A Position On Digital Signature Laws And Notarization

A Position Statement From The
NATIONAL NOTARY ASSOCIATION
A Nonprofit Educational Organization

Purpose of this Paper

There is an emerging crisis that has begun to weaken critical consumer protections against document fraud.

In this age of e-commerce, state efforts to implement digital signature legislation are abandoning one of the most beneficial and time-tested principles of law and commerce – that the signer of a valuable instrument must appear in person before, and be identified by, a trusted, impartial third party – a Notary Public.

While the National Notary Association has actively encouraged the development of new electronic technologies that might simplify transactions involving documents, the NNA has always held that the fundamental process of an acknowledgment – the notarial act most often used to authenticate documents of great sensitivity or value – must be the same for both paper and electronic instruments.

The cornerstone of the acknowledgment is the signer's personal appearance before the Notary Public, which enables the Notary not only to identify the signer but also to make observations about this person's willingness and basic awareness.[1]

Yet, recently enacted "electronic notarization" laws ignore the requirement of a signer's personal appearance before a trusted, impartial third party. This is potentially harmful not only to lenders and insurers, but even more so to consumers. Such harmful legislation has been driven by technology rather than by principle.

The following explains the role of the Notary Public in the arena of electronic notarization and identifies the dangers of letting technology rather than principle set public policy.

---

[1] Although often misunderstood by the lay public, an "acknowledgement" only speaks to the document signer's certification, upon proper proof of identity, that the signature is genuine and serves to adopt the document as the signer's act. *See*, Pardo v. Creamer, 310 S.W.2d 218 (Ark. 1958); and Favello v. Bank of Amer. Nat. Trust & Savings Ass'n, 75 P.2d 1057 (Cal. App. 1938). In acknowledging one's signature, the person makes no statement whatsoever concerning the truthfulness or accuracy of the contents of the document. *See*, Geelan v. St. Patrick's Church of West Neck, 39 N.Y.S.2d 263 (1943); and Bristol v. Buck, 194 N.Y.S. 53 (App. Civ. 1922). A jurat is a notarial certificate in which the signer swears to the truth of the contents of the document. *See*, Jemison v. Howell, 161 So. 806 (Ala. 1935). *Also, compare,* UNIF. LAW ON NOTARIAL ACTS §§1 and 4 (1983), *and see*, Kellner v. Christian, 539 N.W.2d 685, 689 (Wisc. 1995) where the Wisconsin Supreme Court clearly enunciated the difference between an acknowledgment and a jurat.

The Emerging Crisis

What has caused the growing threat to the states' consumer protections against document fraud?

In 1999, the National Conference of Commissioners on Uniform State Laws published the *Uniform Electronic Transactions Act.*[2] *UETA* permits notarial officers to use "electronic signatures" in executing acknowledgments, verifications and oaths.[3] The *Act* defines an electronic signature as "an electronic sound, symbol, or process, attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record."[4] Unfortunately, *UETA* does not elaborate on the Notary's role in electronic notarization, but it does suggest that the protections afforded by proper notarial procedures are to be maintained.[5]

Since its publication, over two dozen states[6] have either enacted or introduced the landmark *UETA*. In addition, the U.S. Congress in 2000 borrowed freely from *UETA* in passing its own electronic signature law, the *Electronic Signatures in Global and National Commerce Act,*[7] which authorizes electronic notarizations for transactions in or affecting interstate or foreign commerce.

Now, states are either introducing legislation or drafting rules and regulations that define electronic notarization. The problem is that in the interest of making it cheaper, faster and easier to conduct e-business, they are forgetting about security, safety and integrity. Some laws and regulations discard the requirement that a person appear before a Notary each time a document needs to be notarized, if the person uses a digital certificate. These laws and regulations allow persons owning a digital certificate issued by a licensed certification authority to use that certificate unilaterally in creating "notarized" digital signatures without limit and without the witnessing services of a Notary. Here are three examples:

---

[2] The *Uniform Electronic Transactions Act* was drafted by the National Conference of Commissioners on Uniform State Laws. It was approved and recommended for enactment in all states at the Conference's 108th annual meeting, held July 23-30, 1999, in Denver, Colorado. It can be found at "<http://www.law.upenn.edu/bll/ulc.frame.htm>.". *See*, *infra* n. 6 for a list of states that have adopted or are considering *UETA* in one form or another.

