UIC John Marshall Journal of Information Technology & Privacy Law

Volume 17
Issue 3 *Journal of Computer & Information Law - Spring 1999*

Article 7

Spring 1999

Potential Liability under the Illinois Electronic Commerce Security Act: Is It a Risk Worth Taking?, 17 J. Marshall J. Computer & Info. L. 909 (1999)

Stephen G. Myers

COMMENT

POTENTIAL LIABILITY UNDER THE ILLINOIS ELECTRONIC COMMERCE SECURITY ACT: IS IT A RISK WORTH TAKING?

I. INTRODUCTION

> It is true, that a written signature in script, maybe a safer mode of subscribing one's name, but where a party has adopted a signature made in any other mode, and had issued an instrument with such adopted signature, for value, he is estopped from denying its validity.
>
> Illinois Supreme Court (1864)[1]

The era of documenting transactions with the handwritten signature has changed forever. A new technology has arisen that will allow users to make binding agreements over the Internet. With this new technology, participants now have the ability to become more active in commerce and, thus, create a faster and more efficient market.[2] This

[1] Weston v. Myers, 33 Ill. 424, 432 (1864) (citations omitted); *see, e.g.,* Hillstrom v. Gosnay, 614 P.2d 466 (1989); Franklin v. County Coop. v. MFC Services, 441 So. 2d 1376 (Miss. 1983); Hideca Petroleum Corp. v. Tampimac Oil Int'l Ltd., 740 S.W.2d 838 (Tex. Ct. App. 1987); Watson v. Tom Growney Equip. Inc., 721 P.2d 1302 (N.M. 1986); Matter of Save On Carpet of Arizona, Inc., 545 F.2d 1239 (9th Cir. 1976). Modern cases have expanded their holdings to account for modern technology. For example, in *U.S. v. Miller,* 70 F.3d 1353, 1355 (D.C. Cir. 1995), the court held that unauthorized use of a PIN number to withdraw funds from an ATM machine was forgery because such un^uthorized use of the PIN number was "tantamount to cashing a check with a forged signature." Also, in *Spevak, Cameron & Boyd v. Nat'l Community Bank of New Jersey,* 677 A.2d 1168 (N.J. Super. Ct. App. Div. 1996), the court held that the use of an account number as an endorsement on a check constituted a signature. Thus, according to the court, "in this computer age the use of numbers as a means of identification has become pervasive. Indeed, numbers are more readily recognized and handled than signatures." *Id.*

[2] By fully implementing digital signatures into commerce, there are both costs and benefits. The costs consist of:

> Institutional overhead: The cost of establishing and utilizing certification authorities, repositories, and other important services, as well as assuring quality in the performance of their functions. Subscriber and Relying Party Costs: A digital signer will require software, and will probably have to pay a certification authority some price to issue a certificate. Hardware to secure the subscriber's private key

new technology is called digital signature, and its application is infinite.

The digital signature process, if implemented in the right manner, can replace present notarial procedures. In using present notarial procedures, a signer must appear before the notary and sign his or her signature in the physical presence of the notary. However, if a signer were to choose a digital signature as the security procedure, the signer could electronically transmit the information to a certification authority who would then electronically certify the electronic document. The certification authority would then forward the electronic document to the recipient, thus, eliminating the need for the physical appearance of the signer, unlike a notarization.

Digital signature technology also offers participants a higher level of security than current notarial procedures, since forgery of a digital signature is significantly more difficult than forgery of a traditional handwritten signature.[3] Furthermore, digital signature technology allows an electronic document to remain digital for its lifetime,[4] thereby decreasing the amount of paper and space needed to store the document.[5]

> may also be advisable. Persons relying on digital signatures will incur expenses for verification software and perhaps for access to certificates and certificate revocation lists (CRL) in a repository.

Digital Signature Guidelines, 1996 A.B.A. SEC. SCI. & TECH. 16 (citations omitted) [hereinafter *Digital Signature Guidelines*]. The benefits consist of:

> [T]he principal advantage to be gained is more reliable authentication of messages. Digital signatures, if properly implemented and utilized, offer promising solutions to the problems of Impostors, by minimizing the risk of dealing with impostors or persons who have attempted to escape responsibility by claiming to have been impersonated; Message integrity, by minimizing the risk of undetected message tampering and forgery, and of false claims that a message was altered after it was sent; Formal legal requirements, by strengthening the view that legal requirements of form, such as writing, signature, and an original document, are satisfied, since digital signatures are functionally on a par with, or superior to paper forms; and Open systems, by retaining a high degree of information security, even for information sent over open, insecure, but inexpensive and widely used channels.

Id.

[3] *See* Digital Signatures: Signing on the Digital Line (visited Sept. 4, 1998) <http://www.uwi.com>.

[4] *Id.*

[5] *Id.* However, long term paper storage *seems* safer than long-term computer based storage because of the nature of paper. For example, in *The Notary & EDI*, a paper presented before the work group on notarization and nonrepudiation of the A.B.A.'s Information Security Committee, author Charles N. Faerber discussed the nature of paper:

> [I]n contrast to modem electronic mechanisms, paper appears to be a flimsy, crude instrument for storing and transmitting information, but it has many advantages. Many of you know, for example, that there has been much talk of replacing court reporters with audio taping machines. This would certainly save a lot of money, but at what price? Have you ever tried to find a pertinent piece of spoken testimony on a lengthy tape? It is much easier to flip through pages of a document. Did you know that in time the tape will turn to the equivalent of peanut butter- but we will still have the paper on transcript? Paper is much underrated. In a plane

In response to digital signature technology, Illinois Attorney General Jim Ryan, in April 1996, established the Illinois Commission on Electronic Commerce and Crime [hereinafter Commission].[6] The Commission was charged with the task of drafting electronic and digital signature legislation for Illinois.[7] The Commission drafted legislation entitled the "Electronic Commerce Security Act" [hereinafter Act].[8] The

> crash or an earthquake, for example, every electronic device, every computer disk drive may be obliterated. But what usually survives undamaged? Paper.

Michael L. Closen & R. Jason Richards, *Notaries Public-Lost In Cyberspace, or Key Business Professionals of the Future?*, 15 J. MARSHALL J. COMPUTER & INFO. L. 703, 731 (1997).

[6] *See* COMMISSION ON ELECTRONIC COMMERCE AND CRIME, *Final Report of the Commission on Electronic Commerce and Crime*, H.B. 3180, 3 (Ill. 1998) (visited June 16, 1998) <http://www.mbc.comllegis/cece-fin.html>. The Attorney General of Illinois, Jim Ryan, established the Commission on Electronic Commerce and Crime in April of 1996 in order to analyze the issues surrounding electronic commerce in Illinois, and to develop legislation. *Id.* The Act was introduced into the House of Representatives on February 11, 1998 as House Bill 3180. *Id.* The Act was passed unanimously on March 30, 1998. *Id.* Next, the Act was introduced in the Senate. After making minor technical amendments, the Senate unanimously passed the Act on May 15, 1998. *Id.* The House unanimously concurred with the amendments on May 20, 1988. *Id.* The Governor signed the Act on August 14, 1998, and it becomes effective as of July 1, 1999. *See* Info. Tech. and Electronic Com. L. Dep't., McBride Baker & Coles, *Summary of Electronic Commerce and Digital Signatures Legislation*, 1 (visited Sept. 9, 1998) <http://www.mbc.com>.

[7] *See* COMMISSION ON ELECTRONIC COMMERCE AND CRIME, *supra* note 6, at 4. The legislation that the Commission was in charge of developing was geared toward the protection and promotion of the interests of Illinois businesses and citizens engaged in "online business, commercial, and personal activities." *Id.* The Commission tried to create laws that would:

> 1) remove existing legal barriers to electronic commerce,
> 2) ensure the legal authenticity and integrity of electronic documents during both communication and subsequent storage,
> 3) facilitate the creation of enforceable electronic contracts,
> 4) minimize the incidence of electronic forgeries and deceptive online practices and otherwise deter fraudulent and criminal activity online,
> 5) establish and promote a system for the reliable authentication and validation of electronic documents, and
> 6) facilitate the electronic creation, storage, and preservation of a variety of business records as well as state and public records, such as deeds, UCC financing statements, and court filings.

Id.

[8] COMMISSION ON ELECTRONIC COMMERCE AND CRIME, *supra* note 6, at 5. The Illinois Electronic Securities Act prepared by the Commission creates:

> [A] technology and industry- neutral legal infrastructure necessary to implement secure electronic commerce and record keeping practices for business and government agencies in Illinois. The Act accomplishes four unprecedented, substantive objectives related to online commerce. First, it defines electronic writings (records) and electronic signatures and establishes their legal legitimacy. Second, it creates a new category of "secure electronic records" and "secure electronic signatures" to establish the trust necessary to facilitate and promote electronic commerce. Third, it specifies the legal rules relating to a special type of electronic signature known as digital signature. Fourth, it authorizes all state agencies to conduct their business electronically.

Act was signed by the Governor on August 14, 1998, and goes into effect on July 1, 1999.[9] The Act is generally applicable to all communications,[10] but specifically addresses electronic signatures,[11] secure elec-

Id. The Act will "advance public and private sector commerce by providing a strong, but flexible, statutory infrastructure for all kinds of electronic exchanges without privileging a particular industry, business type, or technology." *Id.* The Act is divided into four parts:

> 1) Part I of the Act (Article 5) addresses electronic records and electronic signatures generally. It basically provides that they should be treated in much the same manner as paper records and paper signatures for purposes of complying with statutory writing and signature requirements, evidentiary requirements, and record keeping requirements. The purpose of this part of the Act is primarily to remove any existing barriers to electronic commerce that may exist.
>
> 2) Part II of the Act (Article 10) deals with the question of trust. It defines a subset of electronic records known as secure electronic records, and a subset of electronic signatures known as secure electronic signatures. Secure electronic record and secure electronic signatures define categories of records and signatures that are accorded heightened evidentiary presumptions because of their enhanced reliability and trustworthiness, just as notarized documents are accorded heightened evidentiary presumptions for the same reason. The concept of a secure electronic record and a secure electronic signature is critical to enabling electronic commerce. Businesses will be much more willing to enter into commercial transactions, extend credit, commit resources, ship goods, or otherwise rely on messages from contracting parties transmitted over public networks such as the Internet when they can be assured that such records and signatures will be accorded the heightened evidentiary presumptions necessary to effectively make their transactions nonrepudiable.
>
> 3) Part III of the Act (Articles 15 and 20) addresses digital signatures, a form of electronic signature, and specifies when a digital signature qualifies as a secure electronic record and a secure electronic signature, and defines the basic rules governing the creation and use of certificates and digital signatures, and the obligations of the respective parties involved. This includes the allocation of risk and liability between the certification authority, the subscriber, and any relying parties, and a determination of when it is appropriate to give rebuttable presumption of validity to a digitally signed message.
>
> 4) Finally, Part IV of the Act (Article 25) addresses the acceptance and use of electronic records and electronic signatures by state and other governmental agencies.

Id. at 8.

[9] *See* Info. Tech. and Electronic Com. L. Dep't., *supra* note 6, at 1.

[10] *See id.*

[11] *See* Illinois Electronic Commerce Security Act, H.B. 3 180, § 5-105 (effective July 1, 1999) <http://www.mbc.com/legis/cecc-fin.html>. Electronic signature as defined by the Act is "a signature in electronic form attached to or logically associated with an electronic record." *Id.* On a paper document it is assumed that a signature is "attached" or "located" somewhere on the paper that the signer intends to have validated. *Id.* at cmt. Furthermore, "since electronic records can be communicated separate from any tangible media on which they exist" the definition of electronic signature requires that the signature be "'attached to or logically associated with'" the electronic record being signed. *Id.* at cmt. The theory of attachment is similar to the approach taken by the Food and Drug Administration in its attempt to regulate electronic signatures as set forth at 21 C.F.R. section 11 (1997). *Id.* at cmt. In section 11.70 of the Food and Drug Administration regulations, it requires that the electronic signatures be "linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means . . . ." *Id.* at cmt. (citation omitted). However, an

tronic signatures,[12] and digital signatures.[13]

electronic signature as defined by the Act requires a linking, it does not require that the signature cannot be "excised, copied, or otherwise transferred." *Id.* at cmt.

