SINGER FRUMENTO
LLP
ATTORNEYS AT LAW

NEW YORK OFFICE
40 Exchange Place
20th Floor
New York, NY 10005

(212) 809-8550
(212) 344-0394 facsimile

E-MAIL: BSINGER@SINGERFRU.COM
WEBSITE: HTTP://SINGERFRU.COM

DIRECT DIAL: (212) 849-1260
DIRECT E-MAIL: afrumento@singerfru.com

NEW JERSEY OFFICE
Maritime Law Center
37 Marin Boulevard
Jersey City, NJ 07302

(201) 507-9900
(201) 507-3995 facsimile

How to Think About Electronic and Digital Signatures
A Tutorial From a Litigator's Perspective

By

Aegis J. Frumento
Litigation Partner
Singer Frumento LLP
New York, New York

Prepared for
The American Conference Institute
Conference on Internet Securities Regulation
New York, New York
June 26-27, 2000

> *When all preliminaries were over and Peleg had got everything ready for signing, he turned to me and said, "I guess, Quohog there don't know how to write, does he? I say, Quohog, blast ye! dost thou sign thy name or make thy mark?"*
>
> *But at this question, Queequeg, who had twice or thrice before taken part in similar ceremonies, looked no ways abashed; but taking the offered pen, copied upon the paper, in proper place, an exact counterpart of a queer round figure which was tattooed upon his arm; so that through Captain Peleg's obstinate mistake touching his appellative, it stood something like this:--*
>
> *Quohog.*
> *his* **[** *mark.*
>
> *H. Melville,* ***Moby Dick***

I. The General Problem of Signatures*

Courtroom Vignette: The Case of the Holographic Signature

Examination by Plaintiff Counsel:

Q: Mr. Smith, have you seen this document, Exhibit A, before.

A: Yes.

Q: When was that?

A: When I received it from Mr. Jones.

Q: Has there been any change to this document since you

* I thankfully acknowledge the able assistance of Stephanie Rosenblatt, Esq., associate of Singer Frumento, LLP, in preparing the final text of this article. Thanks also to my colleagues Bill T. Singer, Esq., Thomas A. Rigilano, Esq., and Aimee E. Goldstein, Esq., for their review and editorial comments.

received it?

A: No.

Q: Do you see a signature at the bottom there?

A: Yes, I do.

Q: Do you know whose signature that is?

A: Yes, that is Mr. Jones' signature.

Q: Have you seen Mr. Jones' signature before?

A: Yes many times. He wrote me often.

Plaintiff Counsel: Your Honor, I offer Exhibit A in evidence.

The Court: Objection?

Defense Counsel: Yes, Your Honor. We contend that signature is a forgery.

The Court: The Exhibit has been properly authenticated by this witness. He testified of his own knowledge that he knows and recognizes the signature as Mr. Jones's. You will have the opportunity to prove it is a forgery as part of your case. Objection overruled. Exhibit A is received in evidence.

This scene is enacted time and again in courts, arbitration hearing rooms, and other tribunals, to the point of seeming trivial. A signed document has just been admitted into evidence. The rest of the case now flows with reference to the rights and obligations laid out in that document. Elementary trial procedure, to be sure. Yet, it is a good point from which to consider the problem of signatures in general, as a prelude to discussing

the problems of electronic and digital signatures in particular.[1]

It is interesting to note that signatures do not count for much in the substantive law. The legal validity of very few documents depends on their being "subscribed:" wills, contracts governed by the statute of frauds, and not much else.[2] Yet, even when not required, we routinely sign documents. We do so for one or another of the following reasons:

1. To identify the signer.
2. To signify that the signer has adopted the document has his own act.
3. To signify that the content of the document is complete and final, that it is in some way "the last word."
4. To show that the document was considered, and not a frivolity or an accident.

Those reasons do not serve merely our own vanity. The signature on a document communicates something to the recipient of the document and indeed to the world. My signature on a document says that *it came from me ("**identity**")*, that I authored or otherwise *adopted the content ("**adoption**")*, that the document is *complete*

---

[1] In these courtroom vignettes, I have intentionally taken a strict view and made the hypothetical judge a stickler for evidentiary rules. I recognize that in making evidentiary rulings, trial judges have wide latitude, and that many judges might rule differently given these scenarios without fear of reversal. I also recognize that many disputes in the securities industry are resolved by arbitration panels that are not bound by the rules of evidence. Accordingly, many of you might think that the problems I identify here are theoretical only, and of no practical concern, and you may be right. However, my purpose is not to teach a course on evidence, but to give a framework for analyzing the evidentiary issues surrounding electronic and digital signatures, and to that didactic end, using a conservative judge serves well. If these issues never cause you any real-world grief, so much the better.