[3] ULA ELEC. TRANS. §11 (1999).

[4] ULA ELEC. TRANS. §2(8) (1999).

[5] The Official Comment to ULA ELEC. TRANS §11 makes clear that Notaries Public are expected to be the persons "authorized to perform" electronic acknowledgments. More importantly, the Comment states that "…the section does not eliminate any of the other requirements of notarial laws…" The accompanying examples in the Comment explicitly illustrate the point. There should be no mistaking the drafters' intent to make traditional paper notarial requirements a part of the electronic acknowledging process.

[6] As of August, 2000, 22 states had enacted the *Uniform Electronic Transactions Act* (*UETA*) or some variation thereof. *See*, ARIZ. REV. STAT. ANN. 41-132 (2000); CAL. CIV. CODE § 1633.1 (2000); DEL. CODE § 12A-101(2000); FLA. STAT. ANN. § 282.70 (2000); HAW. REV. STAT. § (Not Yet Codified) (2000); IDAHO CODE § 67-2354 (2000); IND. CODE § 26-2-8-101 (2000); IOWA CODE § 554C.201 (2000); KAN. STAT.ANN. § 60-2616 (2000); KY. REV. STAT. ANN. § 369.010 (West); MD. CODE ANN., STATE GOV'T § 8-504 (2000); ME. REV. STAT. ANN. § 3-14-1 (2000); MINN. STAT. ANN. § 325K.01 (2000); NEB. REV. STAT. § 86-1701 (2000); N.C. GEN. STAT. § 66-308 (2000); OHIO REV. CODE § 1306.01 (2000); OKLA. STAT. § 15-101 (2000); PA. STAT. § (Act. No. 69) (2000); R.I. GEN. LAWS § 42-131-1 (2000); S.D. CODIFIED LAWS § 53-12-16 (2000); UTAH CODE ANN. § 46-3- 102; and VA. CODE ANN. § 59.1-479 (2000). Legislation to enact *UETA* was introduced but not passed in a number of other jurisdictions, including Alabama, Arkansas, Colorado, District of Columbia, Michigan, New Jersey, Vermont and West Virginia. *See*, "*UETA*: *On the Fast Track,"* NOTARY BULLETIN, Aug. 2000, p. 5 (National Notary Association).

[7] 106 PUB. L. NO. 229; 114 STAT. 464.

Subdivision 1. Unless otherwise provided by law or contract, a certificate issued by a licensed certification authority satisfies the requirement for an acknowledgment... of a digital signature verified by reference to the public key listed in the certificate, regardless of whether words of an express acknowledgment appear with the digital signature and regardless of whether the signer physically appeared before the certification authority when the digital signature was created, if that signature is: (1) verifiable by that certificate; and (2) affixed when that certificate was valid.

Subdivision 2. If the digital certificate is used as an acknowledgement, then the certification authority is responsible to the same extent as a notary up to any limit on liability stated in the certification authority's certification practice statement for failure to satisfy the requirements for an acknowledgement. The certification authority may not disclaim or limit, other than as provided in section 325K.17, the effect of this section.

MINN. STAT. ANN. § 325K.23 (2000).

Except as otherwise provided by a specific statute, regulation or contract, a digital signature that is verifiable ... shall be deemed to satisfy the requirements for an acknowledgment, regardless of whether the person who executed the digital signature appeared before the certification authority or a person who is authorized to take acknowledgments…

NEV. ADMIN. CODE CH. 720 § 770 (2000).

(T)he (notary service) electronic signature certificate has the same legal force and effect as any notarial act made before a notary public...

ARIZ. REV. STAT. ANN., § 41-355(5) (2000).

Such laws legally equate the independent affixing of a digital signature – without a Notary present – to that of a Notary personally taking the acknowledgment of a signer. This is dangerous because technology is overtaking principle without regard for long-established requirements that were put in place for sound legal and commercial reasons.

