June 23, 2022

Hon. Janice D. Schakowsky, Chair
House Committee on Energy & Commerce
Subcommittee on Consumer Protection & Commerce
2125 Rayburn House Office Building
Washington, DC 20515

Hon. Gus M. Bilirakis
House Committee on Energy & Commerce
Subcommittee on Consumer Protection & Commerce
2322 Rayburn House Office Building
Washington, DC 20515

RE: H.R.3962/S.1625 (SECURE Act/Online Notarization) Mark-Up

Dear Chair Schakowsky and Ranking Member Bilirakis,

As individual members of the leadership of the Information Security Committee of the American Bar Association Section of Science and Technology ("Section"), we thank the U.S. House of Representatives Commerce and Energy Committee for the opportunity to provide comments on H.R.3962, the Securing and Enabling Commerce Using Remote and Electronic Notarization Act ("SECURE Act") for an upcoming Mark-Up. These comments have not been reviewed or approved by the House of Delegates or the Board of Governors of the American Bar Association or the entire Section and, accordingly, should not be construed as representing the position of the Association. A process to obtain formal Section approval of the comments is underway.

I. Observations and Experiences

Based on analysis of the SECURE Act the Section has important concerns to bring to your attention. Existing state electronic notarization laws and regulations intended to provide strong consumer protections will be preempted by the SECURE Act's technology and technical specification neutrality provision, which mandates lower security standards.

First, the Section is concerned that the current federal and state legal framework for electronic notarization authorization, as embodied in the ESIGN Act (15 U.S.C. 7001(g)) and the state enactments of the Uniform Electronic Transactions Act (UETA)(Section 11), will be superseded by the SECURE Act's legal framework. Section members actively worked on the development of these laws back in 1990 and 2000. Notably, the UETA specifically provided for signer attribution and document integrity by means of a security procedure. A wide majority of

states with electronic notarization laws have specified the technology means by which notaries can be attributed. And, to-date, there have been no legal hurdles with either enforceability or interstate recognition. Nevertheless, the SECURE Act combined with the Revised Uniform Law on Notarial Acts represents a conflicting legal framework to that created by ESIGN and UETA.

Second, there is no need for a federal remote online notarization (or "RON") law. When first introduced in the last Congress, the SECURE Act was intended to facilitate efforts to authorize RON throughout the entire United States. At the time of introduction, only 16 states had RON laws. However, now all but 9 states and Washington, D.C. have chosen to enact RON laws. And all of the current RON laws have operated without legal rejections as to validity or acceptability for cross-border recognition.

Third, in its current form, the SECURE Act will pre-empt notarial laws in 43 states. An unintended result of this will be diminished consumer fraud protections that are provided by the current state secure e-notarization laws. Specifically, the technology neutrality provision in the "exception to pre-emption" in Section 9 will overrides or pre-empt existing state requirements (whether in statute or regulations) that require notaries to use specific secure technologies and technical performance criteria, typically in the form of a digital certificates (X.509 standard) or Public Key Technology, needed to assure notary attribution as well as document integrity. As a result, the SECURE Act's technology neutrality requirement will serve to mandate lower security standards for notaries public.

An additional unintended consequence of pre-empting current state electronic and online notarization laws will be to render the notarizations defective or void. Trustees in bankruptcy look to allege defective notarization as a basis for defeating mortgage security interests. To the extent electronically notarized records are involved, the state law pre-emptions resulting from the SECURE Act will provide a new basis for alleging defective notarization and undermine mortgage security interests in 36 states.

II. Proposed Amendments

Four amendments are needed (see attached markup) that address two chief concerns: 1) too low a "floor" for security and fraud prevention in Section 3 (electronic notarization) that is inconsistent with current state-based secure electronic notarization laws and 2) pre-emption of current state laws and regulations that provide technology-specific requirements and performance criteria for electronic and/or remote electronic notarization.

<u>Amendment 1 (SEC. 2)</u>

In Section 2 (Definitions) a new term is needed – "Security Procedure" – with definition language taken verbatim from the Uniform Electronic Transactions Act (UETA)(1999), Section 2(14). For twenty years, the UETA (Section 11), along with the Federal ESIGN law (Section 101(g), have authorized electronic notarization throughout the United States. The UETA has been enacted in 49 states and DC. The exception is New York, which has now authorized electronic notarization in the form of secure electronic signatures with a separate law.

The "Security Procedure" in the context of electronic signatures and electronic records addresses two essential consumer protection and evidentiary reliability aspects: 1) attribution of an electronic signature as the act of a particular identified person and 2) content integrity of the

electronic record, otherwise referred to as “tamper-evidence.” Attribution of an electronic signature as the actual act of a notary public (or any signer) is an essential forgery/fraud prevention measure. As a result, states have used UETA as authorization to specify that electronic notarization must be performed in the manner of a security procedure so as to avoid ease of impersonating the notary.

