ALTA BEST PRACTICES GUIDANCE - IDENTITY VERIFICATION

VERSION: 01.00
PUBLISHED 08-19-2025

ALTA Best Practices Executive Committee and Work Group

Contents

Summary – Purpose of this Guidance

Fraud and forgery concerns continue to be a growing and persistent challenge in processing financial and property transactions in all industries. Implementing identify verification processes, though presenting challenges such as potential transaction delays and privacy concerns, can provide significant benefits that far outweigh the risks to all parties in the real estate transaction, including:

- Robust identity verification effectively 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.

ALTA Best Practices has continued to implement and update the requirements to address risks and threats to the real estate industry. In support of these changes, ALTA is providing this document to support the understanding and analysis of the available approaches to identity verification. Because the threats that identity verification are designed to prevent are emerging and evolving threats, this Guidance will be updated periodically as new threats emerge and as tools and approaches to combat these threats are improved. ALTA understands that no approach will prevent all fraud, but that effort appropriate to the risk should be made to mitigate fraud.

This Guidance is aimed at providing methods for a settlement agent to answer the following basic questions when presented with a government ID by a person who has signed or proposes to sign a conveyance document:

- Is this a valid government ID?
- Does the person on the government ID match the individual who presented it?
- Is the person on the government ID the actual seller, buyer, or borrower (as applicable) in the transaction?

This Guideline outlines some of the approaches that can be utilized but does not set a minimum standard or requirement for what methods to utilize. Some of the methods discussed may not be readily available to settlement agents. Thus, settlement agents may wish to consider engaging a technology company that may provide an option to utilize such tools.

Identity Verification Methods

The following section discusses the various methods of identity verification that are available. No method or methods completely eliminate the risk of impersonation or forgery, but the objective is to use the tools available to reduce the risk.

1. Verification of Government ID provided by a signer

- Description: Physical document verification of a government issued photo ID (driver's licenses, passports). Designed to answer the question: Does the individual possess an authentic Government issued identity document that supports their claim to a physical identity?
- Potential actions to verify:
  - Where possible, obtain and validate the ID of a signer in advance of the closing.
  - Require multiple forms of government ID, at least one of which is unexpired.
  - Cross referencing data sources: Data in the government ID cross-referenced with DMV database, or similar, to determine if:
    - ✓ The database corroborates the ID and the provided personal information
    - ✓ The expiration date, issue date, and id number can be verified
    - ✓ The data in the ID cross-references with data provided using the bar code or other similar coding.
  - Tamper and manipulation detection methods (color, text patterns).
  - Automated security feature detection (holograms, UV patterns).
  - The expected features of the government ID of the jurisdiction.
  - Use of systems or tools to identify forged government IDs:
    - ✓ Print quality and color matching: Advanced systems check for inconsistencies in print quality and color across the document, which may indicate physical alterations.
    - ✓ Font consistency analysis: Systems examine the consistency of fonts used throughout the document to identify potential tampering.
    - ✓ Photo replacement detection: Some fraudsters physically replace the photograph on a genuine document, which can be caught by sophisticated verification systems.
    - ✓ Image compression analysis: Systems check for signs of image manipulation by analyzing compression artifacts.
    - ✓ Pixel-level analysis: Advanced algorithms perform detailed examinations of pixel arrays to identify modified principal components.

2. Database Verification of Personal Information provided by the signer

- Description: checking that information an end user provides about themselves - such as name, date of birth, etc. - matches a record in a known database, and that at least some of the records tie the person to the property.

- Potential actions to verify:
  - Verification of claimed personally identifiable information (PII) against credit bureaus, government agencies, and other authoritative databases. Recommended elements to verify include:
    - ✓ First Name
    - ✓ Last Name
    - ✓ Address
    - ✓ Phone Number
    - ✓ Date of Birth
    - ✓ Social Security Number (or national ID if outside of US)
  - Watchlist screening and compliance checks

  Unless otherwise required, there is no need to disclose the databases being utilized to persons being verified or persons involved in the transaction.

