
ONLINE NOTARIZATION: IMPLICATIONS FOR THE REAL PROPERTY BAR

By Timothy S. Reiniger (July 15, 2019)

INTRODUCTION: VIRGINIA FRAMEWORK FOR ONLINE NOTARIZATION

Virginia’s Electronic Notaries Act of 2011¹ has emerged as the national model for implementation of “online notarization” – electronic notarization by means of webcam or audio-video teleconference technology² – wherein a signer who is located anywhere in the world can lawfully “appear” online before a notary public who is physically located in the state of commissioning. And, on July 31, 2018, the United States Department of the Treasury called for online notarization to be enacted in all states.³

States that also have enacted the Virginia framework, either in whole or substantial part, now include: Montana (2015), Nevada (2017), Texas (2017), Indiana (2018), Tennessee (2018), Minnesota (2018), Michigan (2018), Ohio (2018), North Dakota (2019), South Dakota (2019), Idaho (2019), Kentucky (2019), Utah (2019), Arizona (2019), Maryland (2019), Washington (2019), Iowa (2019), Oklahoma (2019), Nebraska (2019), and Florida (2019).⁴ In addition, the Uniform Law Commission’s new amendment to the Revised Uniform Law of Notarial Acts (RULONA)⁵ (2018) as well as the National Notary Association’s Model Electronic Notary Act (2017)⁶ incorporate the policy essentials of the Virginia model.

Because of these enactments, real property law practitioners should consider how online notarization may benefit their practices as well as clients. Online notarization leverages audio-video communication technologies to improve the evidentiary function of the notary by: 1) providing strengthened capability of proving document integrity, 2) enabling the means of performing multi-factor authentication as another method by which to confirm the signer’s identity, and 3) requiring that a recording of each online notarization session be made and retained.

ONLINE NOTARIZATION: THE SIX CORE LEGAL PRINCIPLES

The Virginia framework is built on the foundations of the first online notarization law, which was enacted by Utah in 2000.⁷ Unfortunately, the Utah law was tied to a first in the nation digital signature act that ultimately didn’t achieve widespread consumer acceptance and faced concerns about being pre-empted by the technology neutral electronic signature provisions of the federal E-SIGN law.⁸ Nevertheless, the Utah online notarization model has provided three enduring principles: 1) use of audio and visual communications *technology* as a basis of personal appearance before a notary, 2) the notary’s required use of a digital signature or secure electronic signature in performing the online notarial act, and 3) the notary must be physically present in the commissioning state when performing online notarizations.⁹

The Virginia law incorporates the Utah policy principles¹⁰ and adds three others: 1) the signer may be physically located outside of the notary’s commissioning jurisdiction,¹¹ 2) the signer’s identity may be confirmed by means of emerging capabilities for multi-factor authentication¹² consistent with NIST federal standards,¹³ and 3) the notary must make and retain a recording of the audio-video online notarization session.¹⁴

With minor exceptions, the eighteen other states enacting the Virginia framework for online notarization have implemented these six combined policy principles. South Dakota has the greatest variation in that it permits online

notarization only with respect to paper documents. In addition, South Dakota does not recognize any means of confirming the signer's identity other than personal knowledge or a credible witness. As for the other states, the greatest variation can be seen in the decision whether to prescribe or limit the methods for accomplishing successful multi-factor authentication.¹⁵ Other minor variations can be found concerning the electronic journal's retention period and disposal. The Iowa law includes consumer data security restrictions on the transfer and use of personal information collected in the notary's electronic journal.

The kind of audio-video communications technology used in online notarizations has been deemed trustworthy and reliable for court purposes throughout the country. Generally, the standards governing appearance by two-way electronic audio and video communication in courtrooms require that the parties must be able to "simultaneously see and speak to one another" using a live, real-time signal that is secure from unlawful interception.¹⁶ Where such audio-video conference technology is available, the use of this technology constitutes an "appearance" before "a magistrate, intake officer or, prior to trial, before a judge" and these officers "may exercise all powers conferred by law and all communications and proceedings shall be conducted in the same manner as if the appearance were in person."¹⁷

THE BENEFITS OF ONLINE NOTARIZATION: LEVERAGING MULTI-FACTOR AUTHENTICATION, PKI, AND AUDIO-VIDEO RECORDING TECHNOLOGIES

Online notarization significantly strengthens protections against fraud for consumers and businesses by leveraging technologies previously unavailable to traditional notaries.