[12] *See* Illinois Electronic Commerce Security Act § 10-110. A secure electronic signature is accomplished if:

> A) Through the use of a qualified security procedure, it can be verified that an electronic signature is the signature of a specific person, then such electronic signature shall be considered to be a secure electronic signature at the time of verification. If the relying party establishes that the qualified security procedure was:
> 1) commercially reasonable under the circumstances,
> 2) applied by the relying party in a trustworthy manner, and
> 3) reasonably and in good faith relied upon by the relying party.
>
> B) A qualified security procedure for purposes of this Section is a procedure for identifying a person that is:
> 1) previously agreed to by the parties, or 2) certified by the Secretary of State in accordance with Section 10-135 as being capable of creating, in a trustworthy manner, an electronic signature that:
> a) is unique to the signer within the context in which it is used;
> b) can be used to objectively identify the person signing the electronic record;
> c) was reliably created by such identified person, (e.g., because some aspect of the procedure involves the use of a signature device or other means or method that is under the sole control of such person), and that cannot be readily duplicated or compromised; and
> d) is created, and is linked to the electronic record to which it relates, in a manner such that if the record or the signature is intentionally or unintentionally changed after signing the electronic signature is invalidated.

Id.

[13] *See* Illinois Electronic Commerce Security Act § 5-105. The definition of a digital signature under the Act is:

> [A] type of an electronic signature created by transforming an electronic record using a message digest function, and encrypting the resulting transformation with an asymmetric cryptosystem using the signer's private key such that any person having the initial untransformed electronic record, the encrypted transformation, and the signer's corresponding public key can accurately determine whether the transformation was created using the private key that corresponds to the signer's public key; and whether the initial electronic record has been altered since the transaction was made.

Id. "In certain cases, as specified in sections 10-105 and 10-110, and 15-101, and 15-105, [of the Act] a digital signature may also qualify as a secure electronic signature, and a digitally signed electronic record may qualify as a secure record." *Id.* at cmt. 2. When a person digitally signs an electronic record, the computer program executes the following functions:

> 1) using the electronic record as the input data, the software executes a message digest function to translate the electronic record into a sequence of bits, referred to a message digest, which is, in effect, a number that is unique to the message, and is sometimes referred to as a "digital fingerprint" of the message;
> 2) using the message digest and the signer's private key as the input data, the software then executes a public key encryption algorithm that encrypts the message digest using the signer's private key to create the digital signature; and
> 3) the digital signature is then appended to the electronic record otherwise communicated or provided to the relying party.

Id. at cmt. 3. It is also important to know that a digital signature has no relationship to a person's handwritten signature. *Id.* at cmt. 4. "When printed, a digital signature is not normally readable, as it looks much like the following:"

Through the implementation of the Act, Illinois has assumed a national leadership role in this new area of law.[14] The Act will help promote "private and public sector commerce by providing a strong, but flexible, statutory infrastructure for all kinds of electronic exchanges without privileging a particular industry.[15] However, new legislation and new technology generally brings new legal problems, and such is the case with the Act.

This Comment argues that the potential liability of digital signatures under the Act is too great and, therefore, is not an effective mode of communication. Part II of this Comment explains the purpose, the significance, and the traditional role of the handwritten signature. Furthermore, Part II establishes the basics of the digital signature process[16] as it relates to each participant. The participants in a digital signature process consist of a subscriber,[17] a recipient,[18] and a certification author-

```
———— BEGIN SIGNATURE ————
owHtWXl-
sUlUUP=91G=22ysbHhDHcBeZaVmq7L9AuNJ2Uuh2soUSpaufVsftu8tby
IkUXTGsGhAgsE
———— END SIGNATURE ————
```

Id. at cmt. 4. Also, a digital signature, unlike a handwritten signature, will be different each time it is created. *Id.*

[14] *See* Commission on Electronic Commerce and Crime, *supra* note 6, at 5.

[15] *See id.*

[16] *Sée* Closen & Richards, *supra* note 5, at 742. The digital signature process consists of a subscriber, a recipient, and the certification authority. *Id.* A certification authority issues the keys that will verify the digital signatures. *Id.* The subscriber can then send its electronic documents securely through the use of the issued private key. *Id.* The recipient will then receive the electronic documents and, with the use of its public key, it can access the message. *Id.*

[17] *See* Illinois Electronic Commerce Security Act, H.B. 3180, § 5-105 (effective July 1, 1999) <http://www.mbc.comllegis/cecc-fin.html>. A subscriber under the Act is: "[A] person who is the subject named or otherwise identified in a certificate, who controls a private key that corresponds to the public key listed in the certificate, and who is the person to whom digitally signed messages verified by reference to such certificate are to be attributed." *Id.* "The concept of a 'subscriber' is tied to the certificate." *Id.* at cmt. 2. Thus:

> [T]he subscriber refers to a person named or otherwise identified in a certificate (sometimes the subscriber is referred to as the "subject" of a certificate). Thus, a person who digitally signs an electronic record, but who has not been issued a certificate, is not a subscriber, even though such a person is using a digital signature.

Id. at cmt. 2.

[18] *See Digital Signature Guidelines*, *supra* note 2, § 1.27. A recipient/relying party is defined as: "A person who has received a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them." *Id.* A relying party can mean a person "actually or potentially relying upon a particular certificate and/or a digital signature verifiable with reference to a public key listed in the certificate. *Id.* § 1.27.1. Thus:

> [T]he relying party relies upon the certificate to bind the public key to the identity of the subscriber. Therefore, if the digital signature is verified, reliance upon the

ity.[19] Part III of this Comment analyzes and argues why the use of digital signatures, under the Act, is too great of a liability for the participants to be considered an effective mode of communication. Next, Part III argues why potential digital signature participants, because of the overwhelming liability imposed by the Act, must continue to use the notarization process until the Act is properly amended. Finally, Part III proposes amendments to the Act as well as suggests defensive tactics for the subscriber. Part IV of this Comment concludes with the assertion that the Act creates too great of a liability for digital signature participants, and that digital signatures must not be used as a mode of creating binding agreements until the Act is properly amended.

II. BACKGROUND

> A person may be bound by any mark or designation he thinks proper to adopt, provided it be used as a substitute for his name.
>
> New York Court of Appeals (1844)[20]

A. The Handwritten Signature

A signature is not a part of the substance of a transaction, but is instead a representation.[21] The handwritten signature traditionally serves four purposes.[22] First, the signature acts as evidence.[23] A signature makes a writing authentic by identifying the signer to the signed

> certificate is anticipated to lead to reliance upon the digital signature as the digital signature of the subscriber identified in the certificate.

Id. § 1.27.2 (citation omitted).

[19] *See* Illinois Electronic Commerce Security Act § 5-105. A certification authority under the Act is defined as: "[A] person who authorizes and causes the issuance of a certificate." *Id.* A certification authority performs two functions:

> 1) It is responsible for identifying and authenticating the intended subscriber to be named in the certificate, and verifying that such subscriber possesses the private key that corresponds to the public key that will be listed in the certificate.
>
> 2) The certification authority is responsible for creating (i.e., manufacturing) and digitally signing the certificate. The certificate issued by the certification authority then represents that certification authority's statement as to the identity of the person named in the certificate and the binding of that person to a particular public-private key.

Id. at cmt. 2.

[20] Brown v. Butchers & Drovers' Bank, 6 Hill 443, 444 (N.Y. 1844); *see also* Joseph Denuzio Fruit Co. v. Crane, 79 F. Supp. 117, 128 n.16 (S.D. Cal. 1948), *aff'd*, 188 F.2d 569 (9th Cir.), *cert. denied*, 342 U.S. 820 (1951) (stating that a signature is whatever symbol, mark, or device one chooses to use as a representative of himself).

[21] *See Digital Signature Guidelines*, *supra* note 2, at 3.

[22] *See id.* at 4; *see also* Restatement (Second) of Contracts § 72 (1981). The Restatement notes that signed writings serve as a "deterrent" which seeks to "discourage transactions of doubtful utility." *Id.*

[23] *See Digital Signature Guidelines*, *supra* note 2, at 4.

document.[24] Thus, when the signer makes a mark in a distinctive manner the writing becomes attributable to the signer.[25] Second, the signature acts as a ceremonial device.[26] By signing the document, the signer becomes aware of the legal significance of the signer's act[27] and, thereby, helps prevent inconsiderate engagements.[28] Third, the signature is a sign of approval.[29] Law and custom has defined a signature as an expression of the signer's approval of the writing or the intent that the document have a legal effect.[30] Finally, the signature is an efficient tool.[31] Thus, a signature on a document performs the function of bringing finality to the transaction and lessens the subsequent need to inquire beyond the face of a document.[32]

[24] *Id.*

[25] *Id.* at 4 & n.4. Note 4 explains that the writing is attributable to the signer under RESTATEMENT (SECOND) OF CONTRACTS, statutory note preceding § 110 (1982) ("summarizing purpose of the statute of frauds, which includes a signature requirement"). *Id.* Note 4 also discusses, 6 JEREMY BENTHAM, THE WORKS OF JEREMY BENTHAM 508-85 (Bowring ed. 1962) (1839), in that "Bentham called forms serving evidentiary functions 'preappointed [i.e., made in advance] evidence.'" *Id.* "A handwritten signature creates probative evidence in part because of the chemical properties of ink that make it adhere to paper, and because handwriting style is quite unique to the signer." Joseph M. Perillo, *The Statute of Frauds in the Light of the Functions and Dysfunctions of Form*, 43 FORDHAM L. REV. 39, 64-69 (1974); *see also* U.C.C. § 1-201(39) (stating that "'[s]igned' includes any symbol executed or adopted by a party with present intention to authenticate a writing"). *Id.* at n4.

[26] *See Digital Signature Guidelines, supra* note 2, at 4.

[27] *Id.*

[28] *Id.* at 4 & n.5. Note 5 references "inconsiderate engagements" to 2 JOHN AUSTIN, LECTURES ON JURISPRUDENCE 939-44 (4th ed. 1873).

[29] *See id.* at 4.

[30] *See id.* at 4 & n.6. Note 6 expands the approval theory by stating that under the Model Law on Electronic Commerce, United Nations Commission On International Trade Law (UNCITRAL), 29th Sess., art. 7(l), at 3, U.N. Doc. A/CN. 9/XXX IX/ CRP.1/add.13 (1996), "[w]here a law requires a signature of a person, that requirement is met in relation to a data message if: (a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message." *Id.* at n.6. Note 6 also discusses the Draft Model Law on Legal Aspects of Electronic Data Interchange and Related Means of Data Communication, United Nations Commission on International Trade Law (UNCITRAL), 28th Sess., art. 6, at 44, U.N. Doc. A/CN.91406 (1994). For example, the signature on a contract customarily indicates the signer's assent. *Id.* at n.6. Comparatively, the signature on the back of a check is customarily taken as an endorsement. *See* U.C.C. § 3-204 (1990).

[31] *See Digital Signature Guidelines, supra* note 2, at 4.

[32] *See id.* at 4 & n.7. Note 7 discusses the comparison of a "form of a legal transaction to the minting of coin, which serves to make their metal content and weight apparent without further examination." *Id.* at n.7. Thus:

> The notion of clarity and finality provided by a form are largely predicated on the fact that the form provides good evidence. The basic premise of the efficiency and logistical function is that a signed, written document is such a good indicator of what the transaction is, that the transaction should be considered to be as the signed document says. The moment of signing the document thus becomes decisive.