[2] Even the statute of frauds does not invalidate unsigned contracts--it just makes them unenforceable. That may seem like the same thing, but it is not, for that technical distinction has bred a host of judicially created exceptions (such as the partial performance and promissory estoppel doctrines) by which contracts supposed to be signed get enforced even though they are not.

*and unaltered from when I signed it ("**non-alteration**").* Identity, adoption and non-alteration are the elements of what in computer security jargon is called "non-repudiation."[3] Non-repudiation is what characterizes a document whose authenticity and integrity cannot credibly be denied by the person who "signed" it. Non-repudiation is the Holy Grail of transactional lawyers, and its existence a common object of controversy between adversary litigators. The predictability that it offers makes modern commerce possible.

As a practical matter, the only person really interested in a signature will be the person trying to use a signed document to impose some legal duty upon a signer who wants to repudiate the document. The ultimate test of such a trial is—a trial. The efficacy of a signature depends on whether or not it helps the proponent of the document to prove his case in a court or other tribunal. But a signature cannot help anyone if the signed document cannot be admitted into evidence. Accordingly, the principle problem of signatures—all signatures—is one of admissibility under the law of evidence.

Under existing rules of evidence, a signed document is not hearsay, and can be admitted into evidence if it is "authenticated." Under the Federal Rules of Evidence, to authenticate a document it is enough to present "evidence sufficient to support a finding that the matter in question is what its proponent claims."[4] "Whenever a signed instrument is introduced at trial, such as in a contract action, the authentication requirement must be met by proving that the party actually signed the instrument

---

[3] *See, generally*, Warwick Ford and Michael S. Baum, *Secure Electronic Commerce*, at 315-55 (1997).

[4] Fed. R. Evid. 901(a). State and common law evidence rules are similar.

involved."[5] But the actual signing of the document can be proved by circumstantial evidence, and the most common piece of circumstantial evidence that is used to authenticate a signed document is proof of the ownership of the signature. Thus, in order to admit a signed document in evidence, one need only prove the following:

a. Document is relevant.

b. Document bears a signature (or is handwritten.)

c. Signature (or handwriting) is that of the party or his agent.

d. Document is in the same condition now as when it was executed.[6]

Indeed, the Federal rules of Evidence expressly permit a signed document to be authenticated by the expert opinion of a graphologist, and even the non-expert opinion of an informed witness or the Court, that a handwriting *looks like* that of the party.[7]

Note that one need not prove that anyone actually *saw* the signer place his mark. But note also that the mere fact that a signature is on the document is *never* enough, even if the signature legibly names the party to be charged. There must always be a witness to testify that the signature is that of the party.

As you can see, there are two concepts at work here. One is the concept of ownership, which asks the question, "What human being owns this signature; whose mark is it?" The second concept is that of actual signing, which asks the more legally relevant question, "What human being actually signed this particular document?" When

---

[5] T.A. Mauet, *Fundamentals of Trial Techniques*, at 180 (2d ed. 1988).

[6] *Id*.

[7] *Id*.; Fed. R.Evid. 901(b)(1),(2),(3).

we deal with handwritten, or *holographic,* signatures, there is an implicit but very strong presumption that the person who owns the signature that appears on a document is the same person who actually signed the document at issue, that *ownership presumes signing*. Thus, documents are easily admissible not upon direct evidence of actual signing (which would only exist in those relatively rare cases when the document is signed in front of witnesses), but merely upon evidence that a signature belongs to a party. It is infinitely easier to establish to whom a signature belongs than it is to prove, in the absence of eye-witnesses, that the owner of the signature actually put pen to paper in any particular case.

The effect of this presumption does not end there. The act of signing, itself inferred from the ownership of the signature, goes on to provide strong circumstantial evidence that the signer intended to adopt the document as his own, and that it is complete. Any alteration in a signed document can, of course, be tested by scientific evidence, but all that, again like forgery of the signature itself, is a matter for the party seeking to repudiate the document to prove. Thus, in the absence of sufficient rebuttal evidence, once a party establishes who owns the signature appearing on a signed document, identity, adoption and non-alteration are all presumptively proved, and a legal determination of non-repudiation is not far away. At that point, we can say that a signature is *attributable* to the party and he or she is thereby legally bound by it (regardless whether, in the sense of absolute truth, he or she *really* signed it).