Establishing the authenticity of digital documents requires proof of origin (identity of the signer), content integrity (whether the document has been altered), and time of execution or issuance.¹⁸ A critical part of the authentication inquiry is whether safeguards have been implemented to assure the continuing accuracy and integrity of the originally created record.¹⁹ Thus identity, integrity, and time, recognized as the three main components of authenticity, must be handled in a fashion that will allow the capability of strong evidentiary tests or proof, in the future, should questions arise.²⁰

Because the general authorizing statutes for electronic signatures in the United States do not prescribe a specific form for an electronic signature,²¹ three particular evidentiary challenges are posed with respect to attribution: 1) an e-signature can be applied to the document without any action by the individual to whom the signature is attributed, or without her knowledge, 2) there is a lack of direct evidence in proving *who* clicked the button or caused the particular electronic signature to be made, and 3) the recipient cannot easily determine whether the sending party authorized the use of the electronic signature.²²

IDENTIFICATION ADVANTAGES: MULTI-FACTOR AUTHENTICATION OF SIGNERS

Online notarization recognizes the reality that, with cloud-based services, signers located outside of the notary's physical presence of the notary can have their identities confirmed online by a notary using common and easily understood software and hardware.

To ensure that online notarization is more reliable and resistant to fraud and manipulation than traditional notarization, the online notary must *confirm* the identity of the signer by using one of a broader selection of methods: 1) personal knowledge; 2) credible witness; 3) reliance on prior (i.e., antecedent) in-person identity proofing²³ performed in connection with the issuance of a credential such as state driver's license or a passport; 4) reliance on successful completion of a dynamic knowledge-based assessment; or, 5) reliance on the signer's use of

a validated digital certificate. The signer's identity will be virtually guaranteed by these new standards-based requirements. In this way, online notarization enables notaries to confirm a signer's identity rather than rely on too easily forged identification documents. By contrast, in traditional paper notarizations, the notary typically has no professional training in, or independent means of, determining if the identity document is forged.²⁴

CYBERSECURITY ADVANTAGES: LEVERAGING PKI FOR INFORMATION INTEGRITY

The validity and enforceability of an electronically notarized document rests upon confirming the legitimacy of the notary who signed the document and establishing the integrity of the signed document itself. Legitimacy involves verifying the identity of the electronic notary who created the electronic signature, the notary's official status, and the notary's territorial jurisdiction. Information integrity involves corroborating that the presented document accurately reflects the data and form of the document originally electronically signed by the signer and the notary.

The notary's signature and seal (commission) information must be affixed to the electronic document using tamper resistant technology. With an electronic notarization performed in this manner, any subsequent attempt to modify the document would be detectable to anyone viewing it. Thus, this tamper evident technology would prevent fraudulent alteration of the document. Currently, states have been opting for the notary's use of a digital certificate in a public key infrastructure (PKI) as the technology best suited to achieve these performance results.

PRIVACY ADVANTAGES: THE NOTARY'S DUTY TO CONTROL ACCESS TO THE ELECTRONIC JOURNAL AND AUDIO-VIDEO RECORDING

Online notarization laws require the notary to adhere to a duty of care evidenced by an electronic notary journal record. Every online notarization must include an accompanying journal record that contains important data about the signer and the transaction. In the event the signer appears before the notary online using video and audio conference technology, the notary also must keep a copy of the recording of the entire audio-video conference.

To enhance consumer protection and deter fraud, the notary must complete and retain an electronic journal of notarial acts that contains at least the following information: (i) the date and time of day of the notarial act; (ii) the type of notarial act; (iii) a description of the document or proceeding; (iv) the printed name and address of each signer; (v) the evidence of identity each signer presented to the notary; and (vi) the fee, if any, charged for the notarial act.

