Best Practices:
Review of 2023 Framework (v 4.0) Revisions

2023 ALTA Best Practices 4.0 Revisions

Copyright 2023, American Land Title Association. All rights reserved.

Version 2-28-2023

The ALTA Best Practices Pillars

The ALTA Best Practices underlying Pillar structure remains the same

- Pillar 1: Licensure
- Pillar 2: Escrow accounts
- Pillar 3: Protecting NPI
- Pillar 4: Settlement Policies & Procedures
- Pillar 5: Title production, delivery, and remittance/reporting of title policies
- Pillar 6: Insurance and fidelity coverage
- Pillar 7: Resolving consumer complaints

Best Practices Objective: Operational Improvement

- Prior versions of Best Practices focused on compliance certification being provided to Lenders
- 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

Updates in the “Definitions” Section

Various “Defined Terms” have been updated to clarify their intent within Best Practices

Consumer: Buyer(s), borrower(s), or seller(s) in a real estate transaction

Title Agency: Any person, company or entity which is authorized by a Title Insurer to issue title insurance policies. A Title Agency may also perform one or more of the following functions outside of their relationship with the Title Insurer: (1) collect and/or disburse premiums, escrows, security deposits or other funds, (2) handle escrow, Settlement or closings, (3) solicit or negotiate title insurance business, and (4) record documents.

Title Insurer: Any person, company or entity that is licensed to issue and insure title insurance policies

Content Changes in Pillar 2: Risk of Loss of Funds

Pillar 2 “Purpose” section is updated to note that the loss of funds may fall outside of E&O Coverage; could fall to the Agency

~~to~~risk of loss of ~~client~~ funds. Loss of funds may not be covered by the Title Agency’s Errors and Omissions (“E&O”) insurance or the contract with its Title Insurer. Such losses would then become the responsibility of the Title Agency. Settlement companies may engage outside contractors to

Content Changes in Pillar 2: Non-Settled and Reversible Funds

Pillar 2 updated to address the handling of non-settled funds and avoidance of undue risk

(aka, “Wiring off of the float”)

In making disbursements from Escrow Trust Accounts, and subject to state law requirements, Company should ensure that undue risk is not being undertaken for escrow deposits that are not fully settled or that could be reversible.

Content Changes in Pillar 2: FinTech and Earnest Money

Pillar 2 updated to control the use of "Fintech" applications…

… and require that third-party earnest money platforms meet Good Funds law req'ts and are not subject to the EFTA

Positive Pay or Reverse Positive Pay are utilized, if available for the payment type, and have policies and procedures in place that prohibit or control the use of Automated Clearing House transactions, international wire transfers, and electronic/digital receipt of funds from web based fintech applications.

When utilizing a third-party earnest money deposit or disbursement platform that facilitates the digital transfer of Escrow Trust Account receipts and disbursements, ensure that the platform meets any good funds law requirements and is not subject to the Electronic Funds Transfer Act (EFTA) which allows for reversal of consumer payments.

Content Changes in Pillar 2: Outgoing Wires

Pillar 2 updated to specify that Wire Transfer Procedures should include Multi-Factor Authentication and follow ALTA's published guidance

For outgoing wire transfers, this includes documented procedures to verify wire transfer instructions independent of the initial communication. Such procedures should include the use of multi-factor authentication and should be similar in nature to those currently cited by ALTA in the Outgoing Wire Preparation Checklist.

Content Changes in Pillar 2: Background Checks

Pillar 2 Procedures are updated to extend the background check refreshes not only to those employees having access to client funds, but now to all employees

Background Checks are ~~completed in~~obtained and reviewed during the hiring process. ~~At~~Thereafter, at least every three years, ~~obtain~~updated Background Checks going back five years are obtained and reviewed for all employees ~~who have access to customer funds~~.

Content Changes in Pillar 2: Wire Verification Services

Pillar 2 Procedures are updated to recommend the use of Wire Verification Services

If available, efficient, and economical, make use of wire transfer verification service providers. Such service providers should be vetted to understand any risk of use, security protocols, and the providers' protection of Consumer data.

