited to:

- *Independent contractors and service provider employees who have access to NPI in the course of their work. This group of people may include signing professionals, IT consultant employees, outsourcing company employees, and third-party software provider employees.*
- *Software tools and resources which may have access to NPI or store records containing NPI as part of their setup or operation. These software tools and resources might include third-party software or systems; automated processes for order entry, search, or production; automated or artificial intelligence processes that integrate with other internal or external systems; automated status or communication processes; API data integrations; and software add-ins or plug-ins.*
- *Other systems which may not be designed to have access to NPI but may inadvertently provide a gateway into Company systems, including, but not limited to, security systems, climate control systems, smart home devices, guest Wi-Fi access, and personal devices occasionally connected to the Company network by employees or guests.”*

ALTA's Guidance on Vetting a Vendor

Pillar 4 also contains existing requirement for oversight of RON vendors and signing professionals

- Operations and Capabilities
- Information Security
- Legal and Insurance Protections

Coming next year … Best Practices 5.0?

ALTA's Guidance on Vetting a Vendor

Topics of Inquiry

1. Vendor qualifications and experience
2. Compliance and insurance
3. Financial stability
4. Service quality and reliability
5. Technology and innovation
6. Data security and privacy
7. Wire fraud prevention
8. Contractual considerations
9. Artificial Intelligence inquiries

Red Flags

- Reluctance to provide documentation and clear, written procedures regarding wire fraud prevention or incident response handling
- Inadequate or lapsed insurance coverage(s)
- Poor or no references
- Unclear pricing structures
- Weak security protocols
- Limited disaster recovery capabilities
- High staff turnover
- Outdated technology or lack of commitment to continual improvement
- Unresponsive customer service or limited support hours
- Limited industry experience
- Lack of security certifications
- No multi-factor authentication
- Weak wire fraud controls (where applicable)
- No regular security assessments
- Lack of alignment of the proposed contract to the delivery and protections promised during the sales process

TRUST
NOBODY

Questions?

Contact Us

Craig Haskins

craig@knightbarry.com

Cheri Hipenbecker

cah@knightbarry.com