The notary's capability of controlling access to and use of the notarial electronic journal and the audio-video recording is a main privacy concern. At all times, it is necessary for the notary to know who has access to the electronic journals and recordings and for what purpose. With respect to consumer privacy protections, the online notary must adhere to a duty of care in three respects. First, the online notary must maintain exclusive control of the electronic journal and recording. Second, the online notary must provide for lawful access to the electronic journal and recording, whether for inspection by law enforcement, a commissioning official, or in connection with a civil lawsuit investigation. Third, the online notary must have a means of providing certified copies of entries, be able to identify the requesting individual, and complete an entry in the electronic journal for each such access and certified copy request.

The electronic record of an electronic notarial act must be maintained for a period of years varying from state to state but typically for a minimum of ten years the date of the transaction, although notaries (or parties relying on the journal record) may elect to keep the journals and recordings in perpetuity. Some state laws expressly permit the notary to select a third-party repository or custodian for purposes of storing and backing up the journals and

recordings. Criminals will most likely be thoroughly deterred by this recordkeeping requirement; after all, what criminal would willingly sit still for a digital recording of his or her crime?

Criminals will perpetrate fraud in the physical world and the virtual world. The greatest value a notary provides, even going beyond fraud deterrence, is the evidence collected on the notary's certificate and, most especially, in the notary's journal and audio-video recording. And it is this critical recordkeeping function that is guaranteed to be fulfilled by online notarization.

APPLICATION OF ONLINE NOTARIZATION TO REAL PROPERTY

Several leading title insurers in the United States are now underwriting e-closings that include online notarial acts. On July 28, 2017, the first online e-Closing of a home mortgage refinance occurred, when a husband and wife who were physically located in Illinois electronically signed documents, which were notarized, to complete a transaction in Chicago, Illinois.²⁵ This online e-Closing builds on the first public recording of an online deed in the United States, which took place on June 6, 2013, and involved the sale of a property in Alexandria, Virginia, signers in France, and an online notary in Richmond, Virginia.²⁶

Authorization of electronic financial powers of attorney are gaining national traction with the enactment of the Uniform Power of Attorney Act in 26 states. Except for the New Hampshire version, these enactments give evidential benefits to an electronic power of attorney in which the agent's appointment is acknowledged before a notary.

CHALLENGES GOING FORWARD

Implementation of online notarization has raised a number of legal and policy challenges. First, there are ongoing concerns about interstate recognition of online notarizations performed by out-of-state notaries.²⁷ In response to concerns about interstate recognition of electronic notarizations, in 2010 the U.S. Congress unanimously passed an interstate recognition bill that was vetoed by President Obama.²⁸ And now the U.S. Treasury Department appears to be asking Congress to revisit this previous effort.²⁹

Second, with respect to the acceptance for filing or other purposes of electronically notarized documents, questions have been raised as to whether ESIGN and the Uniform Electronic Transactions Act authorize acceptance of paper printouts of the electronically signed documents. In response, the amended RULONA has expressly incorporated authorizing language that some states may opt to enact to ensure acceptance of paper printouts.³⁰

Third, the online notary's duty to maintain the audio-video recording is raising privacy concerns because, under most enactments, the procedures for responding to third-party access requests are unclear. In this respect, online notarization laws have imposed on the notary and her legal representative a duty to enable lawful access to the recording by both signers and third parties, whether for inspection by law enforcement, a commissioning official's request, or in connection with a civil lawsuit investigation.³¹ In addition, the online notary must have a means of providing certified copies of entries, be able to identify the requesting individual, and complete an entry in the electronic journal for each such access and request for a certified copy.

