



# The Human Element: The Role of Notaries in the Evolving Digital Identity Landscape

June 2023

CONFIDENTIAL. © 2023. Notarize, Inc. (dba Proof.com)



**Introduction:**

The pandemic did not create e-commerce or our desire to complete everyday transactions online - but it was a catalyst for wider adoption. As more of our lives have gone digital, the ability to verify our identities online has become central to participating in the digital economy. In response, governments and private-enterprise implemented solutions such as multi-factor authentication services and biometric authentication to help verify identities online. Despite these improvements, the prevalence and sophistication of online identity fraud have increased at an alarming rate. Artificial intelligence (AI), deepfakes, and sophisticated phishing emails and texts are just a few exploits dominating the news and making the act of proving one's identity all the more difficult in the 21st century.

Does an increased level of online identity fraud mean we should abandon digital services altogether? No. Instead, states should respond by implementing modern and enduring solutions. As online identity verification becomes a vital public service, notaries public and remote online notarization (RON) show us how humans play an important role in building a safer internet.

Since 2012, RON has empowered the notary - public officials specially trained in identity verification - to move beyond pen and paper and provide trust to digital transactions. As states look for ways to help their citizens participate in the digital economy, RON will play an important role. But to ensure notaries are equipped to combat the latest methods of identity fraud, states must assess the technologies available to notaries today and ensure access to next-generation solutions.

A notary's ability to leverage the unique combination of technology and human verification in RON is undercut when the laws enabling RON require the use of outdated and less secure identity proofing solutions. As the methods to commit fraud online become more sophisticated, so too should the tools notaries have to stop it. To continue to advance notarization throughout the 21st century, states should move to create regulatory flexibility and allow the notarial regulator of the state to approve new and improved identity proofing methods as they are proven effective.

**Demand for Digital Services:**

The pandemic quickly accelerated the world into a digital-first marketplace, and many, if not all, of these consumer trends are here to stay<sup>1</sup>, including the use of RON. For centuries, notarizations have played a vital role in verifying the identity of signers and are performed every day to execute affidavits, complete power of attorney documents, and make changes to retirement plans. As the needs of

---

<sup>1</sup><https://www.mckinsey.com/capabilities/growth-marketing-and-sales/our-insights/emerging-consumer-trends-in-a-post-covid-19-world>

business and personal life continued throughout isolation, RON quickly became a vital part of keeping the world moving. Consumer expectations for notarizations quickly changed, and demand for RON is still growing.

Government agencies like the Internal Revenue Service<sup>2</sup> and the Department of Homeland Security<sup>3</sup> are increasingly updating rules and regulations to offer more digital services - including leveraging online notarization - often in use cases that deal with the most sensitive personal data available. As a vast majority of predictions indicate that demand for and consumption of digital services will only increase<sup>4</sup>, it is important for state governments to facilitate a dynamic RON program, leveraging the regulatory process to allow for continued innovations for years to come.

### **Increased Sophistication of Online Identity Fraud:**

As more remote and digital services became available, so did opportunities for fraud. Several reports now indicate that bad actors took advantage of remote and digital services during the pandemic to fraudulently obtain benefits<sup>5</sup> or other property<sup>6</sup>. Much like the demand for digital services, the demand for identity theft protection is also on the rise<sup>7</sup>.

New avenues for those seeking to commit fraud have also materialized. Deepfakes - realistic images or videos produced by AI - have already been a concern for several years<sup>8</sup> and recent advancements in generative AI have heightened concerns about the ability to impersonate individuals online and commit fraud<sup>9</sup>, drastically altering the internet as we know it and the digital identity ecosystem.

Long before the proliferation of digital services, fraud existed. While we must work to mitigate fraud, it is important to understand it will never be eliminated.

By implementing digital services, states can provide solutions that effectively mitigate fraud better than existing paper or in-person processes. States can learn from how they leveraged technology to enhance paper-based notarization to find new ways to enhance the customer experience and reduce fraud across other

---

<sup>2</sup><https://www.napa-net.org/news-info/daily-news/irs-proposes-alternative-person-witnessing-spousal-consents>

<sup>3</sup><https://www.jacksonlewis.com/insights/dhs-takes-step-toward-allowing-virtual-alternative-options-examination-i-9-documents>

<sup>4</sup> <https://finance.yahoo.com/news/global-fintech-faas-market-2028-110300262.html>

<sup>5</sup> <https://www.pbs.org/newshour/politics/how-billions-in-covid-19-pandemic-relief-aid-was-stolen-or-wasted>

<sup>6</sup> <https://www.nytimes.com/2022/08/16/business/economy/covid-pandemic-fraud.html>

<sup>7</sup> <https://finance.yahoo.com/news/identity-theft-protection-services-market-133400152.html>

<sup>8</sup> <https://cybernews.com/security/rise-of-deepfakes/>

<sup>9</sup> <https://finance.yahoo.com/news/generative-ai-tools-lead-rising-130542594.html>

existing document processing use cases. For example, digital documents can provide more data about a transaction, documents can be tamper-sealed, records can be more efficiently retained or even encrypted, and a signer's identity can be verified through identity proofing tools. However, these applications are only effective if state laws offer flexibility in the permitted technology and allow for advancements over time.