The requirements for legal transactions have varied throughout time. Consequently, there has been a variance in the legal consequences of failure to cast the transaction in a required form.[33] Today, legal systems have begun to lower formal standards, or at least have minimized the consequences of failure to satisfy those standards.[34] Nevertheless, sound practice still calls for transactions to be formalized in a manner that assures validity and enforceability.[35] Thus, in today's practice, formalization normally involves documenting the transaction on paper and signing the paper to confirm the transaction.[36] However, this traditional method is beginning to undergo a fundamental change.[37]

The fundamental change[38] is driven by technology. Now, computers read and send information stored as bits, "rather than atoms of ink and paper,"[39] near the speed of light. The information may also be duplicated without limit and at a low cost.[40] Consequently, the law is slowly changing to adapt to this new technology.

However, new laws that regulate new technology may contain unforeseen inefficiencies, which must be corrected to better serve the new technology. Similarly, the Act possesses inefficiencies and it too must be amended to better serve the new technology.

B. The Digital Signature Process

In order to understand the legal liability of each participant in the digital signature process, one must first understand the process itself.[41] An individual has a right to adopt almost any mark as his or her identification symbol.[42] Therefore, a digital signature, when used to endorse an

Id.

[33] *See id.* at 5.

[34] *Id.* at 5 & n.10. Note 10 refers to Perillo, *supra* note 25, and discusses how, in "Anglo-American law, there are many examples of the trend away from formal requirements." *Id.* at n.10. "For example, the common law seal has little remaining significance." *Id.*; *see also* RESTATEMENT (SECOND) OF CONTRACTS, statutory note preceding § 95 (1982).

[35] *Digital Signature Guidelines*, *supra* note 2, at 5 & n.11 (stating that notarizing documents is also sound practice for ensuring validity).

[36] *See id.* at 5.

[37] *Digital Signature Guidelines*, *supra* note 2, at 5 (stating that providing change through technology is a given).

[38] *Id.* at 5.

[39] *Id.* at 6.

[40] *See id.*

[41] *See supra* note 16 (dealing with the digital signature process).

[42] *See* Joseph Denunzio Fruit Co. v. Crane, 79 F. Supp. 117, 128 n.16 (S.D. Cal. 1948), *aff'd*, 188 F.2d 569 (9th Cir.), *cert. denied*, 342 U.S. 820 (1951) (stating that a signature is whatever symbol, mark, or device one chooses to use as a representative of himself); Hessenthaler v. Farzin, 564 A.2d 990, 993 (Pa. Super. Ct. 1989) (holding that a signature need not be in any particular form); U.C.C. § 1-201(39) (1992) (stating that "[s]igned includes any symbol executed or adopted by a party with the present intention to authenticate a

electronic document, is the "functional equivalent or computer generated manifestation of a manual signature."[43]

1. *The Subscriber / Signer*

Using cryptography,[44] a subscriber affixes a digital signature to the electronic document through the use of electronic keys.[45] Two types of electronic keys are involved in the process.[46] The subscriber possesses the first key called the private key.[47] The document signer creates the private key.[48] The signer uses the private key to place his or her signature onto the document.[49] The signature itself is "actually a 'hash'— a string of digits (letters, numbers, and/or symbols) representing a combination of the document and the unique computer-generated code produced by the document's signer."[50] In processing the signature, the document's signer types "in a pass [-] phrase (much like a PIN number for a bank teller machine), and then [the] private key generates a long string of numbers and letters which represents the 'signature.'"[51] Consequently, since each computer-generated signature is unique to each document, each private key produces a different sequence of numbers[52]

writing"); *see also Marks Aren't X-traordinary*, NAT'L NOTARY MAG., Mar. 1997, at 22 (stating that "[b]y custom and law, a witness' mark is the same as a regular signature and may be notarized").

[43] Closen & Richards, *supra* note 5, at 735.

[44] *See* Michael D. Wims, *Law and the Electronic Highway, Are Computer Signatures Legal?*, 10 CRIM. JUST. 31 (1995). "Encryption" is a technique used to convert a message into a secret form. Edward J. Radlo, *Legal Issues in Cryptography*, 13 COMPUTER L.J. 1 (1996). Encryption is a term that relates to many different fields, including digital signatures, decryption, key certification, and authentication. *Id*

[45] Closen & Richards, *supra* note 5, at 735; *see also Digital Signature Guidelines*, *supra* note 2, at 8. Digital signatures use "public key cryptography." *Id.* This system "employs an algorithm using two different but mathematically related ' keys,' one for creating a digital signature or transforming data into a seemingly unintelligible form, and another key for verifying a digital signature or returning the message to its original form." *Id.*

[46] *See* Closen & Richards, *supra* note 5, at 735.

[47] *See id.*; *see also Digital Signature Guidelines*, *supra* note 2, at 8. "The complementary keys of an asymmetric cryptosystem for digital signatures are arbitrarily termed the private key, which is known only to the signer and used to create the digital signature, and the public key." *Id.*

[48] *See* Closen & Richards, *supra* note 5, at 735.

[49] *See id.*

[50] *See id.*; *see also Digital Signature Guidelines*, *supra* note 2, at 9. "The hash function is an algorithm which creates a digital representation or 'fingerprint' in the form of a 'hash value' or 'hash result' of a standard length which is usually much smaller than the message but nevertheless substantially unique to it." *Id.*; *see also* WARWICK FORD, COMPUTER COMMUNICATION SECURITY: PRINCIPLES, STANDARD PROTOCOL & TECHNIQUES 75-84 (1994).

[51] *See* Closen & Richards, *supra* note 5, at 736.

[52] *See id.*

and, therefore, a new signature is created for each document.

2. *The Recipient/Relying Party*

On the other end of the electronic transmission is the document's recipient.[53] The recipient holds the second key, which is known as the public key[54] by which he or she can decrypt the sender's document and signature through the use of a computer program.[55] The computer program matches the private key of the signer with the public key of the recipient to ensure that neither the document nor the signature has been altered prior to or during transmission.[56] This process is referred to as public key cryptography.[57] Therefore, "if a private key other than the one identified with the subscriber . . . [is] used to encrypt the document, or if the document [is] changed in any way between execution and verification, the hashes [will] differ from each other and the signature [will] fail verification."[58]

3. *The Certification Authority*

The responsibility of deciding whether the digital signature is authentic is the responsibility of an independent third party called the certification authority.[59] For example, during an electronic transmission, the sender encodes a signature on the computer using the private key,

[53] *See id.*

[54] *Id.*; *see also Digital Signature Guidelines*, *supra* note 2, at 8. The public key is used by the relying party "to verify the digital signature." *Id.* However:

> If many people need to verify the signer's digital signatures, the public key must be available or distributed to all of them, perhaps by publication in an on-line repository or directory where it is easily accessible. Although the keys of the pair are mathematically related, if the asymmetric cryptosystem has been designed and implemented securely it is "computationally infeasible" to derive the private key from knowledge of the public key. Thus, although many people may know the public key of a given signer and use it to verify that signer's signatures, they cannot discover that that signer's private key and use it to forge digital signatures. This is sometimes referred to as the principal of "irreversibility."

Id. at 8-9. "Computationally infeasible" is defined as a "[c]oncept based on the value of the data protected, the computing overhead required to protect it, the length of time it needs to be protected, and the cost and time required to attack the data, with such factors assessed both currently and in the light of future technological advance." *Id.* at n.23.

[55] *See* Closen & Richards, *supra* note 5, at 736.

[56] *See id.*

[57] *See id.*

[58] *Id.*; *see also* John B. Kennedy & Shoshana R. Davids, Bartleby the Cybertographer, *Legal Profession Prepares for Digital Signatures*, 215 N.Y. L. J. S4 (1996).

[59] *See* Closen & Richards, *supra* note 5, at 737 & n.205. "It is important to keep in mind that while most of the functions performed by certification authorities resemble those of notaries public, a certification authority does not need to be commissioned notary public to verify the authenticity of digital signatures." *Id.* at n.205.

and clicks on the sign document button.[60] By clicking on the sign document button, the digital signature is sent to a repository[61] that stores the coded signature.[62] The repository is the central storage area that warehouses electronic documents such as certification certificates of cybernotaries, lists of subscribers, and other information.[63] The certification authority then contacts the computer's repository to see if the private key as sent corresponds to the public key of the intended recipient on file in the repository.[64] If there is a match, the certification authority digitally signs the document and issues a computer-based certificate of authenticity, similar to the way that a notary would sign and seal a document to signify the validity of an original execution to a signature on paper.[65]

III. ANALYSIS

> People are the common denominator of progress. So . . . no improvement is possible with unimproved people, and advance is certain when people are liberated and educated.
>
> John Kenneth Galbraith (1958)[66]

This Comment analyzes and argues why the use of digital signatures, under the Act, creates too great of a liability for digital signature participants and, therefore, is not an effective mode of communication. Next, this Comment argues that digital signature participants, because of the overwhelming liability imposed by the Act, must continue to use

[60] *See* Closen & Richards, *supra* note 5, at 737. *See also* David P. Vandagriff, *Who's Been Reading Your E-mail? Two Easy-to-Use Tools Can Protect Privacy, Integrity of Documents*, 81 A.B.A. J. 98 (1995).

[61] *See* Closen & Richards, *supra* note 5, at 737; *see also Digital Signature Guidelines*, *supra* note 2, § 1.28. The definition of repository is "[a] trustworthy system for storing and retrieving certificates or other information relevant to certificates." *Id.* Also:

> The basic contents of a repository generally consist of certificates which have been published in that repository. A repository may also contain certification practice statements, as well as further information about certification authorities (particularly those certification authorities who publish information in the repository), notices of suspension or revocation, subscribers, information processing and electronic commerce standards, and similar materials.

Id. § 1.28. 1. Furthermore, "a repository will make its information available on-line." *Id.* § 1.28.2. Thus:

> [A] repository's information may be made available to a broad, generally defined group of users or to a limited group, and its availability may be subject to conditions such as payment of fees, reasonable and regular hours of operation, security measures such as identification of persons or systems having access, etc.

Id.

[62] *See* Closen & Richards, *supra* note 5, at 737.

[63] *See id.*

[64] *Id.*

[65] *Id.*

[66] JOHN BARLETT, FAMILIAR QUOTATIONS 358 (15th ed. 1980).

the notarization process until the Act is properly amended. Finally, this Comment proposes amendments to the Act as well as suggests defensive tactics for the subscriber.

A. The Legal Liability of the Subscriber—A Certain Death

When a subscriber is ready to send an electronic document using digital signature technology,[67] as governed under the Act, he or she simply clicks on the signature button[68] located on the computer screen and the digital signature process begins.[69] However, if the subscriber under-

[67] *See* Illinois Electronic Commerce Security Act, H.B. 3180, § 5-105 cmt. 2 (effective July 1, 1999) <http://www.mbc.comllegis/cecc-fin.html>. Digital signature technology involves an asymmetric algorithm which uses two mathematically related keys for encrypting and decrypting information. *Id*

> [T]he keys that compromise a key pair are simply numbers—typically very large prime numbers. The algorithm is designed so that one key pair is used for signing (i.e. encryption) and the other key is used for signature verification (i.e., decryption). Each pair possesses a variety of fundamental characteristics including the following: one key can sign a message, but the other key must then be used to verify the message; and knowledge of one key does not facilitate calculation of the other corresponding key.