To understand the danger of bypassing the Notary in favor of a new electronic procedure that lacks basic consumer protections, one must be familiar with the notarial act of acknowledgment.

Protections of the Acknowledgment

The acknowledgment is perhaps the most common and important of all notarizations performed in the United States. The acknowledgment is typically used to authenticate documents of great monetary value, particularly real property conveyances that are then filed in the public record as authentic.

There are five essential components of any reliable acknowledgment:

(1) Personal Appearance. The document signer must appear in person before – and communicate with – the Notary Public, face to face, in the same room. Physical presence[8] allows the

[8] Traditionally, this is a requirement imposed by statute. *See*, *e.g.,* N.J. REV. STAT. §14-2(1)(b) (2000), and MICH. COMP. LAWS §565.265 (2000). But the courts also agree. *See*, *for example,* Trowbridge v. Bisson, 44N.W.2d 810 (Neb. 1950); and Aultman & Taylor Co. v. Jenkins, 27 N.W. 117 (Neb. 1886). Taking the acknowledgment of a document in absence of the signer's presence could result in criminal sanctions for the Notary. *See*, S.D. CODIFIED LAWS §18-1- 11; and N.C. GEN. STAT. §10A-12(b).

Notary not only to identify the signer, but also to make observations and commonsense judgments that this individual appears willing and aware. The Notary is also thereby afforded an opportunity to make observations about the signer's demeanor that may prove helpful in settling any subsequent litigation about the document.[9] Personal appearance is the cornerstone of the acknowledgment, because the subsequent four guarantees of the Notary cannot reliably be made without the signer's physical presence.

(2) Identification. The Notary must positively identify the document signer beyond a reasonable doubt,[10] either through personal knowledge of the individual's identity, the sworn vouching of a personally known credible witness,[11] or reliable identification documents ("ID cards"). True identification cannot be based on the Notary's mere familiarity with a signature. The personal physical presence of the signer is critical to the Notary's assessment of identity.

(3) Acknowledgment by Signer. Personal appearance and identification are meaningless without a context, and it is the signer's active "acknowledgment" of a particular signature, document and transaction that provides the context. The signer's acknowledgment is threefold. First, there is the admission of ownership of a previously made signature, which can be a tacit act if the signature is made in the Notary's presence. Second, there is the signer's declaration of free intent to be held to the terms of the signed document. And, third, there is the person's stipulation of signing capacity, whether as individual, attorney in fact, corporate officer, partner, trustee or the like.

(4) Lack of Duress. Essential to the acknowledgment is the Notary's observation that the signer was not under direct physical threat or duress at the hands of a third party.[12]

(5) Awareness. Also essential to the acknowledgment is the Notary's observation and lay judgment that the signer appears to be awake and aware of the document signing.[13] Only a few states stipulate that ascertaining a signer's awareness is a statutory duty for the Notary,[14] however, only a reckless Notary would proceed with a notarization if there were any reasonable doubt about the signer's awareness of the transaction.

The above five vital guarantees and protections of the Notary Public would be eliminated in digital transactions under the new state laws that equate use of a digital certificate with acknowledgment before a Notary.

Digital Certificates Can Be Misused

The public danger in laws such as those passed in Minnesota, Nevada and Arizona lies in their authorization of the unlimited and unwitnessed use of a digital certificate.

---

[9] *See*, *for example,* Jordan v. Cousins, 37 S.E.2d 890 (W.Va. 1946) where the West Virginia Supreme Court recognized the admissibility of the Notary's testimony to help prove that a settlor of a trust had the requisite capacity to execute the document.

[10] Every jurisdiction, by statute, requires the Notary to properly identify the signer. However, the standards of proof for satisfying this requirement differ. *Compare, for example,* IDAHO CODE §51-111(1) (2000) with OHIO REV. CODE ANN. §147.53 (2000) and IOWA CODE §9E.9.6 (2000). In applying the statutes, the courts have ruled that a Notary is responsible for determining the signer's identity. *See*, *e.g.,* McWilliams v. Clem, 743 P.2d 577 (Mont. 1987); and In the Matter of New Concept Realty, 692 P.2d 355 (Idaho 1984).