Fourth, the allocation of liability between the notaries, online notarization signing platforms, and third-party identity providers is unclear. There are several liability concerns facing identity providers that remain ill-defined and uncertain with respect to court treatment. Should identity providers have legal protection if they have complied with the applicable notarial standards to validate credentials that were nonetheless incorrectly issued? What is the liability of an identity provider for an identity attribute that is incorrectly verified? Who has the liability

when a relying party disseminates or provides access to valuable or protected data based on a false identity assertion? Thus far, only Virginia provides statutory grounding and liability clarity concerning private-sector identity providers.³²

Fifth, there is a concern that some states, whether through statute or rule-making, will too rigidly limit the available approved processes for automated third-party credential analysis and identity proofing with the result that online services will be foreclosed to many signers such as foreign citizens doing business in the United States, elder citizens, and individuals without a credit history.³³ In addition, administrative rules in states such as Texas, Nevada, Tennessee, and Minnesota, by being statutorily de-coupled from national identity standards issued by NIST, run the risk of undermining efforts at achieving national uniformity along with imposing prescriptive requirements that will be hard to change in response to market changes and technology obsolescence.³⁴ Finally, there is a concern that some states, by authorizing only the use of government-issued credentials, will prevent the ability for signers to use emerging private sector identity provider services that leverage the ubiquity of mobile phones and the FIDO authentication standard.³⁵

THE CHANGING EXPERIENCE OF NOTARIZATION IN THE ONLINE ENVIRONMENT

For real property law practitioners, the strategic management of electronic records must be based on fundamental evidentiary requirements for proving establishing identity, intent, and document integrity. Online notarization gives notaries an enhanced ability to prove the authenticity of electronic signatures, digital identity credentials, and electronic records. The signer personally appears before the notary via real-time interactive audio-video conference technology and, thereby, invokes the notary's authority and jurisdiction.³⁶ And the online notarial act remains valid through time, regardless of the physical location of the signer and where the document is filed.

Twenty-three states now have enacted online notarization laws.³⁷ And with the Uniform Law Commission having added authorization language to the RULONA, more states are expected to join this trend next year. The Virginia framework for online notarization is now achieving adoption throughout the United States.

ABOUT THE AUTHOR

Timothy S. Reiniger, Esq.

Timothy Reiniger is an attorney and Director of the Reiniger, LLC, in Cape Elizabeth, Maine. Previously, he was the Director of the Digital Services Group at FutureLaw, LLC in Richmond, Virginia where he was an author of the Virginia Online Notarization law (2011) as well as the Digital Identity Management law (2015). He specializes in information governance (identity, privacy, security, and digital evidence). He is a nationally recognized expert on the notary office and electronic signatures, testifying on these topics before the U.S. House Judiciary Committee, and a dozen state legislatures. Tim has been appointed as an ABA Advisor to both the Uniform Law Commission's drafting committee to amend the Revised Uniform Law on Notarial Acts and the Identity Management in Electronic Commerce Study Committee. An internationally recognized expert on information governance, Tim serves on the Advisory Board of the European Union's LIGHTest Project and as a Vice-Chair of the Information Security Committee of the ABA's Science & Technology Law Section. He is a member of the California, District of Columbia, Maine, and New Hampshire Bars.

¹ Virginia Chapter 731 of 2011, *available at*: <http://leg1.state.va.us/cgi-bin/legp504.exe?111+ful+CHAP0731>.

² For purposes of consistency in this article, the term "online notarization" is used. Other descriptors with the same meaning include "remote notarization," "remote electronic notarization," "remote online notarization," "webcam

notarization,” “electronic notarial acts by means of audio-video communication,” and “notarial act performed by remotely located individual.”

³ U.S. Department of the Treasury, *A Financial System that Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation* (July 2018), p. 109 (“Treasury recommends that states yet to authorize electronic and remote online notarization pursue legislation to explicitly permit the application of this technology and the interstate recognition of remotely notarized documents. Treasury recommends that states align laws and regulations to further standardize notarization practices.”), *available at*: <https://home.treasury.gov/sites/default/files/2018-07/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financi....pdf>.