Popular identity verification methods like knowledge-based authentication (KBA), SMS verification, and even standard passwords have all played a role in online identity verification. Unfortunately, with time all technological solutions develop points of failure and must be replaced.

In addition to expanding the technological applications of RON, the preservation of the human in online notarization is another learning states can apply to use cases beyond notarization.

### **Importance of the Human Element:**

RON has not eliminated the role of a notary. Instead, it has increased their importance by allowing them to participate in digital commerce. During a RON transaction, the notary still determines whether or not the person on the screen in front of them matches the presented credential if there are signs of duress or issues of capacity, whether or not the results of the identity proofing methods are to be relied upon, and of course to exercise their state conferred powers and actually perform the notarial act. RON is not a replacement for the crucial role a notary has in identifying someone and imbuing a transaction with trust. It merely provides the notary with additional tools otherwise unavailable in the traditional process in order to enhance a necessary practice in today's society.

It is difficult to overstate the notary's importance in the multi-step identity verification process. Notaries are individuals trained in identity and trusted state officials. They are the epitome of the idea of "decentralized trust." In essence, a centralized entity (whether that's an organization, individual, or single technology) is not given authority to make unilateral decisions regarding identity. Similar to the idea of blockchain, this decentralized approach has many benefits. Firstly, failure at a single point is not catastrophic. There are many notaries performing RON, so the unavailability of one does not eliminate the service for all signers. Secondly, a single database to establish someone's identity is not required, providing greater safety for individual data and privacy. Thirdly, the combination of a live person with the aid of technological tools is just harder to fool. But that combination only works to the fullest when the technological tools at the notary's disposal are kept up to date.

### **Keeping RON Secure:**

RON brings many benefits to the notarial process that don't exist in the paper

world. The a/v recording of the notarial session, the ability to have a document signed and notarized anytime and anywhere, the tamper-evident electronic documents and journal, and, of course, the identity proofing methods.

However, identity proofing methods are based on technology, and technology becomes outdated. Typically, KBA and credential analysis are the forms of identity proofing employed for RON. While credential analysis solutions can improve over time, getting better at identifying spoofed credentials or checking information against issuing sources, the same cannot be said for KBA. Unfortunately, much of the information used to generate KBA questions is now available on the internet due to data breaches. When paired with other methods of identity proofing and the notaries validation, KBA can remain a component of identity proofing despite its lapses, but given recent advancements in digital identity, better alternatives are now available to states.

The point is simply this: laws that have adopted RON in such a way that statutorily require KBA to be performed as one of the two identity proofing methods are likely already technologically obsolete. National standards like those suggested by the National Institute of Standards and Technology (NIST) already discount the use of KBA in their identity proofing frameworks<sup>10</sup>, and federal agencies like the National Highway and Traffic Safety Administration (NHTSA) and the Drug Enforcement Agency (DEA) are already relying on NIST's Identity Assurance Levels (IALs) for remote identity proofing. States are also looking to NIST as the next step in identity proofing standards for RON<sup>11 12</sup>.

To continue to leverage RON to fight online identity fraud, states should embrace technology-neutral statutes allowing regulators to approve new technologies as they are ready to be deployed. This approach will allow states to stay current, ahead of the curve, and on top of the fraud prevention fight.

### **Conclusion:**

Digital identity is an important part of the digital economy and only continues to grow in importance. Notaries are primed to continue to play a crucial role in combating fraud and ensuring digital identity is secure, reliable, and proven. States should empower their notaries with the latest technologies in order to fully equip them with the tools needed to perform their roles as trusted state officials.

### **Contact:**

**James Fulgenzi**, Director of Government Affairs & Advocacy, [James.Fulgenzi@notarize.com](mailto:James.Fulgenzi@notarize.com)  
**Dale Hardy**, Senior Counsel, Government & Regulatory Affairs, [Dale.Hardy@notarize.com](mailto:Dale.Hardy@notarize.com)

---

<sup>10</sup> <https://pages.nist.gov/800-63-FAQ/#q-a4>

<sup>11</sup> [https://dos.ny.gov/system/files/documents/2023/01/public-notice-of-adoption\\_remote-notary.pdf](https://dos.ny.gov/system/files/documents/2023/01/public-notice-of-adoption_remote-notary.pdf)

<sup>12</sup> [https://leginfo.legislature.ca.gov/faces/billStatusClient.xhtml?bill\\_id=202320240SB696](https://leginfo.legislature.ca.gov/faces/billStatusClient.xhtml?bill_id=202320240SB696)