Content Changes in Pillar 3: Written Information Security Plan

Pillar 3 Purpose is updated to include a defined term of “WISP”

3. **Best Practice: Adopt and maintain a written information security plan (“WISP”) and a written privacy ~~and information security program~~plan to protect ~~Non-public Personal Information~~ NPI as required by local, state, and federal law.**

Content Changes in Pillar 3: Security Measures in WISP

Pillar 3 is updated to protect NPI and Company systems by requiring specific security measures: MFA, Password Management, and Software Updates

Establish ~~a written information security plan~~ and implement a WISP designed to protect ~~to protect nonpublic information in~~ the security and confidentiality of NPI and the security of the Company's ~~possession and detect loss of nonpublic information based on the size and complexity of the Company's operations~~information systems. The WISP should include:

- Multi-factor authentication, if available, that requires multiple credentials (factors) for access to systems containing NPI.
- Password management plan that requires unique login names and system passwords to access systems containing NPI. System passwords must meet minimum standards which include:
  - re-entry of the password after system idling;
  - passwords that expire after a certain period of time;
  - difficult-to-guess passwords that include a combination of uppercase letters, lowercase letters, special characters, with a minimum length of eight total characters.
- Timely software updates that require routine updates to systems, software, and code that, when left outdated, can result in data breaches, cyberattacks, exploits, ransomware attacks and other exposure of NPI.

Content Changes in Pillar 3: Service Providers: Background Checks / Physical access to NPI

Pillar 3 is updated to require background checks for not only employees with access to NPI, but also to anyone with access to NPI or information systems - including service providers

Physical security ~~of Non-public Personal Information.~~ • Restrict access to ~~Non-public Personal Information to~~the Company's information systems to only authorized employees and authorized service providers who have undergone Background Checks ~~at hiring~~.
• Control physical access to NPI in physical forms, including cabinets, desks, storage, or other areas where NPI exists in any physical or electronic format to authorized employees and authorized service providers who have undergone Background Checks.

Content Changes in Pillar 3: Cloud, Virtual, and Hosted Systems

Pillar 3 is updated to extend network security requirements to the use of cloud systems, virtual equipment, data centers, and 3rd party hosting

Network and cloud security ~~of Non-public Personal Information.~~to protect NPI.

- Maintain and secure access to Company information technology software applications and data stored on physical or virtual equipment at Company location(s), in a data center, in the cloud, or hosted by third-party vendors.

Content Changes in Pillar 3: DR/BC Plan

Pillar 3 is updated to specifically include in the DR/BC plan instances where there is a compromise of systems or facilities

Establish and periodically test, a written ~~Establish a written disaster management and~~ business continuity and disaster recovery plan outlining procedures to recover and maintain information ~~and~~, business functions~~-~~, and business processes in the event of a disruption or compromise of systems or facilities,

including continuity of operation for Consumer Settlements, and timely notification of parties in case of any delays.

Content Changes in Pillar 3: Application to all cybersecurity incidents

Pillar 3 is updated to require the written response plan to address *any* cybersecurity incident, not just those involving NPI; include periodically testing and follow the recommendations of the ALTA Cybersecurity Incident Response Plan

- Establish, and periodically test, a written incident response plan designed to promptly respond to, and recover from, a ~~breach that compromises the confidentiality, integrity, or availability of Non-public Personal Information in the Company's possession.~~
  - ~~Establish internal and service provider processes for determining the size, nature and scope of any~~ cybersecurity incident~~.~~, which includes all the recommendations of the ALTA Cybersecurity Incident Response Plan template.

Content Changes in Pillar 3: Written Service Provider Policies

Pillar 3 is updated to specify that service provider policies are to be consistent with the Company WISP including:

IT Consultants, outsourcing company employees, and third-party software employees

~~Utilize multifactor authentication for all remotely hosted or accessible~~Select service providers and third-party systems ~~storing, transmitting or transferring non-public personal~~ whose information~~.~~

~~Post~~ 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.

Content Changes in Pillar 3: Software Tools and Resources

Pillar 3 is updated to specify that software tools and resources are to be consistent with the Company WISP – including:

3rd party software / systems; automated processes; APIs; software add/plug-ins

~~Utilize multifactor authentication for all remotely hosted or accessible~~Select service providers and third-party systems ~~storing, transmitting or transferring non-public personal~~ whose information~~.~~

~~Post~~ security policies are consistent with Company's WISP, including but not limited to:

- 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.

