Virginia’s Electronic Notaries Act of 2011 is the first law to authorize remote notarization, cloud-based online notarization by means of audio-video teleconference technology wherein a signer who is located anywhere in the world can “appear” online before a duly commissioned Virginia notary public. The intent of the act is to improve the notary process by strengthening identification methods for principals and notaries, provide better tools to deter and detect fraudulent notary transactions, and to make notarization—virtually unchanged in form or function since Roman times—adaptable to consumer, business, and government transactions in today’s global digital network-based information economy. The act is not without controversy. Indeed, several states and one territory (California, Colorado, Nevada, New Jersey, Ohio, Oklahoma, Oregon, the Northern Marianas, Rhode Island, and Wisconsin) have issued notices that online webcam notarizations are not authorized by law. Still, Virginia’s law is supported by many, and the authors predict the demand for remote notarization will grow rapidly. In this article, we explain the role that virtual appearance seems destined to play as digital networks and cloud computing drive demand for electronic notarization.

What Is All the Controversy About?
A notary public is traditionally defined as “[a] person authorized by a state to administer oaths, certify documents, attest to the authenticity of signatures, and perform official acts in commercial matters, such as protesting negotiable instruments.” The purpose of notarization is to make an instrument self-authenticating. Notarization provides a powerful presumption of authenticity that the document is what it purports to be and that the signer executed it voluntarily with the requisite intent, even in situations where the signer alleges he did not sign the underlying document. It is for this reason that notarization is a prerequisite to recordation of land title and real estate documents in all 50 states. Virginia’s Electronic Notaries Act of 2011 authorizes this function to be fulfilled by use of two-way audio-video conferencing.

As noted above, all states currently require that the signer appear physically before the notary to request a notarization. This traditional requirement is designed to ensure that the notary has the ability to properly identify the signer and to attribute a signature to a specific physical document. This requirement thus helps to deter fraudulent signatures. But it is important to understand that the requirement of personal appearance, as limited to physical presence, does not prevent fraudulent notarizations. That is why perhaps the greatest value a notary could provide is not to deter fraud through the physical appearance of a signer, but to preserve evidence of the signer’s true...
identity in the notary’s certificate and, most especially, in the notary’s journal. Indeed, the journal provides critically important evidence of the signer’s true identity (such as a signature and, in California, a thumbprint) and can be used by law enforcement to prosecute criminals who impersonate signers or commit a fraudulent transaction.

A notary binds a signer to a document and establishes an evidentiary presumption of due execution that is very difficult to overcome. By enabling notaries and signers to meet in real time online and communicate with each other by audio-video conference technology, the act provides the functional equivalent of traditional, pen-and-ink notarization. Both the Uniform Electronic Transactions Act (UETA) and the Federal ESIGN Act recognize that electronically based transactions and records are the “functional equivalent” of their paper counterparts, and both also expressly include the electronic acts of notaries public in this context. Most importantly, the Electronic Notaries Act dramatically strengthens identification requirements for signers and guarantees that an accurate and reliable journal record (that includes a digital recording of the notarization event itself) will be kept by every electronic notary. In addition, the act follows existing legal precedents for the “virtual appearance” of a signer in many legal contexts.

Now Appearing Virtually in a Courtroom Near You

In many states, the kind of videoconference technology contemplated by the act already has been deemed trustworthy and reliable in many criminal and civil proceedings. In Virginia, standards governing appearance by two-way electronic audio and video communication for courtroom use 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. 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.”

The same standards apply to two-way videoconferencing testimony at a criminal trial regarding a certificate of analysis. Such testimony, while subject to objection by the accused, is deemed reliable and trustworthy if certain common sense safeguards are in place.
“Virtual” Appearance by Proxy: Agency Principles
Long before two-way audio-video conference technology came into existence, the common law of signatures and traditional paper notary practices recognized a flexible approach towards personal appearance that, in effect, set a precedent for the concept of “virtual” appearance by an agent of the signer.

