MICHIGAN LAND TITLE ASSOCIATION

Integrity ◆ Responsibility ◆ Service

Cindy Immonen, NTP, CLTP
VP, Sr. Account Manager
P: 248-331-6860 | E: cindy.immonen@fnf.com

FNF FAMILY OF COMPANIES | MICHIGAN AGENCY

1

ALTA Best Practices

ALTA's New Identity Verification Best Practices for Title Professionals

2

Where We Have Been

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.

Changes to Best Practices Objectives

Prior versions of Best Practices (prior to 4.0 in 2023) had focused on compliance certification being provided to Lenders

- Response to CFPB Bulletin 2012-03 and similar OCC and FRB bulletins

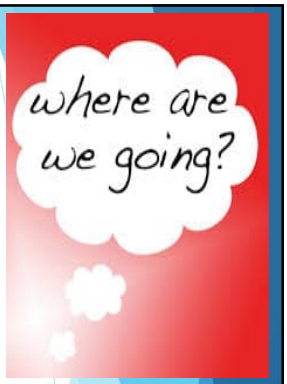
Version History and Notes

Date	Version	Notes
1/2/2013	None	Publication of the ALTA Title Insurance and Settlement Company Best Practices, approved by the ALTA Board of Governors on December 20, 2012.
7/19/2013	2.0	Publication of the revised ALTA Title Insurance and Settlement Company Best Practices, along with other documents in the ALTA Best Practices Framework, approved by the ALTA Board of Governors on July 19, 2013.
10/7/2016	2.5	Publication of the revised ALTA Title Insurance and Settlement Company Best Practices Framework (including addition of third-party signing professionals provision), with other documents, approved by the ALTA Bd of Governors on September 19, 2016.
10/17/2019	3.0	Publication of the revised ALTA Title Insurance and Settlement Company Best Practices, along with other documents in the ALTA Best Practices Framework, approved by the ALTA Board of Governors on June 6, 2019.
1/23/2023	4.0	Publication of the revised ALTA Title Insurance and Settlement Company Best Practices, along with other documents in the ALTA Best Practices Framework, approved by the ALTA Board of Governors on October 13, 2022. Publication on January 23, 2023, with an effective date of May 23, 2023.
9/17/2024	4.1	Approved by ALTA Board of Governors on 6/11/24 and published in 9/17/2024.
08/19/2025	4.2	Approved by ALTA Board of Governors on 6-17-2025 and effective on 8/19/2025.

3

Where We Are Going

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



Changes to Best Practices Objectives

Revisions for 2023+:

- ✓ Continued Agent Certification to 3rd parties, including Lenders and Title Insurers.
- ✓ New major focus is on continual improvement to operations:
  - Safety
  - Customer Experience
  - Efficiency

Version 4.0 (May 2023)

- First major rewrite in 10-year history of BP.
- Designed to address major industry changes
  - ✓ Threats: Fraud, Theft, Cybercrime
  - ✓ Business Has Advanced: RON, Outsourced/Remote workers, more technology
  - ✓ Changes in laws and regulations
- Highly focused on ensuring operational improvements for Agencies

4

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

5

Best Practices Review: Standards and Pillars

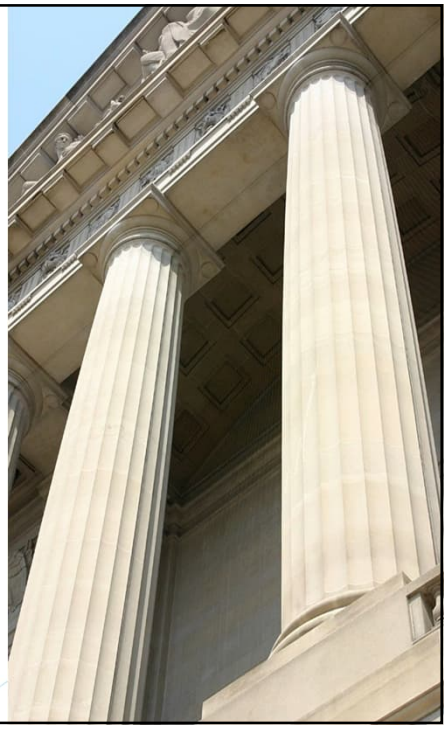
What are the Best Practices Pillars?

Areas of compliance include:

- Pillar 1: Licensure
- Pillar 2: Procedures and Controls of Escrow
- 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

What is a Best Practices Assessment?

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



6

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

7

Scary Facts

Identity theft involves the appropriation and misuse of an existing person's identity. Synthetic identity fraud, on the other hand, involves constructing a fabricated identity that is a mash-up of both authentic and fabricated details. The resulting identity appears legitimate on paper but does not represent an actual person.