Content Changes in Pillar 4: Compliant Settlement Processes

Pillar 4 Description is updated to point to the importance of contractual obligations in the Settlement process

4. **Best Practice: Adopt standard real estate ~~settlement~~ Settlement policies and procedures ~~and policies~~ that help ensure compliance with ~~Federal and State Consumer Financial Laws~~: (i) federal and state consumer financial protection laws and regulations, and (ii) contractual obligations as applicable to the Settlement process.**

Content Changes in Pillar 4: Training of Consumer Objectives

Pillar 4 is updated to include “consumer objectives” in the training of staff

~~Review legal and contractual~~ Train staff to provide a framework which will:

- Minimize errors in completing the Settlement.
- Enable a timely response to concerns raised by any of the parties following the Settlement, including addressing Consumer complaints in compliance with the requirements ~~to determine Company obligations to record documents~~of ALTA Best Practices.

Content Changes in Pillar 4: Disclose Affiliated Business Arrangements

Pillar 4 is updated to require the disclosure of affiliated business arrangements

~~Maintain~~Disclose Affiliated Business Arrangements.

- In compliance with state and federal laws and regulations, establish and implement procedures requiring proper disclosure of any affiliated business arrangements in which Company participates.

Content Changes in Pillar 4: Oversight of Signing Professionals

Pillar 4 is updated to expand Best Practice requirements to monitor and verify that signing professionals have state and contractually required licensing and insurance to notarize documents, conduct the settlement, and safeguard NPI

Oversee Signing professionals

- Establish and implement written procedures to monitor and verify that all signing professionals possess the appropriate ~~qualifications, professionalism, and knowledge, including the standards described below.~~state licensing and insurance to notarize documents (both in person and remotely, if applicable), conduct the Settlement (if applicable), and safeguard NPI. These requirements are determined by a mix of legal and contractual obligations, including state regulations and Title Insurer requirements and restrictions.

Content Changes in Pillar 4: 3rd party Signing Professional requirements

Pillar 4 is updated to require third party signing professionals to have the required professional designation, insurance, and bond as required by state law and/or the title insurer

- For signing professionals~~:~~

~~Furnish~~ who are third parties, require demonstrable evidence of their current: state licensure, where required, or ~~evidence if they have attained~~ a recognized and verifiable industry designation, ~~and;~~E&O insurance and Notary surety bond, if required by state law and/or the Title Insurer.

Content Changes in Pillar 4: Vendors for 3rd party signing professional

Pillar 4 is updated to address that when a vendor is used to provide a third-party signing professional, the Best Practices obligations may be assumed by that vendor

Company may engage a vendor who may assume the obligations to monitor and verify that the third-party signing professional complies with ALTA Best Practices requirements.

Content Changes in Pillar 4: Selecting RON Platforms

Pillar 4 is updated to provide guidance in utilizing Remote Notarization Platforms for employee signing professionals and by third party signing professionals

Selecting Remote Notarization Platforms.

- 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, then the selected software platform must be approved by the state, and the Title Insurer, as applicable.

Resources for Assessment and Certification

- The assessment is the process of aligning and documenting operations to the Best Practices requirements
  - The ALTA Best Practices Framework sets the standards for the assessment evaluation
- Best Practices provides other documents to assist with the assessment evaluation:
  - Assessment Procedures: Tool for evaluating compliance with the standards
  - Assessment Compliance Reports: Frameworks for evaluating against the Assessment Procedures. Different forms are available for 3rd party and internal assessments.
    - Third-Party Assessment Report: For those Companies certifying via a third-party assessment, this form will be used to provide an analysis against the "Assessment Procedures", providing a certification letter, summary of exceptions, and a list of exceptions with a remediation plan.
    - Best Practices Internal Assessment Report and Letter *(fka "Self-Assessment")*: This form will be used for Internal Assessments to provide an analysis against either the "Framework" or the "Assessment Procedures" providing a certification letter, and a list of exceptions with a remediation plan.
  - Various Policies and Procedures templates
  - ALTA Website for information security standards used in Best Practices:
    - https://www.alta.org/business-tools/information-security

Questions?

Submit Questions to:

BestPractices@alta.org

Updates to Information:

https://www.alta.org/best-practices