Appearance by Agent: The Principle of Signatures Under the Common Law
Relying on the common law, for example, legal advisors to the president of the United States have concluded that, “the common law recognized that one could sign a document not only with one’s own hand, but also by the hand of another who was properly authorized to affix one’s signature to the document on one’s behalf or who did so in one’s presence. Furthermore, a document signed in one’s name by the hand of another in either of these manners was equally effective as a document signed with one’s own hand.” All of which is to say that the president does not need to personally sign a bill to enact it into law but can instead designate a third party or “auto pen” to sign for him. The principle of signatures under the common law thus does not require the physical presence of the signer and would seem to allow for an electronic agent or the virtual appearance of the signer electronically.

Appearance by Subscribing Witness
These common law agency principles also resonate in the context of the contemporary statutory authority of a “subscribing witness” to sign for an absent principal before a notary public.

Under California law, for example, a principal bound by a notarized document need not personally appear before a notary public. Instead, the signer may designate a representative, called a subscribing witness, to take an oath before the notary that the principal’s signature on a document is genuine and authentic. Such a “proof of execution” is allowed in other states as well. Similarly, the Uniform Law Commission’s Revised Uniform Law on Notarial Acts allows a person acting in a “representative capacity” to bind an absent principal whom the person represents.

The Benefits of Virtual Appearance
The common law and the subscribing witness illustrate that “appearance” is a fluid term in context. These agency principles likely developed to accommodate commercial complexity and the reality that one person could not act on behalf of a complex organization like the modern-day global corporation. By allowing a company’s agents to execute contracts, the company can do business in multiple places at the same time. Virtual appearance would allow that same busy principal to appear himself before a notary by leveraging online audio-video conference technology.

The act evolves notary law to accommodate these agency principles in the Internet age. More importantly, the act was written to deal with the increasingly troubling issue of fraudulent notary transactions. The problem with traditional notarization is that the tools used by notaries are no longer effective to combat even the most inexperienced user of a desktop computer. A notary’s seal and signature on a paper document can easily be scanned and manipulated electronically. Indeed, one of the authors of this article served as an expert witness in a case involving precisely this kind of fraudulent activity. In addition, the validity of the notary’s rubber-stamp seal cannot be verified independently or electronically—currently, no reliable means exists to determine whether a notary’s commission has been revoked, suspended, or is expired. Parties relying on the notarized document thus have no means to verify the authority of notary to act in the first place, which often leaves courts to wrestle with the fact of an expired notary commission on a document by means of the common law de facto notary doctrine.9

Further, fewer than half the states currently require notaries to maintain a journal record of critical identifying information about the signer or witnesses. And of those states that do require a journal, none reliably enforce the notary’s failure to keep a journal entry. A signer who presents a fake ID to a traditional notary, in other words, can do so with little fear of criminal prosecution.

The reality of traditional notarization is this: signers and relying parties are left with few if any protections against criminals who wish to fraudulently notarize a document. Forging a notary’s seal and signature on a recorded deed of trust, for example, to fraudulently transfer title to property, is accomplished by criminals with little or no effort. When law enforcement searches for the notary’s journal record to verify the identity of the criminal, the journal entry rarely is available because the journal record is a voluntary requirement in many states and laxly enforced as a requirement in states with strict recordkeeping laws.

By the late 1990s, some professional notary commentators lamenting that notaries were stuck using nineteenth century tools to handle twenty-first century transactions were recognizing the inevitability of virtual appearance. To make such virtual appearance practical in the context of notaries, however, these commentators suggested that technologies would need to be developed that included the real-time

The logic of requiring a signer to physically appear before a notary in order to attribute a particular person to a particular document no longer applies.
Remote Notarization Under Virginia Law
Virginia’s Electronic Notaries Act of 2011 recognizes the reality that, with cloud-based services storage, electronic documents and their signers now can act virtually more easily than ever before. Signers located outside of Virginia and not in the physical presence of the notary can still appear online before a Virginia notary using common and easily understood software and hardware.