Id. A digital signature that is created using an asymmetric algorithm certified by the Secretary of State shall be considered to be a qualified security procedure for the purpose of identifying a person if:

> (1) the digital signature was created during the operational period of a valid certificate, was used within the scope of any other restrictions specified or incorporated by reference in the certificate, if any, and can be verified by reference to the public key listed in the certificate; and
>
> (2) the certificate is considered trustworthy (i.e., an accurate binding of a public key to a person's identity) because the certificate was issued by a certification authority in accordance with standards, procedures, and other requirements specified by the Secretary of State, or the trier of fact independently finds that the certificate was issued in a trustworthy manner by a certification authority that properly authenticated the subscriber and the subscriber's public key, or otherwise finds that the material information set forth in the certificate is true.

Id. § 15-105.

[68] *See* Closen & Richards, *supra* note 5, at 737. In a common electronic transaction, the subscriber codes the signature on the computer using the private key. *Id.* The subscriber will then click on the "sign document" button. *Id.* By doing so, the digital signature is sent to a repository. *Id.* The certification authority contacts the repository and verifies whether the private key, as sent, matches the public key of the intended recipient. *Id.* If it does, the certification authority digitally signs the document and issues a certificate of authenticity. *Id.*

[69] *See* Illinois Electronic Commerce Security Act § 5-105 cmt. 2. However, for policy reasons, there are three categories of documents where electronic signatures should not be applied:

> (1) [when] application would involve a construction of a rule of law that is clearly inconsistent with the intent of the law-making body or repugnant to the context of the same rule of law;
>
> (2) to any rule of law governing the creation or execution of a will or trust, living will, or healthcare power of attorney;
>
> (3) to any record that serves as a unique and transferable instrument of rights and obligation including, without limitation, negotiable instruments and other instru-

stood the liability of sending such a document, as entailed under the Act,[70] the subscriber would not use the digital signature process. Instead, the subscriber must use the method of notarization[71] until the Act is properly amended.

1. *The Liability Attached to the Signature Device*

Under the Act, a subscriber and all other persons[72] who can digitally sign a document must exercise reasonable care[73] in maintaining the secrecy of the private key. The private key acts as the signature device.[74] In maintaining the secrecy of the private key through the standard of reasonable care, the subscriber will not only need to prevent unauthorized access, but the subscriber must prevent disclosure of the private key during the period[75] in which a recipient would reasonably rely on a sig-

> ments of title wherein possession of the instrument is deemed to confer title, unless an electronic version of such record is created, stored, and transferred in a manner that allows for the existence of only one unique, identifiable, and unalterable original with the functional attributes of an equivalent physical instrument, that can be possessed by only one person, and which cannot be copied except in a form that is readily identifiable as a copy.

Id. § 5-120(c); *see also* § 5-120 cmt. 5.

[70] Illinois Electronic Commerce Security Act § 10-130. A subscriber is required to prove by a preponderance of the evidence that the signature was neither his nor authorized by him. *Id.* The subscriber has been issued the risk of loss since the electronic document was sent with his signature attached, and if the relying party reasonably relies on the message, the subscriber will be bound. *Id.*

[71] *See* The Nat'l Notary Ass'n, the Model Notary Act § 3-101 (1984). The purpose of the Act is to: "(1) promote, serve, and protect the public interest; (2) to simplify, clarify, and modernize the law governing notaries; and (3) to make uniform notarial laws among states enacting it." *Id.* § 1-102(6-10).

[72] *See* Illinois Electronic Commerce Security Act, H.B. 3180, § 5-105 (effective July 1, 1999) <http://www.mbc.com/legis/cecc-fin.html>. Person(s) under the Act is defined as "an individual, corporation, business trust, estate, trust, partnership, limited partnership, limited liability partnership, limited liability company, association, joint venture, government, governmental subdivision, agency, or instrumentality, or any other legal or commercial entity." *Id.*

[73] Barron's Law Dictionary 396 (3d ed. 1991). "Reasonable care" is defined as "'that degree of care which under the circumstances would ordinarily or usually be exercised by or might be reasonably expected from an ordinary prudent person.'" *Id.*

[74] *See* Illinois Electronic Commerce Security Act § 5-105. Signature device as defined by the Act means "unique information, such as codes, algorithms, letters, numbers, private keys, or personal identification numbers (PINs), or a uniquely configured physical device, that is required, alone or in conjunction with other information or devices, in order to create an electronic signature attributable to a specific person" *Id.* The definition realizes that a signature device which is needed for the creation of an electronic signature can be two different things. *Id.* at cmt. First, it can be a physical device such as a smart card. *Id.* at cmt. Second, the signature device can be information such as a PIN number or a private key or a secret code. *Id.* at cmt.

[75] *See* Illinois Electronic Commerce Security Act § 5-105. As mentioned in this comment, "period" refers to the certification authority's issued certificate which is only good for

nature created by the subscriber.[76]

However, the subscriber's standard of care is so low that it hurts rather than helps the subscriber because the subscriber, in attempting to prevent unauthorized access to the private key, will only take a reasonable standard of care approach. Thus, the subscriber, because it knows that the standard of care is only a reasonable one, will not be as careful

a certain period of time. The period of the certificate is operational as defined by the Act at the:

> [D]ate and the time the certificate is issued by the certification authority (or on a later date and time certain if stated in the certificate) and ends on the date and time it expires as noted in the certificate or is earlier revoked, but does not include any period which a certificate is superseded.

Id. During this period, the certification authority is obligated to maintain records and publish any notice of revocation. *Id.* Furthermore, the certification authority is obligated to exercise due care in protecting the private key from all other persons. *Id.* "Certificate," as defined by the Act, is a record that at a minimum:

> (a) identifies the certification authority issuing it; (b) names or otherwise identifies its subscriber, or a device or electronic agent under the control of the subscriber; (c) contains a public key that corresponds to a private key under the control of the subscriber; (d) specifies its operational period; and (e) is digitally signed by the certification authority issuing it.

Id.

[76] *See* Illinois Electronic Commerce Security Act § 15-320. A certification authority must revoke a certificate based on the policies governing revocation as specified in the certification practice statement. *Id.* A "certification practice statement," as defined by the Act, is "a statement published by a certification authority that specifies the policies or practices that the certification authority employs in issuing, managing, suspending, and revoking certificates and providing access to them." *Id.* § 5-105. However, in the absence of such a policy or procedure, a certificate must be revoked as soon as possible after:

> (1) receiving a request for revocation by the subscriber named in the certificate, and confirming that the person requesting revocation is the subscriber, or is an agent of the subscriber with authority to request the revocation;
> (2) receiving a certified copy of an individual subscriber's death certificate, or upon confirming by other reliable evidence that the subscriber is dead;
> (3) being presented with documents effecting a dissolution of a corporate subscriber, or confirmation by other evidence that the subscriber has been dissolved or has ceased to exist;
> (4) being served with an order requiring revocation that was issued by a court of competent jurisdiction; or
> (5) confirming by the certification authority that;
> a material prerequisite to issuance of the certificate was not satisfied,
> the certification authority's private key or systems operations were compromised in a manner materially affecting the certificate's reliability, or the subscriber's private key was compromised.

Id. Furthermore, the Act also states that, upon revocation, the certification authority must:

> [N]otify the subscriber and relying parties in accordance with the policies and procedures governing notice of revocation specified in its applicable certification practice statement, or in the absence of such policies and procedures, promptly notify the subscriber, promptly publish notice of the revocation in all repositories where the certification authority previously caused publication of the certificate, and otherwise disclose the fact of revocation on inquiry by a relying party.

Id.

in protecting the private key than if the standard of care were absolute. Therefore, under the reasonable standard of care approach, potential liability is greater because of the risk of more unauthorized access and more security breeches stemming from the low standard of care.

Moreover, if the standard were changed to absolute liability, the subscriber would be more careful in protecting the private key because of the liability that would be imposed on the subscriber. Therefore, an absolute liability standard will force the subscriber to take preventative measures to protect the private key, thereby defeating the potential liability that a reasonable standard of care creates. Thus, the subscriber will expose himself to less potential liability with an absolute standard of care, as compared to a reasonable standard of care, which will expose the subscriber to numerous chances of potential liability.

2. *A Subscriber's Private Key v. A Signature Device for Check Signing*

The obligation of the subscriber to exercise reasonable care can be compared to the duty of a person who must exercise reasonable care in regard to devices used to sign a name to a check.[77] For example, an employer keeps a rubber signature stamp along with blank checks in an unlocked desk drawer. An unauthorized person takes the checks and forges the signature of the employer through the use of the rubber stamp. The bank honors the checks in good faith.[78] Who is liable? In Illinois, a person who fails to exercise reasonable care in retaining control of his or her signature device is held liable.[79] Thus, the employer pays for his or her lack of security in guarding the signature device.[80]

[77] *See* Illinois Electronic Commerce Security Act § 10-125. Check signing cases are governed by Section 3-406 of the Uniform Commercial Code which is codified in Illinois at 810 ILL. COMP. STAT. 5/3-406. Section 32-406(a) provides that:

> [A] person whose failure to exercise ordinary care substantially contributes to an alteration of an instrument or to the making of a forged signature on an instrument is precluded from asserting the alteration or the forgery against a person who, in good faith, pays the instrument or takes it for value for collection.

Id. at cmt. 3. Therefore, one must maintain safeguards so that the signature device is not used for fraudulent use. *Id.* at cmt 3. A failure to do so, if the failure is the cause of the forgery, will thus, preclude one from asserting the forgery against the drawee bank. *Id.* at cmt 3. "The burden of proving failure to exercise ordinary care is on the person asserting the preclusion." *Id.*

[78] *See* Illinois Electronic Commerce Security Act, H.B. 3180, § 10-125 cmt. 3 (effective July 1, 1999) <http://www.mbc-com/legis/cecc-fin.html>. This hypothetical is taken from comment three under section 10-125 of the Act. Under the hypothetical, the drawee bank may defend that the employer cannot assert forgery against the bank because of its own negligence. *Id.* The drawee bank would contend that because the employer failed to exercise ordinary care to safeguard the signature device and the checks, its failure to do so contributed to the forgery. *Id.*

[79] *See id.*

[80] *See id.*

Similarly, a subscriber under the Act is held to the same accountability regarding the safekeeping of the signature device.[81] A subscriber is held liable for the subscriber's signature, whether or not it is authorized, if the subscriber failed to exercise reasonable care and the relying party reasonably and in good faith relied on the signature.[82] Therefore, because the standard of care was a reasonable one in the above illustration, the employer exposed himself to potential liability by leaving the checks and signature device unprotected. Thus, the potential liability was high. However, if the standard of absolute liability was used, the employer would have locked up both the checks and the signature device for fear of the potential liability that would stem from an unauthorized use. Absolute liability, thus, creates less potential liability situations, thereby reducing overall liability. Therefore, until the Act amends the standard of care for a subscriber's signature device to absolute liability, a subscriber will continue to expose himself to more chances of potential liability.

3. *Allocation of Risk*

The above example is a classic scenario in American law.[83] The allocation of risk is given to the party who can best control it.[84] Thus, the subscriber is held liable if the subscriber fails to exercise reasonable care. A similar example of such liability occurs when a subscriber has incurred charges through the unauthorized use of his or her password in

[81] *See id.* at cmt. 1.

[82] *See* Illinois Electronic Commerce Security Act § 10-130. The Act states:

> Except as provided by another applicable rule of law, a secure electronic signature is attributable to the person to whom it correlates, whether or not authorized, if:
> (1) the electronic signature resulted from acts of a person that obtained the signature device or other information necessary to create the signature from a source under the control of the alleged signer, creating the appearance that it came from that party;
> (2) the access or use occurred under circumstances constituting a failure to exercise reasonable care by the alleged signer; and
> (3) the relying party relied reasonably and in good faith to its detriment on the apparent source of the electronic record.

Id. Under section (b) of section 10-130 it further notes that:

> (b) The provisions of this Section (10-130) shall not apply to transactions intended primarily for personal, family, or house hold use, or otherwise defined as consumer transactions by applicable law, including but not limited to, credit card and automated teller machine transactions, except to the extent allowed by applicable consumer law.