3. Personal Contacts and References received from the signer

- Description: Ensure that the reference sources the signer claims to have can corroborate the signer's information
- Potential Actions to Verify:
  - Independently search and obtain contact information for the reference
  - Send letter to the reference using the reference's publicly available address
  - Contact signer's real estate agent, attorney, mortgage lender, and/or accountant

4. Biometric Verification for the signer

- Description: In situations where the signer is remote, it may be helpful to determine whether the person presenting the ID is the rightful owner using physical attributes, such as requesting a "selfie" to compare against the ID.
- Potential actions to verify:
  - Facial comparison between selfie and photo ID
  - Liveness detection – preventing spoofing attempts and/or deepfakes by requesting that remote individuals follow action commands (e.g., turn left, turn right, raise your hand)

5. Use of open-source personal information to verify signer

- Description: Determine whether the provided phone number, email address and photo are likely to be those of the person who should be the signer.
- Recommended actions to verify:
  - Public search of email addresses, phone numbers, and photos. This may be used to verify if the phone number and email address have been associated with the individual's name and address in public records or commercial databases. Compare these items to information presented by the person.

- Domain Validation: Checks the validity of the email domain.
- Syntax Check: Ensures the email address follows proper formatting.
- Disposable Email Detection: Identifies temporary email addresses that have not previously been associated with the individual or represents a recently created email address.

General Recommendations

Use a layered approach that does not rely on one factor

1. Don't use knowledge based authentication (KBA) questions as a sole reliable verification
2. Don't use publicly available sources as the only source
3. Use multiple sources of verification
4. Higher risk transactions command higher vigilance

Common Fraud Indicators

1. Geographic mismatches
2. Multiple verification attempts
3. Unusual transaction timing or rush requests
4. Refusal to comply with identity verification requests
5. Abandoned identity verifications

Common Transactions targeted by impersonators

1. High-value transactions
2. Vacant lots, second home transactions, or other non-owner occupied transactions.
3. Remote closing

Employee Training

Conduct regular employee training on items including:

- Current impersonation schemes and red flags
- Advanced document forgery detection
- Social engineering tactics used by fraudsters
- Behavioral indicators of fraudulent activity

Escalation Procedures

Create escalation procedures if fraud is suspected:

- Establish documented protocol(s) for if identity fraud is suspected or concerns exist, including when and who to escalate the matter to.
- Response procedures if concerns are verified
    - Immediate response procedures for compromised identities
    - Notify local or federal law enforcement and respective fraud units
    - Develop communication protocols for affected parties. Implement immediate transaction and funding hold procedures when fraud is suspected

Additional Resources

DEFINITIONS:

Identity Proofing: The collective process of mixing and matching verifications to achieve sufficient assurance that an individual is indeed who they claim to be with the goal of tying digital identities to physical identities.

- Identity Proofing involves collecting and validating identity-related information to establish a person's identity before they can access services or complete transactions. Identity Proofing focuses on the authenticity of data provided during the onboarding or account creation processes.

Identity Verification: The process of confirming that the person presenting an identity (including a government issued ID) is the rightful owner of that identity.

- Identity verification can involve various methods, such as device intelligence, knowledge-based authentication (KBA) questions, biometric verification and multi-factor authentication (MFA).

WEBSITES:

- Experian - https://www.experian.com/business/solutions/identity-solutions/identity-verification-solutions
- National Institute of Standards and Technology (NIST) – US Department of Commerce - https://pages.nist.gov/800-63-3-Implementation-Resources/63A/verification/
- Transunion - https://www.transunion.com/faq/identity-verification
- ALTA's Seller Impersonation Page: https://www.alta.org/business-operations/operations/seller-impersonation-fraud
- ALTA Marketplace – Industry Vendors: https://www.alta.org/marketplace *
- ALTA Marketplace – "Fraud Prevention" list: https://www.alta.org/marketplace/results?code_valueList=FraudPrev *

** A vendor provider or service provider being listed or found in the ALTA Marketplace does not indicate that the providers have been vetted by ALTA; further, the applicable categories are self-reported by the providers.*

ALTA advises that your vetting of any provider's product or service should include, among others, applicability, contractual terms, risk mitigation, data protection, change management, and provider performance. These are some, but not all, of the critical components of vendor selection that a company should analyze in selecting any vendor.