⁴ MONT. CODE ANN. §§ 1-5-601-28; Nevada: (Chapter 15 of 2017 session) <https://www.leg.state.nv.us/Session/79th2017/Reports/history.cfm?ID=1078>; Texas (Chapter 340 of 2017 session) <https://capitol.texas.gov/tlodocs/85R/billtext/html/HB01217F.HTM>; Indiana: (P.L. 59-2018) <https://iga.in.gov/legislative/2018/bills/senate/372>; Tennessee (Chapter 931 of 2018 session) <http://www.capitol.tn.gov/Bills/110/Bill/HB1794.pdf>; Minnesota (Chapter 176 of 2018 session) https://www.revisor.mn.gov/bills/text.php?version=latest&session=ls90&number=SF0893&session_year=2018&session_number=0; Michigan (PA 330 of 2018) <https://www.legislature.mi.gov/documents/2017-2018/publicact/pdf/2018-PA-0330.pdf>; Ohio (Session 2018-121) <https://www.legislature.ohio.gov/legislation/legislation-documents?id=GA132-SB-263>; North Dakota (HB 1110 of 2019) <https://www.legis.nd.gov/assembly/66-2019/documents/19-0254-04000.pdf>; South Dakota (HB 1272 of 2019) <https://sdlegislature.gov/docs/legsession/2019/Bills/HB1272ENR.pdf>; Idaho (Chapter 160 of 2019) <https://legislature.idaho.gov/wp-content/uploads/sessioninfo/2019/legislation/S1111.pdf>; Kentucky (SB 114 of 2019) <https://apps.legislature.ky.gov/recorddocuments/bill/19RS/sb114/bill.pdf>; Utah (HB 52 of 2019) <https://le.utah.gov/~2019/bills/hbillenr/HB0052.pdf>; Arizona (SB 1030 of 2019) <https://www.azleg.gov/legtext/54leg/1R/bills/SB1030S.pdf>; Maryland (SB 678 of 2019) <http://mgaleg.maryland.gov/2019RS/bills/sb/sb0678E.pdf>; Washington (SB 5641 of 2019) <http://lawfilesexet.leg.wa.gov/biennium/2019-20/Pdf/Bills/Senate%20Bills/5641.pdf>; Iowa (SF 475 of 2019) <https://www.legis.iowa.gov/publications/search/document?fq=id:1042726&q=notary>; Oklahoma (SB 915 of 2019) http://webserver1.lsb.state.ok.us/cf_pdf/2019-20%20COMMITTEE%20SUBS/HCSS/SB915%20HCS.PDF; Nebraska (LB 186 of 2019) <https://nebraskalegislature.gov/FloorDocs/106/PDF/Final/LB186.pdf>; Florida (Chapter 2019-71) <http://laws.flrules.org/2019/71>.

⁵ See the REVISED UNIFORM LAW ON NOTARIAL ACTS (2018), as approved by the Uniform Law Commission on July 25, 2018, *available at*:

<https://www.uniformlaws.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=aec212eb-a1e8-183a-13dd-587c7604666e&forceDialog=0>.

⁶ See THE MODEL ELECTRONIC NOTARIZATION ACT (NAT’L NOTARY ASS’N 2017), *available at*:

<https://www.nationalnotary.org/file%20library/nna/reference-library/model-enotarization-act.pdf>. The MENA has influenced the enactments in Texas, Indiana, Minnesota, and Tennessee as well as the recommended legislative package offered by the American Land Title and Mortgage Bankers Association, *available at*:

<https://www.mba.org/audience/state-legislative-and-regulatory-resource-center/remote-online-notarization>. The MENA’s influence is particularly evidenced by a requirement for the notarial certificates to indicate the fact that an online notarization was performed.

³ Utah Chapter 312 of 2000 (repealed in 2006), *available at*: <https://le.utah.gov/~2000/bills/sbillenr/SB0145.htm> and administrative rule R154-10-502 implementing technical specifications (repealed in 2007), *available at*: https://rules.utah.gov/publicat/bull_pdf/2001/b20010415.pdf.

⁸ ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT (“ESIGN”) (2000), 15 USC §§ 7001 *et seq.*

⁹ Every state currently provides for recognition of other states’ notarial acts. For a list of citations, see the Comment to Sec. 6-3 of the MENA, *supra* note 6, at 40. And beyond this longstanding statutory regime, over a century ago the United States Supreme Court, in *Pierce v. Indseth*, 106 U.S. 546, 550 (1882), held that a duly performed notarial act from outside the United States was entitled to full faith and credit in U.S. state courts.