[11] However, some statutes allow a Notary, in identifying an acknowledger, to rely on the sworn word of two disinterested credible witnesses who are strangers to the Notary but who can each present prescribed ID cards as proof of their identity. *See*, *e.g.,* CAL. CIV. CODE §1185(c) and FLA. STAT. ANN. §107.05(5) (2000).

[12] *See*., Coulter v. Coulter, 34 S.E.2d 330 (W.Va. 1945). *Accord,* In re McCauley's Adoption, 131 N.W.2d 174 (Neb. 1964).

[13] *See*, Poole v. Hyatt, 689 A.2d 82 (Md. 1997), where the court stated that assessing the signer's competence is implicit in performing an acknowledgment.

[14] *See*, *e.g.,* FLA. STAT. ANN. §17.107(5) (2000) which provides, "A notary public may not notarize a document if it appears that the person is mentally incapable of understanding the nature and effect of the document at the time of notarization."

Under the technology of Public Key Infrastructure (PKI),[15] a digital certificate is a combination of identity card and electronic pen. As with traditional ID documents like driver's licenses and passports, there is identity screening at the time of issuance, but, once the digital certificate is issued, it is up to the owner to prevent its misuse by others and to report its loss, theft or compromise. In contrast to traditional IDs, with a digital certificate, it is the password or other access procedure that must be safeguarded.

The digital certificate is a "fancy new kind of pen, but a pen nonetheless."[16] The digital certificate and a public or private key enable a signer to encrypt electronic documents and know if a document has been altered, but these features do not prevent a digital certificate from being used fraudulently to sign a document.

There are a number ways in which a digital certificate may be fraudulently used.

- The certificate may have been issued to an imposter.
- The certificate may be accessed and exploited by an unauthorized person. Many trusting spouses, for example, might readily share their access codes with their marital partners, just as they share their ATM numbers.
- The certificate's owner may be coerced into using the certificate to sign an electronic document against his or her desires.
- The certificate's owner may be intellectually vulnerable and manipulated into signing an electronic document against his or her interest. Senility and medication could play a part in rendering certain signers temporarily unaware of the ramifications of making a signature.

Considering the digital certificate's clear potential for misuse, why have legislators in some states now voted to forsake the public protections that are afforded by acknowledgment before a Notary?[17]

One possible answer was given by a Midwestern state lawmaker who said that he and fellow lawmakers were afraid not to pass digital technology legislation that many of them did not fully understand, lest they put their state at a competitive disadvantage and be personally accused of standing in the way of progress.

While a growing number of state legislators have mastered digital technology and sincerely believe in its public utility, some lawmakers have failed to grasp the important ramifications of the digital statutes they enact.

In our rush to adopt technology, we must not compromise the trust and integrity afforded by long-established principles and practices.

The NNA Position

In regard to electronic notarization, the National Notary Association's position is threefold:

(1) Fundamental Notary Principles and Process Do Not Change. The fundamental principles and process of notarization must remain the same regardless of the technology used to create a signature.

---

[15] For a definitive explanation of Public Key Infrastructure, *See* David L. Gripman, *Electronic Document Certification: A Primer on the Technology Behind Digital Signatures?,* 17 J. MARSHALL JOURNAL OF COMPUTER & INFORMATION LAW 769 (1999).

[16] From *Signing on the Dotted E-Line*, a presentation by Gordon W. Romney, Ph.D., President of Arcanvs, Inc., at the National Notary Association's 21st Annual Conference of Notaries Public, in Denver, Colorado, June 9-12, 1999. Arcanvs is a certification authority licensed in Utah.

[17] For an insightful discussion of the political considerations behind enactment of digital signature legislation, *see*, Thomas J. Smedinghoff & Ruth Hill Bro, *Moving With Change: Electronic Signature Legislation as a Vehicle for Advancing E-Commerce,* 17 J. MARSHALL JOURNAL OF COMPUTER & INFORMATION LAW 723 (1999).

As technology and its tools change, there can be no shortcutting on principle.

