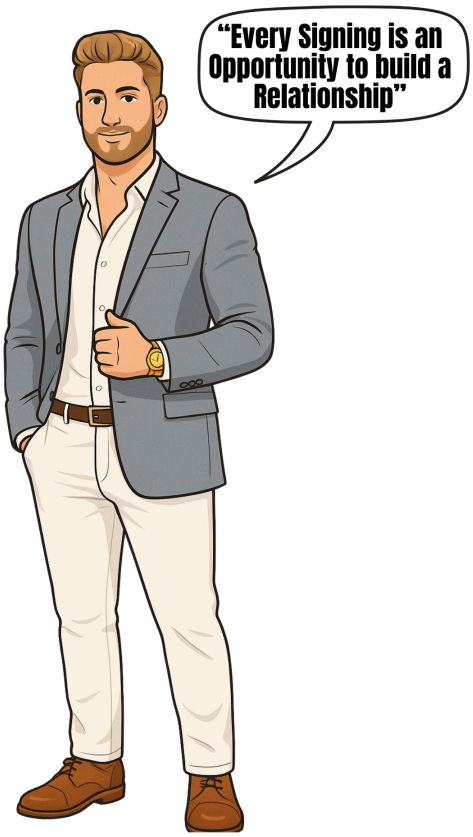
THE HUMAN FIREWALL

-

Leveraging Notary Protocols to Reduce Escrow Liability



By

Conner Brown

President, Caffeinated Closings

*Legal Disclaimer: I am not an attorney and cannot give legal advice. These are simply my developed opinions on best practices against identity fraud, from first hand experiences.

Does the Risk Make Sense?

Escrow officers are expected to follow instructions precisely.

When a transaction is challenged, the issue becomes whether the right person signed and whether that can be proven.

If identity verification fails, the transaction can be unwound and liability can shift back to escrow.

The notary is the final checkpoint in that process.

The Escrow-Notary Liability Link

Escrow can be liable, even if they unknowingly hire a non-compliant notary.

Your protection depends on control of the notary and quality of documentation.

-Keep Records!

- -Your local notary: Always work with notaries that will be available to provide a copy of their journal if requested
- -Always work with a signing service that holds records within the GLBA
    - MISMO
    - SOC 2 Type II
- Timestamps of when the notary and the signer viewed, downloaded, or uploaded the document package.
- **IP Addresses & Device ID**
- **Certificate of Completion**: A summary document that "seals" the transaction history

  The signing company should be able to do this for you!

-Improper Handling of NPPI (Data Breach)

The Risk: If a notary leaves a copy of the loan package in their car and it's stolen, or if they use a public FedEx computer to scan documents back to escrow, they have caused a data breach.

Under GLBA regulations, the escrow company may be responsible for the vendor's failure to protect that data!

Best Practices with your local notary:

-Do they make additional checks for red flags?

-Do they look for ID holograms? Do they understand basic ID validity techniques?

-Do they take good records, and are ABLE to provide you a copy if needed?

-ALWAYS retain a copy of their E&O and other credentials

Physical Examination: Notaries should hold and feel the ID for irregularities, such as peeling laminate, rough edges, or misaligned, bumpy surfaces.

Security Features: Notaries should check for holograms, "ghost" photos, UV light features, and micro-printing when possible

Data Matching: Verify that the signature and physical description (height, eye color, birthdate) on the ID matches the person standing before you.

Contextual Flags: Look for irregularities like unusual fonts, misspelled words, or an unfamiliar state design.

Best Practices with your Signing Company:

ASK

-Can they clearly communicate how they vet their notaries?

-Do they really know how their notaries are protecting you from fraud?

-Can I see the notary's picture? Send it to your clients!!

-Do they confirm commission status with the SOS upon every signing?

-Do they hold MISMO certifications (eClosing, RON, and eVault) and SOC 2 Type II attestation? This is essential to safely hold records

-Identity Verification (IV) Protocols: Ask if the service trains notaries specifically on how to spot fake IDs and handle ID verification according to state laws.

-Many services rely on self-reported data. Escrow officers should verify if the service performs manual compliance reviews.

-Annual Background Checks: Verify that every notary has a background check that is no more than one year old.

-Errors & Omissions (E&O) Insurance: Look for services that require a minimum of $100,000 in E&O coverage for signing agents, as the basic $25,000 may not cover high-value transaction errors.

-Automated Expiration Tracking: Ask if the platform automatically "grays out" or deactivates notaries whose commissions or insurance have expired.

NPPI Handling and Document Security

-Encrypted Portals vs. Email: Ensure the service uses a secure portal for document transmission rather than insecure email attachments.

-Document Destruction Policy: Confirm that the service requires notaries to delete all digital copies of loan packages from their devices immediately after the signing.

-No Mobile Storage: Notaries should be prohibited from storing photos of signer IDs on their personal phones.

Liability often arises when the "wrong" person shows up at the door.

ENSURE

-Individual Account Enforcement: Ensure the platform forbids "team" accounts where multiple notaries share one login, which destroys the audit trail.

-Audit Trails: The service should provide a complete log of who accessed documents and when.

-Multi-Factor Authentication (MFA): Confirm the platform requires MFA for all notary logins to prevent unauthorized access to loan packages.

SOC 2 Type II Attestation: Check if the platform has an independent security audit (like SOC 2 Type II) that covers a continuous period, not just a one-time "Type I" snapshot.

If a signing service has a SOC 2 Type II report, the escrow officer has documented proof that they performed "due diligence."

A SOC 2 Type II report for a platform or a signing service proves:

- Access Control: Not just anyone in the company can see your borrower's SSN or ID.
- Encryption: The data is actually encrypted both when it's sitting on the server and when it's being sent to the notary.
- Disaster Recovery: If their server goes down, your closing doesn't vanish.
- Vulnerability Testing: They are actively trying to "hack" themselves to find holes before a criminal does.



GREEN FLAGS

-Look for signing companies that are vetted and approved by large title companies.

-Work with one that Vets its notaries manually

-Do they verify their notary's commission?

-Work with one that holds on to records in accordance with GLBA

Best Practices for ID Verification:

At a minimum, notaries should do:

The "Tactile" Test: Feeling for raised edges or peeling lamination.

Alignment & Micro-printing: Using light and magnification to spot digital alterations.

The "Second Form of ID" Strategy: When and why notaries should ask for a backup ID (e.g., credit card, work badge) even if not legally required by California Civil Code 1185.

Interrogation for Identity: Asking signers questions based on their ID (e.g., middle name, zodiac sign) to flush out impersonators.

RED FLAGS:

Behavioral Indicators: Spotting coercion, duress, or confusion, especially in elder care or power of attorney signings.

The Rush Job: Why last-minute changes or pressure to "just get it done" are the #1 signal of fraud.

Empowering Notaries: Establishing a "No-Questions-Asked" protocol where notaries are supported by escrow when they refuse to sign due to suspicion.

RONS:

Underwriter Approval: Confirm the specific RON platform (e.g., Proof, NotaryCam) is approved by your title underwriter and the lender.

MISMO (Mortgage Industry Standards Maintenance Organization) Certification: Ensure the platform meets MISMO standards like Snapdocs

ALWAYS require Credential Analysis (automated forensic ID check) and Knowledge-Based Authentication (KBA)

Make sure the platform Stores the RON video according to MISMO!



Conner S Brown
President
Caffeinated Closings

Thank you for participating in my Webinar!

-Conner Brown

CAFFEINATED CLOSINGS

"The most powerful resource we have to being the best, is working to grow together"