Proof[SM]

Updating the Identity Proofing Paradigm for Remote Online Notarization:

How Validation and Verification Create Secure, Convenient Notarization

July 2025

Dale Hardy, Senior Counsel & Director, Government Affairs

I. Executive Summary

Remote online notarization (RON) is no longer new. Since 2012, over 45 states have enabled their notaries to perform RON. Millions have taken advantage of the benefits offered by RON, namely increased security, accessibility, and convenience. RON is now used to execute transactions in all of life's biggest moments, from buying a house, to executing a will, to adopting a child.

The foundation of RON is based on the combination of existing technologies, allowing notaries to securely identify individuals remotely through "identity proofing." To implement this, many states have mandated notaries utilize two distinct forms of identity proofing, oftentimes without any additional guidance. This approach has led to a focus on the number of steps completed in an assessment, rather than the purpose and value of each individual step.

This paper will examine the flaws in approaching identity proofing as simply the number of identity proofing processes employed, and instead propose a new paradigm that emphasizes the importance of the validation of an asserted identity and the verification of the individual's ownership of that identity.

II. Introduction: The Evolution of Notarization and the Promise of RON

Notarization has always been responsive to advances in technology. What once involved the use of a wax seal evolved to utilize an embosser or a rubber stamp. Once electronic notarization was authorized under the Uniform Electronic Transactions Act (UETA) and the Electronic Signatures in Global and National Commerce Act (ESIGN), the pace of technological change with notarization has accelerated.

The technological advances that have enabled RON provide features that are not available in traditional notarization:

- A remote signing process, recorded and retained by audio/video technology;
- Electronic signatures and records, sealed by tamper-evident technology; and
- Identity proofing processes, providing the notary with additional resources and information to better identify signers.

These features are easily identifiable as requirements within the enabling legislation of adopting states. However, as with all technology, the regulatory frameworks that support the technology must be both flexible and regularly re-evaluated to ensure that the framework continues to support the initial intent of RON, not hinder it.

When it comes to identity proofing, state statutes often simply mandate the use of at least two distinct identity proofing processes. This approach contains flaws that, unless addressed, will keep RON from adapting to ever-changing security and identity challenges, while also ensuring that the consumer experience contains more friction than necessary.

III. The "Two Forms" Fallacy: Moving from Quantity to Quality in Identity Proofing

The prevailing "two forms" approach to identity proofing in Remote Online Notarization (RON) operates on a fundamental assumption: that safety increases proportionally with the number of identity verification methods employed. This logic posits that by simply requiring more "hoops to jump through," signers are more likely to be positively identified, and fraudsters more effectively deterred. However, this is not necessarily true, and this quantitative focus can mask critical vulnerabilities.

In its simplest and most robust form, the process of identifying an individual should involve two distinct objectives:

1. **Validation:** Confirming that the asserted identity actually exists.
2. **Verification:** Ascertaining that the person asserting that identity is the validated identity's true owner.

Validation: Establishing the Identity's Existence

Validation confirms the authenticity of a claimed identity. This is typically achieved by cross-referencing asserted details against authoritative or credible databases, whether public or private. Such checks provide essential assurance that the identity itself is real and not fabricated. In the context of RON, credential analysis is the most crucial method for achieving this. When a government-issued identification is presented, sophisticated automated processes confirm the integrity of the document's security features and verify personal details against authoritative or credible sources. This step is paramount because without validating the credential and its underlying reliance on the authority of the issuing source, the asserted identity cannot be validated as existing.

Verification: Confirming Ownership of a Validated Identity

Once an asserted identity has been validated, the next step is to determine the individual's ownership of that identity – linking the live person to the now-validated identity. In RON today, this most often occurs through two primary methods:

- **Knowledge-Based Authentication (KBA):** This involves posing a series of questions, largely derived from credit history and public records. The premise is that only the true owner of the identity would possess the specific knowledge to answer these questions

correctly, which are ostensibly based on events within that identity's history.