Id.

[83] *See* Illinois Electronic Commerce Security Act § 10-130 cmt. 2. The system of law in America has always asked the basic question of which of the "two largely innocent parties must bear the loss occasioned by the misconduct of a third person who cannot be located or who was not in position to make good the loss." *Id.*

[84] *See* Illinois Electronic Commerce Security Act, H.B. 3180, § 10-130 cmt. 2 (effective July 1, 1999) <http://www.mbc.com/legis/cecc-fin.html>.

an on-line service.[85] The end result is the same. The subscriber is liable to the on-line service provider for charges incurred.[86]

Another example of a device, which can cause liability to a subscriber through unauthorized use, is when unauthorized calls are made using a subscriber's equipment.[87] The subscriber again is held liable regardless of who used the equipment.[88] Therefore, unauthorized use translates into liability for a subscriber who fails to exercise reasonable care.[89] However, in the above illustrations, if the subscriber would have been held to the standard of absolute liability for the device, the subscriber would have secured the devise for fear of the potential liability. Therefore, absolute liability can actually reduce potential liability, rather than increase liability, as the standard of reasonable care will do.

4. *The Hardship of Dealing with Real-Time*

When engaging in digital signature transactions, one is dealing with real-time.[90] A recipient will immediately react to the transmission and will possibly induce reliance with other parties based on the transmission.[91] Therefore, the Act gives the recipient rebuttable presumptions with respect to secure records and signatures, thereby giving the recipient the confidence to participate in real-time transactions which can be enforced in court.[92]

However, if a subscriber claims that the signature is false, the subscriber must prove his or her claim.[93] A subscriber will have a difficult

[85] *See id.*

[86] *See id.*

[87] *See id.*

[88] *See id.* (providing security to prevent such unauthorized use can be as easy as downloading security based software).

[89] *See* Illinois Electronic Commerce Security Act, H.B. 3180, § 10-130 cmt. 2 (effective July 1, 1999) <http://www.mbe.com/legis/cecc-fin.html>. The rule in the Act at section 10-130 is consistent with the U.C.C. section 3-406(c) (codified in Illinois at 810 ILL. COMP. STAT. 5/3-406(c)) in that the holder of a signature device is required to exercise reasonable care. *Id.*

[90] *See* Illinois Electronic Commerce Security Act § 10-120 cmt. 1 (defining "real-time" as a computer expression that means that the actions that are taking place are immediate).

[91] *See id.*

[92] *See id.* For a digital signature to be effective, the relying party of an electronic transmission must be in a position to know, at the time the message is received, whether the relying party can rely on the message or not. *Id.* More importantly, a relying party must be able to enforce the message in court. *Id.* Thus, the "existence of rebuttable presumptions with respect to secure records and secure signatures will provide such assurances to relying parties thereby enabling them to engage in real time commercial activities with confidence." *Id.*

[93] *See id.* at cmt. 5. The subscriber must prove by a preponderance of the evidence that the signature was not his. *Id.* In making the presumption justified, the Act establishes that the subscriber, rather than the relying party, is in a better position to prove who

time proving the claim, since a digital signature is made up of bits (0s and 1s) that are, in all respects, identical.[94] For example, the subscriber's signature may look like the following:[95]

——— BEGIN SIGNATURE ———
owHtWXlsUlUUP=91G=22ysbHhDHcBeZaVmq7L9AuNJ2UuhX2soU
SpaufVsftu8tbylkUXTGsGhAgsE
——— END SIGNATURE ———

Alternatively, a signature in a notarization may look like this: *Milton I. Myers*. At least in the notarization process, the handwritten signature can be examined by an expert to determine whether or not the signature belongs to the signer. When using a digital signature, there are no personal identifiers associated with the digital signature. There are only numbers and symbols, which cannot be traced to the specific person who signed the electronic document.[96] All that can be traced is the signature device that came from the computer of a registered subscriber. Thus, notarization, because of the identification standards, is more reliable in regard to identifying whether the signer is actually who he or she claims to be. The participant, therefore, must not use digital signatures technology as regulated by the Act until either absolute liability is invoked for the subscriber or biometric technology[97] is used.

actually sent the message. *Id.* For example, a subscriber is in a better position than the relying party in establishing that the private key was stolen or copied. *Id.* A relying party will not be privy to such information and, thus, have no evidence other than the security procedure used to "prove that the person to whom the signature correlates did, in fact, send the message." *Id.* Nevertheless, even if under section 10-130, the subscriber to whom the signature correlates can prove that he did not send the message, he may be liable for losses caused to the relying party if the requirements of section 10-130 of the Act are met. *Id.*; *see also supra* note 89 (describing the requirements of section 10-130).

[94] *See* Illinois Electronic Commerce Security Act § 10-120 cmt. 1. Paper-based transactions have many indicators that a relying party can use to determine whether the document and the signature is authentic. *Id.* For example, paper transactions can have watermarks or other forms of identification on the paper to prove that the document originated from the signer. *Id.* The document can also be delivered through a trusted third party, such as the postal service. *Id.* Most importantly, the handwritten signature can be examined by an expert to see if it derived from a particular signer. *Id.* However, these elements which accompany paper transaction do not exist in electronic transactions. *Id.* "All that can be communicated are bits (0s and 1s) that are in all respects identical, and that are easily copied and modified." *Id.*

[95] Illinois Electronic Commerce Security Act, H.B. 3180, § 5-105 (effective July 1, 1999) <http://www.mbe.com/legis/cecc-fin.html>.

[96] *See* Illinois Electronic Commerce Security Act § 10-120 cmt. 1.

[97] *See infra* note 143 (stating that instilling such a security feature can be costly).

B. The Legal Liability of the Recipient-Death in the Waiting

1. *The Legal Liability of the Recipient*

The general theme regarding liability is that the relying party is responsible for information and events that are under the relying party's control.[98] The Act seeks to balance the risk of loss between the subscriber and the recipient of an electronic message on the basis of information, and the procedures that the recipient relies on to verify a message.[99] Thus, the relying party has an immense amount of responsibility if the procedure goes awry. If a problem does arise, the relying party, under the Act, has three burdens to prove.[100] These burdens consist of: (1) proving that the use of the security procedure was commercially reasonable under the circumstances;[101] (2) proving that the security procedure was implemented by the relying party in a trustwor-

[98] *See* Illinois Electronic Commerce Security Act § 10-105 cmt. 2. The relying party has the burden of proof with respect to evidence or information that it has under its own control. *Id.* at cmt. 1. Evidence and information that would be under its control consist of whether the relying party reasonably and in good faith relied upon the electronic message. *Id.* If the relying party had knowledge that the security procedure was not reliable, it should be held accountable for that knowledge and, therefore, it should not have relied on the security procedure. *Id.*

[99] *See id.*

[100] *See* Illinois Electronic Commerce Security Act § 10-105. If, in its use of a qualified security procedure, a relying party can verify that an electronic record has not been altered from a specific point in time, then the electronic record can be considered to be secure from that point, if the relying party can establish that the procedure was: "(1) commercially reasonable under the circumstances, (2) applied by the relying party in a trustworthy manner, and (3) reasonably and in good faith relied upon by the relying party." *Id.* § 10-105(a). A qualified security procedure under the Act is "a security procedure to detect changes in the content of an electronic record." *Id.* The security procedure can be "(1) previously agreed to by the parties, or (2) certified by the Secretary of State in accordance with Section 10-135 as being capable of providing reliable evidence that an electronic record has not been altered." *Id.*; *see also* 810 Ill. Comp. Stat. Ann. 5/4A-201, 202; U.C.C. Article 4A §§ 201, 202.

The first category allows parties to agree among themselves on a security procedure "they believe to be appropriate for their purposes." *Id.* at cmt. 4. The second category is directed to parties "that have not agreed on a security procedure prior to their communication." *Id.* The second category recognizes that security procedures are "sufficiently secure such that they are entitled to the benefit of enhanced evidentiary presumptions even in the absence of an agreement between the parties to the communication." *Id.* Therefore, the Secretary of State reviews such technology and makes a determination as to "whether such technology is generally accepted as capable of adequately establishing the integrity of an electronic record, and if so, to exercise its rule making authority pursuant to Section 10-135 to certify such technology as appropriate as a qualified security procedure." *Id.*

[101] *See* Illinois Electronic Commerce Security Act, H.B. 3180, § 10-105(a)(1) (effective July 1, 1999) <http://www.mbe.com/legis/cecc-fin.html>. Commercial reasonableness, as defined by the Act, is "a relative term that depends not only on the nature of the security procedure itself, but its implementation in specific situations. It is determined by the court in light of the purposes of the procedure and the commercial circumstances at the time the

thy manner;[102] and (3) proving that the security procedure was implemented and relied upon by the relying party reasonably and in good faith.[103]

procedure was used." *Id.* at cmt. 5(a). Factors relevant in determining commercial reasonableness include:

> [T]he nature of the transaction, the sophistication of the parties, the volume of similar transactions engaged in by either or both of the parties, the availability of alternatives offered to but rejected by either of the parties, the cost of alternative security procedures, and security procedures in general use for similar types of transaction.

Id. The purpose of having commercial reasonableness allows "a court to take into consideration new developments in technology relating to the security procedure that may have an adverse impact on the trustworthiness or viability of the security procedure." *Id.*

[102] *See* Illinois Electronic Commerce Security Act § 10-105(a)(2). "Trustworthy manner" as defined by the Act means:

> through the use of computer hardware, software, and procedures that, in the context in which they are used, they
> (a) can be shown to be reasonably resistant to penetration, compromise, and misuse;
> (b) provide a reasonable level of reliability and correct operation;
> (c) are reasonably suited to performing their intended functions or serving their intended purposes;
> (d) comply with applicable agreements between parties, if any; [and]
> (e) adhere to generally accepted security procedures.

Id. § 5-105. The term "trustworthy manner" is intended to be flexible. *Id.* It concentrates "on the context at hand and focuses on what is 'reasonable' within that context. Consequently, specified computer hardware, software, and/or procedures may be considered trustworthy and appropriate in one situation, but not in another." *Id.* at cmt. 1. The definition of "trustworthy manner" also concentrates on a variety of trustworthiness. *Id.* at cmt. 3. Examples of "trustworthy manner" include:

> (1) security from intrusion and misuse;
> (2) reliability and correct operation;
> (3) suitability to performing intended functions or purposes;
> (4) compliance with applicable agreements of the parties; and
> (5) adherence to generally accepted security procedures.

Id. Being implemented in a trustworthy manner "is a recognition that no matter how good the procedure is, if not implemented properly[,] it will not achieve the desired goal." *Id.* § 10-105 at cmt. 5(b). Digital signatures are generally considered "to be an appropriate security procedure for purposes of achieving secure status, this goal is achieved only if the software that creates and interprets the digital signature works properly and is accurate. *Id.*

[103] *See* Illinois Electronic Commerce Security Act § 10-105(a)(3). In determining whether the requirement of whether a relying party's reliance on the security procedure is reasonable and in good faith is met, all of the surrounding circumstances must be examined. *Id.* at cmt. 5(c). Factors that are considered in determining whether the relying party acted in good faith consist of:

> [I]nformation that the relying party knew or should have known at the time of the reliance that would suggest whether reliance was or was not reasonable; the value or importance of the electronic record involved; any course of dealing between the parties; any usage of trade; and whether an independent third party was involved in the process.