Synthetic identity document fraud rose by over 300% with attackers exploiting generative AI to create fake passports, IDs, and biometric data.

Synthetic identity fraud is the fastest-growing type of financial crime, with recent estimates placing lender exposure in the billions of dollars and projecting continuous growth through 2030. Unlike traditional identity theft, which involves a single victim's stolen information, synthetic fraud creates fake identities by combining fabricated and authentic personal details from multiple sources.

Generative AI tools are making synthetic fraud more sophisticated. In 2025, 40% of financial institutions saw an increase in AI-driven attacks, and 29% observed deepfakes being used in synthetic fraud attempts to create convincing fake documents and images.

Fraudsters combine real and/or fictitious information to create an identity.

51%
of organizations have suffered financial losses due to identity-related breaches.

8

We are dealing with a $4B+ synthetic identity fraud crisis! Reports from Experian & TransUnion show that synthetic identity fraud is the fastest rising type of fraud in 2025.

We are to the point that a human cannot detect if an ID is FRAUD!

The ease of obtaining fake IDs has risen dramatically with advancements in technology. Online platforms and websites offering easy access to high-quality fake IDs have proliferated, catering to a wide range of age groups. For example, there are websites where individuals can upload their photos and personal information, and within days, receive a convincing counterfeit identification document in the mail. Fraudsters are using AI tools to create hyper-realistic synthetic identities, making them difficult to detect.

Michigan has started to roll out new driver's licenses and IDs, with enhanced security technology. The new look is based on security best practices and new technology aimed at reducing the risk of counterfeiting and fraud, according to the Michigan Secretary of State.

9

FinCEN Warns Criminals Using Fake Passports Cards in Identity Theft, Fraud Schemes

The U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) warned financial institutions to be vigilant in identifying and reporting suspicious activity related to the use of counterfeit U.S. passport cards.

In conjunction with FinCEN, the U.S. Department of State's Diplomatic Security Service (DSS) issued a notice to encourage financial institutions identify and report suspicious activity potentially related to passport card fraud.

According to DSS and other law enforcement agencies, individuals and fraud rings are falsely making, selling and using counterfeit U.S. passport cards to impersonate and defraud persons holding accounts at financial institutions.

10

Best Practices 4.2

Protection Against Seller Fraud: 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 seller impersonation fraud, safeguarding buyers 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.

11

Best Practices 4.2

Protection against Signer Fraud: Identity Verification

- Fraud and forgery concerns continue to be a growing and persistent challenge in processing financial and property transactions in all industries.
- Identity verification can provide significant benefits in the real estate transaction:
  - Robust identity verification reduces seller impersonation fraud, safeguarding buyers from substantial financial losses and emotional distress.
  - Builds trust in real estate platforms and agencies, fostering a healthier market environment.
  - Provides crucial legal protection for all parties involved, creating a clear audit trail for potential disputes.
  - Ensures compliance with increasingly strict regulations aimed at combating money laundering and
  - fraud in real estate transactions.

12

Best Practices 4.2

Protection against Signer Fraud: Identity Verification

Company will create and implement an identity fraud prevention program designed to verify the identity of the parties who are signing documents for a Settlement.

- Train staff on fraud in the real estate sector, including buyer, borrower, and seller impersonation fraud.
- Control the selection of the signing professional who the buyer(s), borrower(s), and seller(s) will meet with to sign the documents.
- For signing professionals who are employed by Company (Agent), provide training and tools to:
  (i) validate that the government issued ID (both foreign and domestic) presented by the signer is an authentic ID
  (ii) verify that the signer presenting the ID is the person on the ID.

13

Best Practices 4.2
Protection against Signer Fraud: Identity Verification

- For signing professionals who are third parties retained by Company (Agent), confirm that the signing professional is utilizing tools to:
  (i) validate that the government issued ID (both foreign and domestic) presented by the signer is an authentic ID
  (ii)verify that the signer presenting the ID is the person on the ID.
- 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.
- 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.
- Create protocols and processes to identify and respond to suspected fraud or impersonation attempts.

14

Best Practices 4.2
Protection against Signer Fraud: Identity Verification

✓ 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.

15

Best Practices 4.2: Selecting Remote Notarization Platforms.