¹⁰ Virginia law integrates the Utah principles in the following provisions respectively: VA. CODE ANN. § 47.1-2 and § 47.1-15 (A)(1) (policy one); § 47.1-16 (D) (policy two); and, § 47.1-2 (definitional distinctions between ‘electronic notarial act’ and ‘notarial act’) and § 47.1-13 (A) (policy three).

¹¹ Pursuant to VA. CODE ANN. § 47.1-13 (D), the online notarial acts are deemed to have taken place in Virginia and under Virginia law.

¹² Standards-based authentication is based on three factors consisting of something you have, know, or are. Multi-factor authentication requires a combination of these.

¹³ VA. CODE ANN. § 47.1-2. See NIST 800-63-3 guidance series for digital identity proofing and verification and digital identity management generally, and which govern the Federal PKI Authority and Federal Bridge Certificate Authority, *available at*: <https://pages.nist.gov/800-63-3/>.

¹⁴ VA. CODE ANN. § 47.1-14 (C).

¹⁵ For example, in many of the enactments, the only acceptable identity credential is one that is government issued.

¹⁶ *See, e.g.*, VA. CODE ANN. § 19.2-3.1 (B). Note that the Virginia law expressly cross-references the Virginia Supreme Court standards for audio-video conference testimony.

¹⁷ VA. CODE ANN. § 19.2-3.1 (A).

¹⁸ WINN & WRIGHT, *THE LAW OF ELECTRONIC COMMERCE* § 20.05 (4th ed. Aspen Publishers, Inc. 2007); *See generally* George L. Paul, *The 'Authenticity Crisis' in Real Evidence*, 15 *THE PRACTICAL LITIGATOR* No. 212-13 (2004).

¹⁹ *See In re Vinhnee*, American Express Travel Related Service Co. Inc. v. Vinhnee, 336 B.R. 437 (9th Cir. B.A.P. 2005) (proponent failed to authenticate computer generated business records because of an inability to assure content integrity over time).

²⁰ GEORGE L. PAUL, *FOUNDATIONS OF DIGITAL EVIDENCE* (American Bar Association 2008) at 36.

²¹ *See* E-SIGN, 15 USC § 7006(6) and UNIF. ELEC. TRANSACTIONS ACT § 2(8) (Nat'l Conf. of Comm'rs on Unif. State Laws 1999), both of which define an electronic signature as "an electronic sound, symbol, or process" attached to or logically associated with a contract or other record and "executed or adopted by a person with the intent to sign the record." This definition reflects the historical case law emphasis on the legal function of the signature instead of the form.

²² For a discussion of the evidentiary proof challenges concerning electronic signatures generally, see STEPHEN MASON, *ELECTRONIC SIGNATURES IN LAW* 155, 170, 185, and 301 (Cambridge University Press 4th ed. 2016), *available at*: <http://humanities-digital-library.org/index.php/hdl/catalog/book/electronic-signatures>.

²³ As a baseline, NIST 800-63-3 defines "identity" as "[a]n attribute or set of attributes that uniquely describe a subject within a given context" and "identity proofing" as "[t]he process by which a CSP [Credential Service Provider] collects, validates, and verifies information about a person." The term "identity proofing" encompasses a wide variety of methods, including but not limited to antecedent proofing (previously issued digital certificates, government identity credentials, and private sector credentials based on an in-person vetting), credential analysis, biometrics, and dynamic knowledge-based assessment.

²⁴ NIST 800-63A permits validation of identity credentials by means of professionally trained personnel or automated checks with appropriate technologies.

²⁵ *See* ANDRE MACDOUGALL, *THE COMPLETE GUIDE TO REMOTE ONLINE NOTARIZATION* 43 (2019), *available at*: <http://notarize.com/guide-to-remote-online-notarization>.

²⁶ *See* Phillip Marson & Timothy Reiniger, *The Deed is Done*, 10 *DIGITAL EVIDENCE & ELECTRONIC SIGNATURE LAW REVIEW* 144 (2013) *available at*: <http://journals.sas.ac.uk/deeslr/article/view/2034>.