(2) Physical Presence before Notary Is Critical. For each electronic signing that is called – or equated to – "notarization," the signer must appear in person before a Notary Public to affix or acknowledge the signature. Just as it would be improper to allow the signer of a paper document to visit a Notary once and then to regard each signature subsequently affixed by this person on hundreds of other paper documents as "notarized," so it should be improper to let an applicant for a digital certificate visit a Notary a single time and then use a digital signature without limit on electronic instruments that are thereby regarded as notarized.

(3) Notary Office Must Be Strengthened. Because the complexity of digital signature technology heightens rather than diminishes the role of the Notary, the office of Notary must be strengthened through new mandatory training, testing and certification programs that stress both technical and ethical instruction. The NNA is hardly alone in the view that the emerging digital technology – still unfathomed and untrusted by so many – lends a new importance to the Notary office:

> At first blush it might seem that a notary's purpose, to note the identity of one who signs a document, is rendered moot in the digital age since computers and not people will be generating documents. But perhaps the greater complexity…of today's technological documents should demand a greater effort to identify the person at the keyboard who signs or acknowledges an electronic document. Instead of causing the death of notaries public, technology might instead increase their importance.[18]

Underlying all three components of the NNA's position is the bedrock principle that fraud deterrence depends on face-to-face interaction between signer and Notary. The fundamental tenet on which there can be no compromise is the mandatory physical presence of the document signer before the Notary at the time of the transaction. In 1955, a Texas court said, "A notary can no more perform by telephone those notarial acts which require a personal appearance than a dentist can pull a tooth by telephone."[19] Accordingly, any acknowledgment or other notarial act requiring a positive determination of a signer's identity, willingness and awareness cannot properly be executed without the signer's personal presence.

However, the NNA, does not foreclose on the possibility that future communications technology may allow interactive audiovisual linkups between Notary and signer that may prove to be a reliable alternative to "personal presence."[20]

The Electronic Notary

If electronic notarizations are authorized under the *Uniform Electronic Transactions Act* now being enacted into law in dozens of states, as well as under the new federal *Electronic Signatures in Global and National Commerce Act,* who exactly will perform these electronic notarial acts?

---

[18] Glen-Peter Ahlers, Sr., *The Impact of Technology on the Notary Process,* 31 J. MARSHALL L.REV. 911, 912 (1998).

[19] *See*, Charlton v. Richard Gill Co., 285 S.W.2d 801, 803 (Tex.App. 1955).

[20] *See*, UTAH CODE ANN. 46-1-2(1) which provides, "Acknowledgment means a notarial act in which a notary certifies that a signer, whose identity is personally known to the notary or proven on the basis of satisfactory evidence, has admitted, and which admission is made either in the presence of the notary or by an electronic communication that is as reliable as an admission made in the presence of the notary, provided that the electronic communication is authorized by law or rule, signing a document voluntarily for its stated purpose." However, Utah Notary Administrator Fran Fish has informed the NNA that the only electronic communication that would be regarded "as reliable as an admission made in the presence of the notary" would be an interactive audiovisual system so adaptable that it would allow the remote examination of a signer's ID cards by the Notary.

It will largely be Notaries specially commissioned for that purpose. In fact, the NNA has begun formulating parameters and qualifications for the office of Electronic Notary (EN) to be published in detail in a revised *Model Notary Act,* scheduled for publication in 2001.

In the NNA's deliberations so far on the office of Electronic Notary, certain debatable issues have emerged and certain desirable attributes of the EN office have become evident:

(1) Must Be Traditional Notary. The Electronic Notary must first qualify as a "traditional" paper-based Notary. Mastery of the principles and practices of notarization in relation to pen-and-ink signatures and paper documents provides a solid ethical and experiential base for operating with electronic signatures and documents. An Electronic Notary should have power to perform both traditional and electronic notarial acts.

(2) One Commission, One Term. For ease of administration by the state, one commission, with one corresponding term of office, should simultaneously grant both the traditional and the electronic powers of the Notary. After commissioning, however, the electronic powers could only be used upon presentation to the state of proof of successful completion of an approved course on electronic notarization. Currently, in a somewhat similar way, all Notaries in many states are given power to take depositions, but only those Notaries who have acquired training to attain shorthand reporting skills can actually use the powers.