Amendment 2 (SEC. 3(b)(1)

In Section 3(b)(1) (Electronic Notarization Authorization), the requirement that the notary’s electronic signature be attributed as the notary’s act needs to be expressly added to raise the level of consumer protection to reflect the UETA and prevent impersonation of the notary. For consistency with UETA, reference should be made expressly to the “Security Procedure” concept. The current draft of the SECURE Act references only the tamper-evidence aspect of the security procedure and, therefore, sets too low a “floor” for consumer protection by omitting the notary attribution aspect.

Since 1999, one of the clear standards that has arisen in the field of electronic notarization is that an electronic notarial act must qualify as a “security procedure” with the important capabilities of establishing who signed and notarized an electronic record and rendering a notarized electronic record as tamper-evident. Currently, 36 states, either by statute or administrative rules, have established security procedure requirements for notary attribution. Typically, this is in the form of technology specific solutions such as digital certificates or technology-specific security performance criteria that only can be met currently by use of digital certificates.

The Electronic and Online Notarization Standards of the National Association of Secretaries of State incorporate the attribution requirement:
“The notary public's electronic signature is deemed to be reliable if the following requirements are met: a) it is unique to the notary public, b) it is capable of independent verification, c) it is retained under the notary public's sole control, and d) it is attached to or logically associated with the electronic document in a tamper-evident manner. Evidence of tampering pursuant to this standard may be used to determine whether the notarial act is valid or invalid.”

According to a leading member of the ABA SciTech Section, George L. Paul - “Concerning electronically notarized documents, an international and national e-document authenticity standard has emerged that reflects the evidentiary need for electronic documents to have the capability of authenticity testing. This standard requires that any relying party be able to verify the origin and integrity of the notarized electronic document. Establishing the authenticity of a notarized document thus requires the capability, in perpetuity, of independently authenticating the notary, and verifying whether the content of the electronic document is complete and unaltered.” (George L. Paul et al., FOUNDATIONS OF DIGITAL EVIDENCE, p. 212 (ABA, 2008).)

Finally, consistent with the Federal Rules of Evidence (Rule 902(1)) and the rules of evidence in nearly every state, a reference to the notary public’s “seal of office” needs to be included as a minimum criterion in performing electronic notarizations.

Amendment 3 (SEC. 9(a))

In Section 9 (Exception to Pre-emption), an amendment is needed to omit express reference to technology and technical specification neutrality in order to prevent unintended pre-emption of the 36 state laws that have technology specific requirements for the performance of an electronic notarization as a security procedure. Left intact, the SECURE Act's technology neutrality provision, combined with the minimal security requirement of tamper-evidence, would pre-empt the state laws and regulations that address notary identity attribution and, thus, have the effect of removing an essential consumer protection. With this amendment, the notary forgery prevention "ceiling" would be raised beyond the mere requirement of tamper-evidence.

Also subject to pre-emption for violation of technology neutrality will be the states that have specified certain technologies and performance criteria for verifying or authenticating the identity of signers. Such specific technologies include biometrics, knowledge-based assessment tests, and Federal NIST 800-63 standards for authentication assurance. Fifteen states give express authorization for notaries public to rely upon biometrics.

For several reasons, an amendment is also needed to remove express reference to RULONA as the only model electronic notarization law. First, electronic notarization has already been authorized by UETA for twenty years, including the security procedure provision that many states have applied in the notary context. RULONA is designed and intended as a supplement to the UETA. For this reason, RULONA does not contain a security procedure provision for attribution because it would be duplicative of UETA. By analogy, the Uniform Real Property Electronic Recording Act supplements the underlying authorization for official electronic recording set forth in UETA. Second, RULONA (2021) contains a remote ink-signed notarization authorization that has not gained wide acceptance (aside from temporary state COVID-19 emergency orders) and, in fact, raises serious security concerns because of diminished controls around the paper documents as compared to the remote and electronic notarization processes. Third, RULONA, although highly regarded, is not the only model law for electronic and remote notarization. In fact, the Model Electronic Notarization Act (2017), has influenced the MBA/ALTA Model RON Law and electronic notarization enactments in Arizona, Delaware, Florida, Illinois, Indiana, Missouri, Nebraska, Nevada, New York, North Carolina, Ohio, Oklahoma, South Carolina, Tennessee, Texas, and Virginia.

Amendment 4 (SEC. 8(a))

Finally, because state electronic and online notarization laws will be immediately subject to pre-emption by the SECURE Act, it would be advisable to add express reference to Section 9 in the "Validity Not Affected" clause (Section 8(A)) or, alternatively, an entire Savings Clause for those notarizations that will continue to be performed until such time as the affected state laws are formally amended.

III. Conclusion

As individual leaders of the Information Security Committee, we respectfully request that the House Commerce and Energy Committee work with Section members and interested state officials to develop appropriate amendments to the SECURE Act that would avoid the state law preemption problems. Should you have any questions or would like to discuss these issues further, please do not hesitate to contact us.

Respectfully submitted,

/s/

Michael Aisenberg, Committee Co-Chair

/s/

Timothy Reiniger, Committee Vice-Chair