²⁷ While state notary laws fall within the terms of the Full Faith and Credit Clause of Article IV of the United States Constitution, all states have enacted interstate recognition provisions to ensure cross-border enforceability of individual notarial acts. *See supra* note 9. However, this state-level treatment has proven to be inconsistent with respect to the types of out-of-state notarial acts that are deemed enforceable. For example, Iowa limits interstate recognition of online notarizations. IOWA CODE ANN. § 9B.11(4) (specifying that personal appearance is satisfied only by the performance of online notarizations by out-of-state notaries in a manner specified by Iowa law as opposed to the law of the notary's commissioning state).

²⁸ With the "Interstate Recognition of Notarizations Act of 2010" (the "IRON Act"), shepherded by Representative Robert Aderholt of Alabama, the United States Congress sought to establish a uniform national evidence-based approach for ensuring the enforceability of both paper and electronic out-of-state notarial acts. *See*, H.R. 3808, 111th Cong., 2d Sess., 111 CONG. REC. S7558 (2010) ("Each court that operates under the jurisdiction of a State shall recognize any lawful notarization made by a notary public licensed or commissioned under the laws of a State other than the State where the court is located if...in the case of an electronic record, the seal information is

securely attached to, or logically associated with, the electronic record so as to render the record tamper-resistant”) *available at*: <http://www.gpo.gov/fdsys/pkg/BILLS-111hr3808enr/pdf/BILLS-111hr3808enr.pdf>. The bill hearing is *available at*: <https://www.gpo.gov/fdsys/pkg/CHRG-109hhr26412/html/CHRG-109hhr26412.htm>. For a discussion of the veto of the Interstate Recognition of Notarizations Act of 2010 (“IRON Act”), *see* <https://www.secureidnews.com/news-item/iron-act-veto-impacts-national-strategy/>.

²⁹ *See supra* note 3, at 109 (“Treasury further recommends that Congress consider legislation to provide a minimum uniform national standard for electronic and remote online notarizations. Such legislation would facilitate, but not require, this component of a fully digital mortgage process and would provide a greater degree of legal certainty across the country. Federal legislation is not mutually exclusive with continued efforts at the state level to enact a framework governing the use of electronic methods for financial documents requiring notarization.”).

³⁰ RULONA Section 4(c) and Section 20(c).

³¹ Note that Minnesota 358.645 Subd 12(b) permits third-party access to the recording only with the prior consent of the signer or the signer’s legal representative. In fact, Minnesota expressly provides that the notary’s electronic journal and recordings are not public records.

³² Virginia Chapter 483 of 2015, *available at*: <https://lis.virginia.gov/cgi-bin/legp604.exe?151+ful+CHAP0483+pdf>.

³³ The Minnesota statute and the rules issued by the Secretaries of State in Tennessee and Texas are examples of a rigid approach toward identity proofing that authorizes only automated means of credential analysis. In contrast, the RULONA requires two factors of identity proofing without specifying or limiting the types of processes or technologies that may be used.

³⁴ For an example of an industry-specific approach, see the MISMO standard efforts that some states are looking to as an alternative to the NIST guidelines, *available at*: <http://www.mismo.org/get-started/participate-in-a-mismo-workgroup/remote-online-notarization-dwg>. In contrast, see the Treasury Report, *supra* note 3, at 199: “Treasury supports the efforts of OMB to fully implement the long-delayed U.S. government federated digital identity system. Treasury recommends policies that would restore a public-private partnership model to create an interoperable digital identity infrastructure and identity solutions that comply with NIST guidelines and would reinvigorate the role of U.S. government-certified private sector identity providers, promoting consumer choice and supporting a competitive digital identity marketplace.”

³⁵ For information about the FIDO Standards, see <https://fidoalliance.org/>.

³⁶ See the comments to THE MODEL ELECTRONIC NOTARIZATION ACT § 2-1 at 5 (NAT’L NOTARY ASS’N 2017) (“‘Personal appearance’ is the fundamental manner in which principals avail themselves of the jurisdiction, authority, and legal power of a notary public as a public officer.”).

³⁷ In addition to the twenty-two previously referenced states, last year Vermont enacted a version of RULONA that gave the Secretary of State power to authorize online notarization by means of rule-making (H 526), *available at*: <https://legislature.vermont.gov/bill/status/2018/H.526>. The rules, however, have not yet been issued.