In the case of remote notarization, the signer does not have to be in the physical presence of the notary at the time of notarization. Instead, the signer and notary meet online via audio-video conference technology. To enable this connection, both the signer and the notary must have a computer with a webcam and audio capability so that the signer and notary can both see and hear each other. For sake of discussion, we will describe the generic remote notarization process below in the context of a very traditional event: a borrower closing a loan on a new home.

As is common in most business environments today, the title company sends an email to the borrower that contains a scheduled date and time for the online conference with the notary. Prior to this, the title company would have alerted the notary and confirmed the notary’s availability for the conference. In most situations, the title company would provide an online contract signing tool using encrypted communications and secured servers to provide a secure and confidential online contract signing software service to both the borrower and the notary.

In a typical home loan closing, a borrower must sign two or three documents that also require notarization. The title company would upload the documents to be signed and notarized into the secure online system, and both the signer and the notary would log in and view the document simultaneously on their respective computer monitors. The signer would electronically sign the document by clicking a “Sign Here” button or similar button, and the signer would verbally acknowledge his intent to sign the document to the notary. The notary would then countersign the document by clicking a similar “Notarize Here” button. When the notary clicks the button, the notary’s commission information, including the notary’s full name, date of commission expiration, and commission number, would be affixed to the document along with the notary’s electronic signature. The electronic signature of the notary and the signer would appear as a “script font,” much like this example: *John Doe.*

Both the signer’s signature and the notary’s signature and commission information must be affixed to the electronic document using tamper-evident technology. Any attempt to modify the document after notarization would be detectable to anyone viewing the document. This tamper-evident technology would prevent fraudulent alteration of the document.

In traditional notarization, a notary identifies a signer by viewing the signer’s identity document (typically a driver’s license or passport). The notary, of course, has no means to determine if the identity document is forged. To ensure that remote electronic signing is more reliable and resistant to fraud and manipulation than traditional notarization, the remote notary must confirm the identity of the signer by using one of three methods: (1) personal knowledge; (2) reliance on prior (antecedent) in-person identity proofing by a trusted third party (such as a state department of motor vehicles, bank, law firm, or title company) that can be confirmed electronically with independent database checks; or, (3) reliance on the signer’s use of a digital certificate that is authenticated either by a biometric or a high-security PIV card issued by the federal government or a PIV-I card issued by a nonfederal identity provider. Antecedent in-person proofing, which will likely be the most common methodology initially employed, must conform to the high standard of reliability defined by the Federal PKI Management Authority. Methods two and three, in particular, require that the signer be identified using some of the most stringent identification standards available today—standards that military personnel and federal government officials, for example, must submit to in order to be issued a government identification card. The signer’s identity will be virtually guaranteed by these new stringent requirements. In this way, remote notarization enables notaries to confirm a signer’s identity rather than rely on too easily forged identification documents.

Perhaps most significantly, the Virginia law requires a notary to adhere to a duty of care evidenced by an electronic notary journal record. Every remote notary transaction must include an accompanying journal record that contains important data about the signer and the transaction. In addition, every electronic journal record must include a digital recording of the entire video and audio conference between the signer and the notary. The electronic record of an electronic notarial act must be maintained for a period of at least five years from the date of the transaction, although notaries (or parties relying on the journal record) may elect to keep the records in perpetuity. 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 crime?

The Removal of Physical Presence: Cloud Computing
The cloud’s capacity for remote or nonclient applications and storage is forcing a re-examination of the legal definition of “appearance.” With digital networks...
and cloud computing, there is no longer a geographic-bound physical connection between the document and the signer. Therefore, the logic of requiring a signer to physically appear before a notary in order to attribute a particular person to a particular document no longer applies.