Id. In focusing on time of verification, as discussed in section 10-105(a) of the Act, "the fact that an electronic record is verified by a security procedure and qualified as a secure elec-

With all of these burdens required by the Act, the burden does not outweigh the benefit. Proving that the security procedure was commercially reasonable under the circumstances, adequately implemented, and relied upon in good faith will cost time and money. These burdens are too great of a risk for anyone simply seeking a binding agreement to undertake. A digital signature is nothing more than a security procedure commenced over the Internet. Therefore, unless a recipient is willing to take on the responsibility of being able to prove the above burdens, the

tronic record at a particular point in time does not necessarily establish its status as a secure electronic record indefinitely into the future." *Id.* at cmt. 6. The time of verification has a limitation which takes into account two situations:

> [F]irst, although the status record as a secure electronic record may have been established as of the time it was received, there is the possibility that an electronic record may have been tampered with or altered sometime after it was received and prior to the time that it is tendered to a court for the resolution of a dispute. By reapplying the security procedure at the time of the dispute, such alteration will be disclosed. Second, there also exists the possibility that a strong security procedure used at the time an electronic record was communicated may no longer be considered a strong security procedure at the time the record becomes material to a dispute (i.e., with the passage of time it may have become possible to "crack" the security procedure, and thus alter the electronic record in a manner that cannot be detected by the security procedure). In such a case, the court or other trier of fact will need to make a determination as to the continued viability of a security procedure that it used— i.e., that evidence regarding the vulnerability of a security procedure may be used to rebut the presumption accorded to its status as a secure electronic record by Section 10-120. In the event that technology changes, and new developments render unreliable a security procedure that was previously considered trustworthy, it is contemplated that the requirement of commercial reasonableness, the requirement of a trustworthy implementation, and the requirement of good faith reliance will all operate to allow a court to conclude that a previously accepted security procedure is no longer secure in a given set of circumstances.

Id. Furthermore, the application of "time of verification" requirement:

> [C]ontemplates that the proponent of an electronic record will retain the information, software, digital certificates, and/or other materials necessary to execute or implement the appropriate security procedure so that it is available at such time when it may be necessary to establish the integrity of the electronic record (e.g., in court). If there is a possibility of degradation in the strength of the security procedure over time, such party may also have the burden of addressing this issue, such as by retaining an independent third party to preserve the evidence or otherwise protecting the electronic record through the use of a new more secure security procedure.

Id. at cmt 7. However, one must also note that the effect of the "time of verification" requirement does not render "the initial verification of an electronic record through the application of a security procedure at the time that an electronic record is received." *Id.* Verification is important to determine, "the reasonableness of reliance by the relying party of the message, and thus, is important even if a message is subsequently altered or a security procedure subsequently becomes ineffective as a result of advances in technology." *Id.* The reference to "specific point in time" in section 10-105(a) of the Act is not intended to require calculation of a specific time, although that may be necessary in some cases. *Id.* at cmt. 8. Instead, the point in time that will be necessary to know may be defined by reference to an event which will suffice for resolving the dispute. An example of such [an] event can consist of record creation or signing. *Id.*

risk is too great and, thus, potential participants must be hesitant to use the digital signature process as regulated by the Act.

2. *Why Using a Digital Signature as Regulated by the Act is too Great of a Risk for the Relying Party*

A subscriber is only held to a reasonable standard of care.[104] In a normal transaction where reasonable care was taken, a subscriber can defeat his or her liability. In order to understand the significance of such an event, the checkbook analysis used above serves as a good illustration.[105] For example, an employer possessing a checkbook and a signature device will not be held liable where there is a showing that no inadequacy of security precautions were taken.[106] In one case, an employer was not found negligent during a series of burglaries in which checks were removed from the back of the checkbook and the checks were signed using the employer's rubber signature stamp.[107] The checkbook and the signature stamp were left in their regular place and appeared to be left untouched.[108] The employer, upon receiving notice of a bank statement, promptly notified the bank that a forgery had taken place.[109] The court found no inference of negligence.[110]

A relying party must realize that the standard of reasonable care that a subscriber will use in protecting the signature device is not acceptable. Therefore, a recipient must not use digital signatures, as regulated by the Act, until the standard of care is heightened to absolute liability for the subscriber regarding the safekeeping functions of the subscriber's private key.[111] Therefore, a relying party must continue to use the notarization process until the Act is properly amended, so that the relying party can conduct business without worrying about the subscriber and the whereabouts of its private key.

C. Certification Authority—A God Like Stature

A certification authority mirrors the responsibility of a notary[112] in

[104] *See* Illinois Electronic Commerce Security Act § 10-125(2).

[105] *See supra* note 80.

[106] *See* Illinois Electronic Commerce Security Act § 10-125 cmt. 3.

[107] *See* Illinois Electronic Commerce Security Act, H.B. 3180, § 10-125 (effective July 1, 1999) <http://www.mbc.com/legis/cecc-fin.html>.

[108] *See id.*

[109] *See id.*

[110] *See id.*

[111] *See* Closen & Richards, *supra* note 5, at 745 (stating that safekeeping the private key is a preventive measure that the subscriber must undertake).

[112] The standard to become a notary varies throughout the jurisdictions. A notary public is defined as:

> A public officer whose function is to administer oaths; to attest and certify; by his [or her] hand and official seal, certain classes of documents in order to give them

the sense that it is an official verification authority, just like a notary who signs and affixes a seal[113] on a document to signify the identity of a document signer and the validity of the signature.[114] However, one significant difference between the two verification authorities is that a notary in most jurisdictions must be at least eighteen years old and must proclaim no record of felonies.[115] Additionally, notaries in some thirty

> credit and authenticity in foreign jurisdictions; to take acknowledgments of deeds other conveyances, and certify the same; and to perform certain official acts, chiefly in commercial matters, such as the protesting of notes, bills, [and] the noting of foreign drafts . . . .

BLACK'S LAW DICTIONARY 1060 (6th ed. 1990). In general, an applicant must be about eighteen years old. *See* Closen & Richards, *supra* note 5, at 721. The applicant must also be a resident of the state in which they act. *Id.* Notary applicants may also need to proclaim on their application whether they have any criminal record of felonies; however, most states do not verify the criminal records of these applicants. *Id.* Notaries in some thirty states are also required to obtain a surety bond to "'assure the faithful performance of duties, and to compensate any person who may suffer a loss because of the notary's misconduct.'" *Id.* The notary applicant pays a minimal fee and, after taking an oath of office, the applicant becomes an official notary for a term of about four years. *Id.* at 722. A number of states require that the notary applicant be literate in English or some other language. *Id.* A few states also require notary applicants to submit to a written examination. *Id.*

A notary is vested with the full authority by the state's notary law. *Id.* The statutory authority of notaries will vary from state to state. *Id.* at 723. However, all notaries possess at least two types of authority: "(1) they can administer oaths (such as given to witnesses, and to public officials when they are sworn into office), and (2) notaries can attest to the authenticity of signatures on documents." *Id.* Notaries also, in some states, can perform weddings, can protest against commercial paper, can open and inventory bank deposit boxes, and they also can verify copies of certain documents. *Id.*

[113] The seal has it origins from ancient Rome. Kumpe v. Gee, 187 S.W. 2d 932, 934 (Tex. Ct. App. 1945); Raymond C. Rothman, NOTARY PUBLIC PRACTICES AND GLOSSARY 1 (1978). Parties in contracts were often not able to write. *Id.* at 1. The parties, therefore, "would use metal or a clay disk, called a private seal,' which was engraved with a special design or family coat of arms as their signature to the agreement." *Id.* A sticky substance was then "melted onto the paper at the end of the document, upon which the private seal was impressed." *Id.* "In the centuries to follow, people learned to write, and the art of making paper became more merchandised, thus increasing supply." *Id.* Eventually contracts were taking up more than one page; thus, two holes were made in the margin of the papers and tied together with ribbon. *Id.* at 2. The notary would melt wax over the ribbon's knot and impress it with a seal. *Id.* This process is how today's definition of the word "seal," meaning to "make secure," came into being. *Id.* For information regarding promises under seal, *see generally* Eric Mills Holmes, *Stature and Status of a Promise Under Seal as a Legal Formality*, 29 WILLAMETTE L. REV. 617 (1993).

[114] *See* Closen & Richards, *supra* note 5, at 742; Emilo Jaksetic, *Notaries Who Undermine Our Property System*, 22 ILL. L. REV. 748, 749 (1928). Computer-based transactions have now given rise to an entity whose responsibility is to ensure the integrity of the transaction. *Id.* at 21. The entity is known as the certification authority. *See generally* Benjamin Wright, *Eggs in Baskets: Distributing the Risks of Electronic Signatures*, 15 J. MARSHALL J. COMPUTER & INFO. L. 189 (1997). "Just as risks plague the authentication of paper documents, so too will they plague the authentication of electronic documents." *Id.* at 191.

[115] *See* Closen & Richards, *supra* note 5, at 720.

states are required to obtain a surety bond to assure the faithful performance of duties, and to compensate any person who may suffer a loss because of the notary's misconduct.[116] Unfortunately, the Act does not require a minimum age limit, no background check exists, and no minimum insurance is necessary. In fact, there are absolutely no requirements to become a certification authority.[117] The certification authority could be an eleven-year-old or a convict who has just been released from prison for committing computer fraud. The standard to become a certification authority is not sufficient.

In response to certification authority requirements, the Act declares that for public policy reasons the regulation of certification authorities is not appropriate.[118] The Commission believes that it will "inhibit rather

[116] *See id.* at 721.

[117] At least Utah has created some basic requirements for persons who want to obtain a license as a certification authority:

> (1) To obtain or retain a license a certification authority shall:
>
> (a) be the subscriber of a certificate published in a recognized repository;
>
> (b) employ as operative personnel only persons who have not been convicted of a felony or a crime involving fraud, false statement, or deception;
>
> (c) employ as operative personnel only persons who have demonstrated knowledge and proficiency in following the requirements of this chapter;
>
> (d) file with the division a suitable guaranty, unless the certification authority is the governor, a department or division of state government, the attorney general, state auditor, state treasurer, the judicial council, a city, a county, or the Legislature or its staff offices provided that:
>
> (i) each of the above named governmental entities may act through designated officials authorized by ordinance, rule, or statute to perform certification authority functions; and
>
> (ii) one of the above named governmental entities is the subscriber of all certificates issued by the certification authority;
>
> (e) have the right to use a trustworthy system, including a secure means for controlling usage of its private key;
>
> (f) present proof to the division of having working capital reasonably sufficient, according to the rules of the division, to enable the applicant to conduct business as a certification authority;
>
> (g) maintain an office in Utah or have established a registered agent for service of process in Utah; and
>
> (h) comply with all other licensing requirements established by division rule.

UTAH CODE ANN. § 46-3-201.

[118] *See* Illinois Electronic Commerce Security Act § 15-115 cmt. 2. The Act states that at some point in time it may be appropriate to regulate when "the marketplace has matured, appropriate business models have been established, and specific abuses and problems have been identified." *Id.* at cmt. 2(a). There are four reasons for regulating the issuance of certificates and the conduct of the certification authorities:

> (1) to ensure quality control of certification authorities in order to protect the citizens of the state from fraudulent or inappropriate conduct by certification authorities, and the damage that may flow from improperly issued certificates (i.e., public policy reasons);
>
> (2) to provide a source of revenue, such as that which might be generated by a collection of license fees;

than enable the development of electronic commerce."[119] However, with-

> (3) to ensure the quality control of certificates issued by certification authorities for the purpose of determining when a digital signature qualifies as a signature under the laws of the state; and
>
> (4) to measure the trustworthiness of a certificate for purposes of determining when it is sufficiently trustworthy such that a digital signature verified with reference to such a certificate will be accorded heightened evidentiary presumptions (e.g., status as a secure electronic signature).