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

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

- If Company employees will be notarizing Settlement documents via remote notarization, select a remote notarization platform authorized by the state in which the notary public is located and that is approved by the Title Insurer, as applicable. Ensure that the software platform is capable of meeting the minimum requirements of the state, including retention of the video and safeguarding of NPI.
- Implement procedures to charge fees as authorized by the state regulations.
- If Company will engage a third-party to notarize documents via remote notarization, oversee the selection of the platform in compliance with ALTA Best Practices. If the state in which the property is located has a process to approve remote notarization platforms, the selected software platform must be approved by the state and the Title Insurer, as applicable.

16

Escrow technology for Identity Verification

Identity Verification is the verification of a person's identity.
Identity verification is usually performed just once, but once verified, a person's identity may need to be authenticated each time they access a system or resource.
There are multiple methods for Identity Verification. The methods available to notaries for verifying a signer's identity for notarizations vary depending on the state where the notary is commissioned.

Know there here are multiple methods for Identity Verification:

1. IAL2-Compliant Identity Verification (Credential Analysis + Selfie Comparison)
   - is a method of confirming a person's identity that is compliant with NIST IAL2 identity proofing, the highest level of remote identity verification.
2. Multi-Step Verification
   - is a type of Identity Verification that requires a user to present two or more forms of identification to prove their identity. This can include combinations of the following:
     - Something you have (Driver's license, passport, utility bill, etc.)
     - Something you know (Personal information, phone number validation, etc.)
     - Biometric validation (Comparing a real-time selfie capture to a valid credential/ID provided)
   - Knowledge-based Authentication (KBA)
   - Credential Analysis
   - Selfie Comparison
3. Personal Knowledge of Identity
4. Credible Identifying Witness

17

Best Practices 4.2: Vetting the 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."*

18

Best Practices 4.2: Vetting the Vendor

- Vendor Qualification and Experience
  Goal: Gain comfort knowing this vendor has a strong reputation for supporting other companies in the industry or similar sectors.
- Compliance and Insurance
  Goal: Ensure that the vendor you select is compliant and that if something were to go wrong, the vendor has the necessary coverage to support their customers.
- Financial Stability
  Goal: Make sure this vendor has the financial stability to support you and won't end up causing business disruptions due to inadequate finances.
- Service Quality and Reliability
  Goal: Gathering these details upfront can help you set expectations contractually to ensure you get the service required to support your business.
- Technology and Innovation
  Goal: When you select a vendor, consider the impact they may have on your business for many years to come. How they are managing their business and security today is a good indication of how they will manage it moving forward.

19

Best Practices 4.2: Vetting the Vendor

- Data Security and Privacy
  Goal: Security and privacy have never been more important. Confirm vendors maintain safe data security and privacy practices and protocols to keep your business safe.
- Wire Fraud Prevention
  Goal: Wire fraud is one of the leading causes of loss of funds. Ensuring that not only are your operations taking the necessary steps to prevent wire fraud, but that your vendors are providing adequate protection and coverage(s) is critical to your business.
- Contractual Considerations
  Goals: Vendors may promise a lot during the sales process, so make sure those promises are included in the contract and that you have the right to terminate, litigate, and/or recover if they aren't met.
- AI Inquiries
  Goals: Vendors may be putting your data at risk by their use or provision of AI tools or third-party services. It is important to understand how your data is being utilized and exposed so you can determine whether a solution introduces risks of disclosure.

20

Best Practices 4.2: Vetting the Vendor

Red Flags to Consider

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

21

Best Practices 4.2: Vetting the Vendor

Additional Resources

Forbes – https://www.forbes.com/councils/forbestechcouncil/2023/04/04/16-key-considerations-when-vetting-a-new-tech-vendor-or-partner/

Kirkpatrick Price - https://kirkpatrickprice.com/blog/vendor-due-diligence-checklist/#

ALTA Webinar: Let's Go Shopping For Tech: https://www.youtube.com/watch?v=SPBDqnRfJvg

CFPB Complaints Search: https://www.consumerfi nance.gov/data-research/consumer-complaints/search

ALTA Best Practices website: https://www.alta.org/policies-and-standards/best-practices/

Handouts from this presentation – at the MLTA website
- ALTA WISP Guidance and FAQ - v1.0 - Published 09-17-2024
- Identity Verification Guidance - ALTA BP - (Published 08.19.25)
- Vetting a Vendor - ALTA BP - (Published 08.19.2025)
- ALTA Best Practices Framework v4.2 - (Effective 08-19-2025)

22

Best Practices 4.3 (2026) in Development

Areas Being Considered

- FINCEN Compliance
- Best Practices for Commercial Transactions
- Risks of using AI

23

MLTA est. 1901
MICHIGAN LAND TITLE ASSOCIATION
Integrity ◆ Responsibility ◆ Service

Thanks for attending!

24