(3) One Bond. One bond should cover both the traditional and electronic official acts of the Notary, because there is no reason to believe that electronic transactions would be of an intrinsically higher monetary value than transactions using traditional notarization.

(4) Higher Fees. While, ideally, consumers should not be penalized through higher fees for choosing either a paper or electronic instrument for their transactions, the inherent costs to the Notary of operating electronically (*i.e.,* training, hardware, software) may justify higher fees for electronic notarizations than for traditional notarial acts.

(5) Journal of Notarial Acts.[21] The Electronic Notary must keep either a bound, sequential, paper journal of notarial acts, or a sequential electronic journal, provided that in the case of an electronic journal: (a) safeguards are in place to prevent and reveal any unauthorized access and tampering with the electronic record; (b) a backup system is in place to prevent loss of the electronic record by theft, vandalism or natural disaster; (c) the electronic recording system has the capability of capturing a signature and thumbprint as they are made by a signer, in order to prove personal appearance before the Notary; and (d) any entry in the electronic journal may be printed out on paper and include the image of any related signature and thumbprint. So that there will be only one original, definitive, sequential record of notarial acts, the Electronic Notary may not maintain both a paper and an electronic record at the same time.

(6) Training, Testing, Certification. The *sine qua non* for the Electronic Notary will be training, testing and certification – not only on the technical complexities of electronic notarization but also on the ethical precepts that must guide every Notary.

---

[21] Notary journals are required in some states (*See*, *e.g.,* ALA. CODE § 36-20.7 (2000); CAL. GOV'T CODE § 8206 (2000); 57 PA. STAT § 161 (2000); and TEX. GOV'T CODE ANN. § 406.014 (2000) but no jurisdiction bars their use. Consequently, Notaries may maintain a journal even though it is not required by law. *The Notary Public Code of Professional Responsibility* (NNA 1998) strongly recommends that all Notaries maintain sequential notarial journals. (Id., Guiding Principle VIII.)

Summary and Conclusion

In the states, the allure of e-commerce and new technologies has begun to weaken vital statutory consumer protections against document fraud.

In authorizing use of electronic signatures by Notaries, the widely enacted *Uniform Electronic Transactions Act* has spawned implementing laws that ignore the critical role of the trusted impartial witness. Indeed, some states are labeling as "notarization" electronic acts that do not even require a digital signer to appear before a Notary.

The fundamental principles and process of notarization must remain the same regardless of the technology used to make a signature, because, while technology may be perfectible, the basic nature of the human beings who use it is not. Any process – paper-based or electronic – that is called notarization must involve the personal physical appearance of a signer before a commissioned Notary Public.

In the electronic arena, the role of the Notary Public as a trusted impartial witness must not only be retained but strengthened so that execution of contracts and property conveyances will not be compromised by a technology that, despite its complexity, cannot make trustworthy guarantees about a signer's identity, willingness and awareness. The Notary office must be strengthened through well-conceived training, testing and certification programs that stress ethical as well as technical instruction.

Numerous experts share the NNA's view that emerging digital technology heightens rather than diminishes the role of the Notary Public.

In today's society, the Internet permits a risk-free anonymity that has emboldened a new generation of forgers and criminal identity thieves. Identity theft complaints grew from fewer than 40,000 nationwide in 1992 to 750,000 in 1999.[22] "As identity becomes more digital, it becomes possible to reproduce and take on the identity of another (person) much more rapidly," said U.S. Treasury Secretary Laurence Summers.[23] In such an environment, there is more need than ever before for reliable human gatekeepers to prevent the exploitation of technology.

---

[22] Caitlin Liu, *Stealing a Person's Good Name a New Choice of Thieves,* LOS ANGELES TIMES, January 16, 2000.

[23] Elizabeth Crowley, *Citicorp Joins up with Secret Service to Fight E-Fraud,* WALL STREET JOURNAL, March 16, 2000.