Id. at cmt. 2. However, the Act negates the first three. The Act, in negating the first suggested factor, states that regulation of certification authorities for public policy reasons "is deemed not to be appropriate at this time for a variety of reasons." *Id.* at cmt. 2 (a). One reason is that because the use of digital signatures is so new, there is concern that if the state tried to regulate the conduct of certification authorities that it will "simply interfere with the development of the marketplace and appropriate business models, and thus inhibit rather than enable the development of electronic commerce." *Id.* The Act further states that regulation is "deemed inappropriate because it appears to be unworkable at a state-by-state or country-by-country level as applied to a system of global commerce." *Id.*

The Act, in addressing the second suggested factor, states that regulation of certification authorities "for purposes of raising additional revenues is also deemed to be inappropriate because of the potentially inhibiting effects that it may have on the implementation of electronic commerce." *Id.* at cmt. 2(b). The purpose of the act is to "enable and promote electronic commerce, not inhibit or restrict it, such that taxation is deemed inappropriate." *Id.* The Act further states that in the current marketplace it would not be a profitable idea. However, the Act does allow the Secretary of State to charge a fee in relation to the "certification or accreditation of certification authorities if appropriate to recover costs." *Id.*

The Act, in addressing the third suggested factor, states that there is no need to regulate "certification authorities in order to determine when a digital signature qualifies as a signature." *Id.* at cmt. 2(c). The Act states that pursuant to section 5-120, that "any electronic signature qualifies as a signature, regardless of the level of security inherent within it. Thus, an electronic 'x,' a digitized handwritten signature, a digital signature of low trustworthiness, and a highly reliable digital signature, all qualify as a signature for purposes of statutory writing and signature requirements." *Id.* There is not "minimum threshold" that an electronic mark must meet. *Id.* All that matters is that the mark can be shown that it was made by the purported signer with the "requisite intent." *Id.* "Proving such facts may be difficult for the recipient of many forms of electronic signatures, and the ability to prove such facts may effect the willingness of a recipient to rely on messages signed with certain forms of electronic signatures." *Id.* However, if the recipient is able to prove that the symbol was made by a specific person "with the requisite intent, the signature is considered valid, just as it would be if the same 'x' were typed onto a paper document by the same person with the same intent." *Id.* This position "recognizes that there may be many uses for certificates that do not carry a high level of reliability, and that it is the intent not to inhibit or restrict the use of such certificates at this time." *Id.*

The Act, in addressing the fourth suggested factor, states that this is the only "regulation of certification authorities deemed appropriate for the state at this time. *Id.* at cmt. 2(c). This approach is similar to the approach taken by the state in addressing handwritten signatures. *Id.* For example, "the creation of handwritten signatures is not regulated except in situations where the state grants heightened evidentiary presumption to a handwritten signature." *Id.* An example of this occurs with respect to the notarization of signatures, "which makes a document self-authenticating under applicable rules of evidence, obtaining the benefit of such a presumption requires the use of a notary licensed by the state." *Id.*

[119] Illinois Electronic Commerce Security Act § 15-115 cmt. 2(a).

out immediate basic regulation, the advancement of electronic commerce will not progress, but instead regress through the errors and misconduct of an unregulated verification authority, and thus, the goals of the Act will be defeated.[120] Therefore, until certification authority requirements are implemented under the Act, one must not use digital signatures as a mode of communication.

[120] Section 15-115(a) of the Illinois Electronic Commerce Security Act states that the Secretary of State may:

> (a) [A]dopt rules applicable to both the public and private sectors for the purpose of defining when a certificate is considered trustworthy under Section 15-105 such that a digital signature verified by reference to such a certificate will be considered a qualified security procedure under Section 10-110. The rules may include (1) establishing or adopting standards applicable to certification authorities or certificates, compliance with which may be measured by becoming certified by the Secretary of State, becoming accredited by one or more independent accrediting entities recognized by the Secretary of State, or by other means, and (2) where appropriate, establishing fees to be charged by the Secretary of State to recover all or a portion of its costs in connection therewith.
>
> (b) In developing the rules, the Secretary of State shall endeavor to do so in a manner that will provide maximum flexibility to the implementation of digital signature technology and the business models necessary to support it, that will provide a clear basis for the recognition of certificates issued by foreign certification authorities, and, to the extent reasonably possible, that will maximize the opportunities for uniformity with the laws of other jurisdictions (both within the United States and internationally).
>
> (c) The Secretary of State shall have exclusive authority to adopt rules authorized by this section.

Id. Illinois has many statutes that "grant privileges or authority to persons or entities accredited by third party private accreditation agencies." *Id.* at cmt. 4(c). For example:

> (a) Adult developmental training day services which must meet minimum standards specified by the Department of Human Services or alternatively, may be accredited under nationally recognized accreditation programs, in which case they will be deemed to have met the standards established by the department. Mental Health and Developmental Disabilities Administrative Act, 20 ILL. COMP. STAT. 1705/15.2.
>
> (b) A substitute teacher's certificate may be issued to persons who meet certain requirements, or alternatively, who hold a Bachelor of Arts degree from an institution of higher learning accredited by the North Central Association or other comparable regional accrediting association. Certification of Teachers, 105 ILL. COMP. STAT. 5/21-9.
>
> (c) Licenses to practice clinical psychology are issued to person[s] who have graduated from schools accredited by the American Psychological Association or similar regional accrediting body. Clinical Psychologist Licensing Act, 225 ILL. COMP. STAT. 15110.

Id. In subsection (b), two points are recognized:

> First, that it is important not to adopt regulations that might unduly restrict the development and implementation of digital signature technology to facilitate electronic commerce. Second, that to the extent possible, it is important to promote uniformity of law and interoperability of regulatory provisions on a national and international level in order to facilitate and promote international electronic commerce.

Id. at cmt. 5.

D. Potential Digital Signature Participants Must Continue To Use the Notarization Process, Because the Act Creates Too Great of a Potential Liability

1. *The Advantages of the Notarization Process*

An advantage of using the notarization process is the liability coverage that a notary maintains.[121] A certification authority under the Act, however, is not required to maintain any liability coverage. This omission alone immediately warns a potential participant of the digital signature process that there is the potential to incur great loss. Why speculate in a business transaction in which the most important part, being the verification of the digital signature, is done by a person who has no liability insurance? At least in the notarization process, there is some type of basic coverage.[122] Without insurance, participants will be

[121] *See* Closen & Richards, *supra* note 5, at 725. "The standard of liability for the notary public is almost uniformly one of objective reasonable prudence, meaning that under the law a notary must act as a reasonable notary would act under similar circumstances." *Id.* A notary public will nearly always be liable for "negligent, reckless, or willful conduct." *Id.* The notary may be liable for all proximately caused injuries. *Id.* The liability may also extend to the notary's employer under "common law vicarious liability principles or under the employer responsibility provisions of state notary statutes." *Id.* at 726. However, "notaries are not held liable for acknowledging a forged signature on a document where they have acted in good faith, and with reasonable efforts to discover the identity of the individual whose signature is being notarized." *Id.* at 727. Nevertheless, if a notary does engage in negligent conduct, he or she may be held liable and, if the notary commits a willful violation, "such as executing a knowingly false attestation, s/he may be liable for all proximately caused injuries, possibly including punitive damages." *Id.* Furthermore, "any conduct rising to the level of criminal activity may result in criminal prosecution, for official misconduct or for violation of the state notary statute's criminal provisions." *Id.* A notary's negligence is not tolerated in courts of law, as evidenced by the court in *Summers Bros. Inc. v. Brewer*, 420 So. 2d 197 (La. Ct. App. 1982), where it held that:

> Even if [the notary] did not know that the signature on the contract were forgeries, he knew that by authenticating the document, as a notary, he was telling the world that the parties had appeared before him and affixed their signatures in his presence. Thus, he committed fraud in that he purposely let third parties rely on a document purporting to be genuine but actually without validity as an authentic act. The "proof of validity he supplied was misleading to all who relied on the contract.

Id. at 204. *See also* Immerman v. Ostertag, 199 A.2d 869, 874 (N.J. Super. Ct. Law Div. 1964) (concluding that a notary displayed a "high degree of negligence" in certifying an acknowledgment without determining whether the individuals purporting to have made the statements even knew of the nature or the contents of what they were signing); Galloway v. Cinello, 423 S.E.2d 875, 881 (W. Va. 1992) (finding that a notary's negligent act proximately caused the defendant to lose her status as a secured creditor); City Consumer Serv. Inc. v. Metcalf, 775 P.2d 1065 (Ariz. 1989) (finding that the notary negligently notarized a woman's deed based solely upon representation).

[122] *See* Closen & Richards, *supra* note 5, at 709. However, one must note that bonds "do not actually protect notaries because, if the bond company has to pay a claim resulting from a particular notary's mistake or misconduct, the bond company will seek reimbursement from that notary." *Id.*

at the mercy of the certification authority and, thus, all that participants can do is hope that the certification authority does not negligently or intentionally make a mistake. Therefore, until the Act creates some type of minimal liability coverage for certification authorities, potential participants must use digital signatures at their own risk.

2. *The Advantages of Signing Paper Documents*

The notarization process is more trustworthy than the digital signature process because the verification authority in the notarization process has more reliable documentation standards. For example, the typical legal battle that will emerge in digital signature cases, as regulated by the Act, will involve the unauthorized use of a subscriber's private key and the damage that it caused to the relying party. However, this battle could have been prevented if the parties would have used a notary.

When having a document notarized, the notary can refuse to notarize the document if the notary has knowledge or reasonable suspicion[123] that the transaction that is about to happen is unlawful. The notary can also insist that the signer, and any witness who will be identifying the signer, be present before the notary at the time of notarization.[124] Addi-

[123] NAT'L NOTARY ASS'N., THE NOTARY PUB. CODE OF PROF. RESP., § I-A-2 (1998) (unpublished final draft). The following is a situation where the Notary should refuse to notarize a stranger's document, because there is evidence that the stranger's I.D. has been tampered with, thus, notifying the notary that the stranger is an impostor. *Id.*

> The Notary is asked by a stranger to notarize that person's signature on a document. As proof of identity, the stranger presents a single identification card, a state driver's license. The Notary notices that the photograph on the license is raised from the surface of the card and appears to overlay a state seal and the signature of a DMV official.

Id. The purpose of the Code of Professional Responsibility [hereinafter Code] is to "guide Notaries Public in the United States when statutes, regulations and official directives fall short." *Id.* at 2. The Code has two types of standards. "The majority are principals, policies and practices that have proven over the years to be effective in helping notaries perform their primary function of detecting and deterring fraud; in minimizing fraud, these standards also work to reduce the Notary's exposure to lawsuits." *Id.* The Code's second standard "derive[s] from the conviction that a public officer in a democracy must serve all persons equally, without regard to such distinctions as race, nationality, ethnicity, citizenship, religion, politics, lifestyle, age, disability, gender, or sexual orientation." *Id.*

Furthermore, because the acts of notaries effect "individual rights and property under both civil and criminal law, it is imperative that professional standards for Notaries be widely acknowledged as just, fair and well developed." *Id.* Therefore, the standards of the Code were created from "input of representatives of occupational fields with a large constituency of Notaries Public." *Id.*

[124] *Id.* § III-A-1. For example, a notary "is telephoned by a client who has just signed and mailed several documents for the Notary to notarize without personal appearance." *Id.* The notary should decline to perform a "telephone notarization" without "the physical presence of the signer, since it would be a clear violation of the law, even though the Notary feels relatively certain about the identity, volition and awareness of the signer." *Id.*

tionally, the notary identifies each signer through personal knowledge, at least one reliable identification document bearing a photograph, or the sworn word of a credible witness.[125] Furthermore, the notary cannot notarize if the notary believes that the signer is not aware of the significance of the transaction.[126] The notary can also administer an oath to compel truthfulness in a witness who is identifying a signer[127] and can require that two individuals in addition to the notary witness[128] the affixation of the signer's mark.