Nevertheless, the need for parties to establish the legal authenticity of electronically notarized documents persists. As industry and government move increasingly to cloud-based computing platforms, the message truly matters more than the medium. Online notarization enables a virtual and conscious presence of signers and the individuals who must witness acts for self-authenticating proof and provides a legal means of attributing the document to a particular individual. Thus, remote notarization provides a functionally equivalent experience to traditional pen-and-ink notarization.

The strategic management of information assets in the cloud must be based on fundamental evidentiary requirements for proving authenticity and reliability. Because of the ephemeral nature of digital data, unlimited copying and geographic locations of digital information and ubiquity of networks and access to documents, distinguishing between authentic and forged digital records is a central evidentiary concern.

Thus, following years of discussion and speculation by ABA committees about the future of “cybernotaries,” virtual appearance in the context of notarial acts has now for the first time been authorized in the United States.

Because of state laws governing the interstate recognition of notarial acts and official seals, all states currently accept, for official recording purposes, notarial certificates completed by notarial officers from other states, despite the absence of federal legislation concerning interstate recognition of notarial acts. In addition, because notaries are “public officers,” a notarized document emanating from Virginia and based on virtual appearance should be recognized by other states under the Full Faith and Credit Clause of the United States Constitution without the need for extrinsic evidence to prove the genuineness of the notary’s identity and officer status.

However, some have suggested that other states might attempt either to ban or otherwise regulate Virginia online notarizations being performed with signers who are physically present in the regulating state. This may raise issues under a Dormant Commerce Clause analysis if such a ban on Virginia online notarizations were to be deemed discriminatory against commerce. It remains to be seen how this issue will play out.

Virtual Presence: The Changing Understanding of Personal Appearance in the Global Digital Network-Based Economy

The virtual aspect of digital data renders impractical, undesirable, and even obsolete requirements for physical appearance in many contexts. In fact, online notarization is just the latest example in a long line of societal trends that show the dominance of nonphysical digital or virtual networks. Significant removals of physical appearance have already occurred with telemedicine and long-distance education.

Further, fueling this trend is undoubtedly the pervasiveness of mobile Internet devices and audio-video conferencing capabilities. Recent announcements by Google+ and Facebook+Skype suggest the emergence of a new era in online communication via audio-video conference technology.

Indeed, it seems entirely possible that we will soon largely interact virtually for both personal and commercial reasons. If this prediction is accurate, then remote notarization may seem logical and even necessary. Virginia’s Electronic Notaries Act of 2011 is in the vanguard at the moment. In a few short years it may seem, in hindsight, an inevitability.

Endnotes


2. BLACK’S LAW DICTIONARY 1161 (9th ed. 2009).

3. 58 AM. JUR. 2D Notaries Public § 39 (2007) (“A certificate of a notary public, in due and legal form, makes an instrument admissible in evidence without further proof of its due execution, and the burden is upon the person challenging the truth of its contents to prove his contention by clear and convincing evidence. To impeach a notary’s certificate, the evidence must be clearly cogent and convincing beyond any reasonable controversy”).


5. See, e.g., VA. CODE ANN. § 19.2–3.1 (B). Note also that, 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.


10. Charles Faerber, Being There: The Importance of Physical Presence to the Notary, 31


12. For example, a digital signature can be used by a notary to render an electronic document tamper evident such that any subsequent unauthorized modification of the document will render the notary’s digital signature invalid. In Adobe Reader, this technology invalidates the digital signature visually with a red X, and other visual warning indicators can be displayed to indicate the document has been altered.


15. For example, a signer must undergo a series of challenge/response questions when asserting his identity online, and the use of independent third-party database checks to confirm identity markers (such as a social security number, a residence address, etc.) is used to cross-reference the signer’s identity assertion responses. This process also is subject to the guidelines set forth in the FBCA Supplementary Antecedent, In Person Definition (see fn. 13).