- **Biometric Comparison:** Increasingly popular, this method typically uses facial recognition. A fully automated process compares a biometric characteristic from the validated credential (e.g., the photo on an ID) with a live biometric sample collected from the principal, adhering to stringent standards set by bodies such as the National Institute of Standards and Technology (NIST). Biometrics are generally considered more dispositive in verifying an individual's ownership of a validated identity than KBA, underscored by the fact that NIST explicitly does not allow for the use of KBA for high-assurance identity proofing.

The Peril of Disconnected Steps: Why "Two Forms" Falls Short

The critical risk with a "two forms" approach is that it can entirely circumvent or improperly sequence the distinct objectives of validation and verification. Consider a scenario where a notary or platform allows a signer to be identified using only KBA and biometric analysis. Both KBA and biometric comparison primarily serve the verification step – binding an individual to an identity. However, if the underlying identity itself was never validated, then a signer could be "verified" as owning an unvalidated, potentially fraudulent, identity.

Technologies like KBA and biometrics, while varying in sophistication, exist to serve a similar purpose: binding an individual to an identity. If that underlying identity's existence and authenticity (its validation) are not first confirmed, then the subsequent verification steps, such as biometric comparison, lose their effectiveness. Similarly, one could imagine a scenario where an identity is doubly validated (e.g., through two forms of credential analysis), but without definitive confirmation as to the individual's ownership of it. This highlights the fundamental flaw: the "two forms" approach prioritizes quantity over the essential qualitative steps of first confirming an identity's existence and then linking a person to that confirmed identity. Without requiring credential analysis as a mandatory validation step, pairing KBA and biometrics together not only fails to meet the spirit of robust identity assurance but also renders both subsequent verification methods ineffective due to a lack of a properly validated foundation.

IV. Reusable Identity: Reducing Friction While Maintaining Security

When RON was first enacted, the ecosystem of RON platforms and vendors for notaries was not fully anticipated. Today, platforms enable notaries to conduct RON for signers globally, while simultaneously managing compliance and best practices. However, with the technologies used to power RON, additional efficiency and security is available.

The use of a platform also allows both notaries and signers to have much of their information saved for repeat use. Through RON's history, a signer has had to complete two methods of identity proofing every time they receive a notarization, regardless of how many times their identity has been successfully validated and verified previously.

Under a validation and verification approach, this would not be necessary. Once a validated identity has been established, reconfirmation does not increase the ability of the notary to identify a signer. A validated identity stays validated. All that's left is to verify that the individual owns the identity.

Biometrics are well suited to perform verification for a previously validated identity. The saved identity will include information from the individual's identity credential, including a photograph, the same sample taken to compare against during the initial biometric process. A returning signer could simply scan their face, pass the biometric comparison, and thereby re-verify ownership of the validated identity. The notary would still receive information about the identity proofing process in order to make the final determination, including an image of the validated credential and indicators regarding the results of the biometric comparison.

While pursuing any updates to the law to enable validation and verification, states should consider policies that eliminate the need to perform validation every time a signer returns to a previously used platform. This would save time and inconvenience, while still ensuring that the necessary steps to positively identify the customer are taking place.

V. Conclusion and Call to Action

Validation and verification is a more thoughtful approach to identity proofing than RON has enjoyed so far. It does not overvalue the number of processes an individual must go through. Instead, it focuses on the key functions identity proofing is attempting to achieve: proving an identity exists; and, proving the identity belongs to a certain individual. By shifting to this way of understanding, states can be more adaptable to future developments in identity proofing technologies, choosing the best options that complete one of the two major steps. This would also allow for a more seamless signer experience, without sacrificing security or certainty. We strongly encourage states to evaluate the identity proofing framework laid out in statutes and regulations, and take this step in the evolution of RON.

Contact:

Dale Hardy

Senior Counsel & Director, Government Affairs

dale.hardy@proof.com