Notarize

Remote Online Notarization: A Modern Approach to Security & Fraud Prevention

August 2021

Notarize, Inc.

Introduction:
In today's society where identity fraud is commonplace, a system that enforces integrity and honesty, and enables us to trust and rely on one another is a necessity. As public officials responsible for the certification of signatures and documents, notaries public play a critical role in this system, verifying the identity of signers and acting as disinterested and impartial witnesses to transactions. This important fraud prevention measure has traditionally been performed on paper and in person. This changed in 2012 when the Commonwealth of Virginia became the first state to authorize remote online notarization (RON), bringing notarization into the digital world. Today, RON has been authorized in 37 states with additional states considering legislation at an accelerated pace.

RON was designed to enhance the traditional notarization and introduce additional fraud prevention measures that increase the trust and security of a notarization. This is satisfied by implementing modern communications and identity proofing technology to confirm the signer's identity before a notarization and preserve the integrity of that notarization long after a document is signed.

As digital tools and processes have become mainstream, businesses and consumers have grown accustomed to the convenience and security that online transactions provide. Our collective reliance on digital tools increased dramatically throughout the COVID-19 pandemic as many facets of our business and personal lives were forced online. RON has not only helped the notary public participate in the digital economy, but it has also introduced additional features to the notarization that increase the security and fraud prevention benefits of a notarization.

Multi-Factor Authentication:
The first step of a compliant notarization is the verification of a signer's identity. RON enhances this step by requiring the signer to complete multi-factor authentication in addition to presenting their ID.

Typically, when identifying a signer through multi-factor authentication, the notary confirms the identity of the person appearing before them by requiring them to successfully complete Knowledge-Based Authentication (KBA) and credential analysis.

> **Knowledge-Based Authentication:**
> Before the signer begins a session with a notary, the signer must complete Knowledge-Based Authentication (KBA). KBA relies on third-party databases to generate multiple questions with a range of correct answers. KBA helps deter fraud by asking the signer a series of questions to which only they will know the answers.
>
> **Credential Analysis:**
> After completing KBA, the signer captures and submits a photo of their ID, such as a driver's license or passport, for analysis. The photo and information on the ID are analyzed for signs of alteration or forgery and are then authenticated.
>
> RON still requires the signer to appear before a notary public which is satisfied over a live audio/video connection during the session.
>
> **Notary Validation:**

After completing the initial two steps of the multi-factor authentication process, the signer is connected with a commissioned notary public in a live face-to-face interaction using A/V communications technology. During the session, the notary is provided with the results of the KBA and credential analysis and the images of the signer's ID. The notary then compares the signer's ID to the KBA-validated identity and to the person appearing before the notary in the real-time A/V session. If the notary concludes that he or she has satisfactory evidence of the signer's identity, the notary proceeds with the notarization.

It is important to note that RON laws should remain technology-neutral and avoid requiring the use of specific technologies for multi-factor authentication. This allows for the flexibility to adapt to more advanced technologies in the future.

Audio/Video Recording:
The introduction of A/V communications technology not only preserves the requirement that the signer appear before a notary public, but it also introduces a new method of fraud prevention: a recording of the transaction that is retained for future reference.

RON improves recordkeeping by requiring that an A/V recording of every session is created and retained. Before RON, a notary public would rely on a paper notary journal for recordkeeping, a process that can put both the notary public and the signer at risk. A paper journal is limited, and in most cases, if a signature is contested, the notary public can revisit the paper journal and may testify that he or she checked the signer's ID. However, the extent of available evidence stops there.

An A/V recording of the session will show what the signer looked and sounded like and the circumstances surrounding the notarization of the document. Requiring a recording and the retention of it provides a video record that can be referenced in the future.

Electronic Notary Journal:
Before RON, notaries public relied on a paper notary journal to capture and store basic information surrounding notarizations. Paper records can be easily damaged or misplaced. RON allows a notary public to use an electronic notary journal, which is an electronically stored and encrypted file designed to include all of the information legally required by the notary public's commissioning state, including details such as the name and address of the signer, time and type of the notarial act, the method of identification, and the fee charged. Together the electronic notary journal and A/V recording of a session create a comprehensive record of the notarization that far exceeds the records maintained with a traditional paper notarization.

Tamper Evident Technologies & Other Fraud Prevention Elements:
Documents have always presented a risk of forgery, but RON helps to significantly reduce this risk by requiring the use of tamper-evident technologies which are applied to a document at the end of the signing session.

In a traditional notarization, once a signer leaves there is nothing to stop the signer from altering the documents or adding additional pages after the notarization. With RON however, tamper-evident technology, such as a digital certificate, is applied to the document at the end of the signing session making any modifications obvious and provable.

Furthermore, various standards-setting organizations have instituted a minimum set of technical and procedural standards for RON technology vendors that include additional fraud prevention elements. A common requirement is that all RON transactions generate an audit trail or audit log. An audit trail is a chronological and detailed list of the most important actions that occur in the signing session and includes the date and time that those actions are performed. The inclusion of an audit trail is another example of how RON provides additional fraud prevention measures that are not available with a traditional paper notarization.

Additional Benefits of A/V Communications Technology:

Additionally, conducting a notarization with RON helps protect the notary public and provides an additional level of fraud prevention. One study by the National Notary Association found that 30% of notaries public in traditional notarization settings have faced pressure to ignore or break state laws. With RON, a notary public can complete transactions in a setting in which they are comfortable and can terminate a session if for any reason they suspect fraud.

Conclusion:

Through the introduction of these technologies, RON has created a legal framework and regulatory structure that modernizes the notarization while increasing the security and fraud prevention capabilities of the process. RON helps notaries public expand upon their capabilities and gives them the tools to participate in the digital economy. With RON, states can offer both notaries public and constituents an additional option for getting documents notarized that meet the demands of today's digital world without sacrificing the important fraud prevention and security measures a notarization provides.

Contact:
James Fulgenzi
Public Affairs Communications Manager
james.fulgenzi@notarize.com