In comparison, the signing of an electronic document using the digital signature process, as regulated by the Act, is less concerned with the identity of the subscriber, and instead focuses on the authenticity of the

[125] *Id.* § III-B-1. For example:

> The Notary is approached by a friend and a stranger identified by the friend as a business associate. The friend requests notarization of the associate's signature on a document, but is not involved in the transaction. When the Notary asks the associate for identification, the friend becomes indignant because the Notary won't take his word as bond.

Id. The notary should continue to insist that the "associate produce a reliable form of identification bearing a photograph or that the friend be formally sworn in as a credible witness vouching for the associate's identity." *Id.*

[126] *Id.* § Ill-C-1. For example:

> The Notary is called to the home of an elderly person to notarize that individual's signature on several documents. The Notary is introduced to that would be signer by the person's relative. Acting in a childlike manner, the elderly person appears disinterested in the documents. Though the relative urges the Notary to act, the Notary is unable to get a coherent response to the question, "Why do you want to sign these documents?"

Id. The notary should not notarize the documents, because the person's conduct indicates a strong likelihood that the "individual is not at the moment capable of a responsible action." *Id.*

[127] *Id.* § 111-D-2. For example, a notary is telephoned by a client who tells the notary that he will stop by later that day to sign a deed that needs to be notarized. *Id.* "The client mentions that the deed requires one witness in addition to the Notary, and asks if a friend may witness the signature on the document before it is brought in." *Id.* The notary explains that:

> [T]he client may sign the deed and have the signature witnessed outside of the Notary's presence prior to appearing before the Notary to acknowledge the signature. The Notary also explains that it will not be necessary for the witness to appear and take an oath, since the Notary will positively identify the client based on personal knowledge of identity and not rely on the witness to make the identification.

Id.

[128] *Id.* § 111-D-7. For example, the notary is called to the bedside of patient at a hospital to notarize a "person's signature on a power of attorney naming a spouse as attorney in fact." *Id.* The patient who is ill and weak is only able to affix an "x" on the document rather than the normal signature. *Id.* "The spouse offers to sign as a witness to the mark." *Id.* "The notary explains that two persons in addition to the Notary must witness the making of the mark." *Id.* Therefore, "[t]he Notary disqualifies the spouse as a witness, since the individual is both in and affected by the document. Instead, the spouse finds two neighbors, both of whom present reliable ID cards, to witness the patient's mark." *Id.*

subscriber's signature device. To have an electronic document signed using the digital signature process, the subscriber will encode his or her signature on the computer using the private key, which acts as the signature device.[129] By doing so, the digital signature will go to a repository that has stored the coded signature.[130] The certification authority then checks the repository to see if the private key matches the public key of the relying party which is also on file in the repository.[131] If there is a match, the certification authority digitally signs the document and issues a computer-based certificate of authenticity.[132] This approval of sorts by the certification authority is similar to a notary who signs and seals a document to signify the validity of the transaction. However, a certification authority cannot determine whether the subscriber is authorized or whether the subscriber is an impostor. The certification authority can only determine whether the subscriber has the correct signature device. Therefore, the identity of the subscriber remains anonymous, unlike the signer in a notarization, thereby increasing the chances of fraud and liability.

To cure this defect, the Act must either amend the standard of care to absolute liability or instill biometric technology[133] to accompany digital signatures, or notarization will always be superior to digital signatures in regard to the identification of the signer. Therefore, a participant must not use a digital signature, as regulated by the Act, until the Act adopts better ways to truly know the identity of the signer.

E. Suggested Amendments to the Act

The Act is a great step forward for Illinois and the Nation. The implementation of digital signatures as a security procedure for electronic commerce is an efficient creation destined to be used worldwide. However, the Act must be properly amended and, until such a time occurs, a participant must use it at his or her own risk.

1. *Absolute Liability for the Subscriber*

The Act requires that a subscriber exercise reasonable care to prevent the unauthorized use of his or her private key. This standard is too low. The subscriber must be held to the standard of absolute liability for the unauthorized use of his or her private key. In doing so, the participants in the digital signature process will greatly increase their confi-

[129] *See* Closen & Richards, *supra* note 5, at 737.

[130] *See id.*

[131] *See id.*

[132] *See id.* (stating that authenticating an electronic document is a process that must be regulated for a successful digital signature program).

[133] *See infra* note 143.

dence because of the integrity of the process.[134] Furthermore, with absolute liability, the subscriber is forced to closely guard the private key. Thus, the subscriber reduces his or her overall liability stemming from unauthorized use and unauthorized access, which will happen more often when a reasonable standard of care is used.

2. *Certification Authority Requirements*

A certification authority plays the most important role in the digital signature process. The certification authority is the gatekeeper of authentication. However, the Act has no requirements to become a certification authority. The Act must delineate to a commissioning officer the ability to accept or reject certification authority applicants based on requirements regarding experience, age, and education. Furthermore, the agency in charge of issuing the revocable license to a certification authority should also do a background check for criminal records and other violations, especially focusing on those who have committed fraud.

The suggested type of screening parallels the screening as listed in The Model Notary Act.[135] The Model Notary Act requires an applicant to be at least eighteen years old, possess the ability to read and write in English, and to have passed the notary written examination.[136] Furthermore, the notary-commissioning officer, as regulated by The Model Notary Act, can deny an applicant if the applicant has been convicted of a crime involving dishonesty or moral turpitude.[137]

The Act does not establish any financial responsibility levels for a certification authority. Moreover, the Act does not require the certification authority to carry any liability insurance. This is not acceptable. This Act has not considered the human factor. A human will commit error. A human will lie, cheat, and steal. The other parties must be held responsible for such negligent and intentional misconduct. These human errors create insecurity in the process, therefore, a certification authority must be required to carry minimum insurance for specific levels of transactions.

F. Suggested Security Techniques for the Subscriber

A subscriber can use a number of security techniques to protect the private key. One example of a good defense is the use of a security sys-

[134] *See* Closen & Richards, *supra* note 5, at 754. If absolute liability did exist, insurance companies would most likely insure "private key holders against theft or loss of their private key, thus providing more assurance to both private key holders as well as their intended recipients." *Id.*

[135] *See* The Nat'l Notary Ass'n, *supra* note 71, § 2-101 (9-13).

[136] *See id.*

[137] *See id.* § 2-101 (16-18).

tem in the start up program of the computer. Such a system would not allow a user to proceed beyond the security screen, unless the correct password is entered. Another defensive tactic is to isolate the computer in a room specifically reserved for such transactions. The door to the room could have numerous types of security features itself and only those who have access would be allowed to enter the secured room. Therefore, the key to a good defense is to take security measures not only to protect access to the computer upon which the transaction will take place, but also to deny access to the room that the computer will be placed.

In the future, when digital signatures are commonplace, the first line of defense will not be enough. The more that is known about the technology, the easier it is to master. Thus, passwords that will try to keep away persons that do not belong will become manageable for an unauthorized user. Therefore, more stringent tactics are needed to prevent such intrusions. One such tactic is the use of a cryptographic token or smart card.[138] This method stores the private key in the token or card and, thus, the private key is never divulged outside of the token or card.[139] In doing so, the private key does not pass into the main memory of the subscriber's computer,[140] which can prevent unauthorized users from retrieving the private key upon gaining access to the computer's memory. Another added benefit to such a security system is that the token or card will not fully activate in the computer unless a password or personal identification number is entered, thus, making access even harder.[141] Another example of technology that can make keeping the private key a less foreboding task is the use of biometric authentication[142] such as a retinal scan or fingerprint scan.[143] These types of high-

[138] *See Digital Signature Guidelines*, *supra* note 2, at 8 n.20. Numerous methods are available for securing a private key. *Id.* "The safer methods store the private key in a 'cryptographic token' (one example is a 'smart card') which executes the signature program within an internal microprocessing chip, so that the private key is never divulged outside the token. *Id.* Furthermore, by using a "cryptographic token" the private key does "not pass into the main memory or processor of the signer's computer." *Id.* Moreover:

> The signer must typically present to the token some authenticating information, such as a password, pass phrase, or personal identification number, for the token to run a process requiring access to the private key. In addition, this token must be physically produced, and biometric authentication such as finger prints or retinal scan can assure the physical presence of the token's authorization holder. There are also software-based schemes for protecting the security of the private key, generally less secure than hardware schemes, but providing adequate security for many types of applications.

Id.

[139] *See id.*

[140] *See id.*

[141] *See id.* (providing such a device for the implementation of the subscriber's private key is a good preventive measure for protecting against unauthorized access).

[142] *See id.*

tech security systems will assure the physical presence of the subscriber and/or designated agents of the subscriber,[144] and perhaps are the best means of denying unauthorized user access.

IV. CONCLUSION

> I am not an advocate for frequent changes in laws and institutions. But laws and institutions must go hand-in-hand with progress of the human mind. As that becomes more developed, more enlightened, as new discoveries are made, new truths discovered and manners and opinions change, with change of circumstances, institutions must advance also to keep pace with the times.
>
> Thomas Jefferson (1816)[145]

The ability of persons to use digital signatures with confidence as a documentation device creates new and exciting applications. However, if the act hinders the use rather than advances it, the act has sufficiently defeated the technology. This is the case with the Act. The Act has made the use of digital signature technology impractical due to the increased risk of liability for the participants who use the procedure. Therefore, potential digital signature users must continue to use the notarization process, until the Act can be properly amended to cure its deficiencies.

To cure the deficiencies, the authors of the Act must examine the Model Notary Act,[146] other digital signature acts,[147] and commentaries on the Act,[148] in order to get an overall assessment regarding potential improvements. Suggested improvements consist of making the sub-

[143] *See Digital Signature Guidelines*, *supra* note 2, at 8 n.20. Some notary legislation requires the signer's thumbprint before notarization. Therefore, an exact identifying mark is recorded. For example, California requires notaries to take signer's thumbprints before notarizing real estate deeds. *See* Closen & Richards, *supra* note 5, at 733 n.183. Using thumbprint identification accomplishes many goals. First, thumb printings will "deter impostors from scamming notaries into notarizing forged deeds because it is unlikely that the forger would want to leave a thumbprint." *Id.* Second, thumb printing can deter "signers from falsely attesting to a conartist's forged signature for fear of individual culpability." *Id.* Third, thumb printing "puts all signers, especially the vulnerable, like the elderly, on notice of the serious legal consequences of what they are about to sign." *Id.* It seems that digital signature legislation should take some lessons from notary legislation with regard to protecting the participants.

[144] *See Digital Signature Guidelines*, *supra* note 2, at 8 n.20.

[145] John C. Yates, *Recent Legal Issues in Electronic Commerce and Electronic Data Interchange*, 430 PRAC. L. INST. 271, 277 (1996).

[146] *See* THE NAT'L NOTARY ASS'N, *supra* note 71.

[147] *See* The Basics of Digital Signatures, 2 (visited September 4, 1998) <http://www.uiw.com>. There are over thirty-five states that have passed digital signature legislation.

[148] This Comment along with other law journal articles can provide a good source of non-bias information.

scriber absolutely liable for the standard of care given to its private key, creating certification authority requirements,[149] and requiring a certification authority to possess minimum liability insurance for specific transactions. Therefore, only upon making such amendments, can the Act regain its true intent of protecting and promoting "the interests of Illinois businesses and citizens engaged in online business, commercial, and personal activities."[150]

Stephen G. Myers

[149] *See* Illinois Electronic Commerce Security Act, H.B. 3180, § 10-135 (effective July 1, 1999) <http://www.mbc.com/legis/eecc-fin.html>. The Act gives the Secretary of State the power to adopt rules for the certification or decertification of security procedures, and for adopting standards for the use of electronic signatures by the State. *Id.* The Secretary of State can also authorize standards for both the public and private certification authorities through State certification or accreditation by an independent accrediting agency. *Id.* § 15-115.

[150] COMMISSION ON ELECTRONIC COMMERCE AND CRIME, *supra* note 6, at 4.