When dealing with holographic signatures, the presumption of actual signing from mere ownership is natural, supported by common sense as well as common law. We are instinctively comfortable with this presumption because holographic signatures

are of *biological origin*. By that I mean that the flesh-and-blood person who owns the signature actually, physically places it on the paper, as only he or she is capable of doing. The uniqueness with which each of us creates our signature is borne out by the experience of centuries, which has taught us that holographic signatures are very difficult to forge beyond expert detection. We believe them to be, and they generally are, reliable indicators of the act of the signer. We suffer little risk of injustice when we presume that the person whose signature appears on a document actually placed it there. The presumption allows us easily to attribute signatures to their owners, which has made resolution of commercial disputes relatively predictable, swift, and economical, so much so that hardly anyone bothers even to contest a holographic signature anymore. This has played no small part in the growth of commerce over the millennia.

Of course, a legally sufficient signature need not be a person's name, and need not be biological in origin. Common law is reflected in the UCC's provision that a signature may be "any symbol executed or adopted by a party with present intention to authenticate a writing."[8] When the disputed signature is not holographic, however, the implicit, natural, presumption that it was drawn by its owner weakens, and special problems arise.

[8] *See, e.g.*, N.Y. U.C.C. §1-201(39) (McKinney 1993).

II. The General Problem of Machine Signatures

Courtroom Vignette: The Case of the Rubber Signature

Plaintiff Counsel's Examination

Q: I show you what has been marked as Exhibit A for identification. Do you recognize that document?

A: Yes. This is our standard form customer agreement.

Q: Does this agreement bear a signature?

A: It bears a facsimile signature of Mr. Jones. It appears to be a rubber stamp facsimile of Mr. Jones's handwritten signature.

Q: Have you ever seen Mr. Jones's handwritten signature?

A: Yes. I have seen it on the letters he wrote to us complaining about his account.

Q: And does this facsimile signature look like Mr. Jones's handwritten signature?

A: Yes, they are alike.

Plaintiff Counsel: Your Honor, I offer Exhibit A.

Defense Counsel: Objection Your Honor. This witness has not testified that it was Mr. Jones who affixed the rubber stamp facsimile to the document. There is no foundation.

By the Court:

Q: Do you know how Mr. Jones came to have a rubber stamp facsimile of his signature?

A: No.

Q: Do you know who is authorized to use the rubber

stamp?
A: No.
Q: Do you know where Mr. Jones keeps the stamp?
A: No.
Q: Do you know for a fact that it was Mr. Jones who authorized the use of a rubber stamp facsimile on this document?
A: No.
The Court: The objection is sustained. The document cannot be authenticated through this witness. Move on.

The rubber stamp signature is an example of what I call a *machine signature.* It emanates not directly from the hand of the party, but from a machine or device that *can* be used by *anyone*. Other examples are digitized holographic signatures (created by running an exemplar through a scanner), inked "signatures" applied by a machine, even a typed version of one's name on a fax or an E-mail or the use of letterhead stationery or preprinted forms to denote the document's author.

The more people who have access to one's signing device, the weaker is the inference that a machine signature is the true act of its owner, and rarely are signing devices kept in extremely tight security. Since anybody can use the signing device, there is no inherent basis for presuming that its owner affixed it to the document in question, much less that he or she did so with the requisite present intent to authenticate that

document. Therefore, in the absence of legislation, one could seldom if ever authenticate a document merely by identifying the owner of the signing device. Some proof of the security surrounding the signing device will ordinarily be needed.[9]

To establish that the security of a signing device has not been compromised requires much more elaborate evidence than is needed to prove who owns a holographic signature. Indeed, it may be impossible to prove that the security of a signing device has *not* been compromised. If a co-worker "borrows" my rubber stamp, uses it to create a document against me, and puts the seal back without a trace, how can one prove either that it did or did not happen? Likewise, how can one prove that a computer file has or has not been copied by a hacker? Proof can require an extensive examination of evidence that may all be in the adversary's control. You might not be able to get the evidence you need, or it might be tampered with. One can in theory authenticate a document bearing machine signature, but it cannot be done as predictably, quickly or cheaply as with one bearing a holographic signature.

Unable to benefit from the presumption of attribution from mere ownership, machine signatures are more easily repudiated than holographic signatures. The problem of machine signatures is basic to what follows, for electronic and digital signatures are both fundamentally machine signatures.

---

[9] For commercial paper, including checks and other negotiable instruments, for which public policy dictates quick and efficient dispute resolution, the U.C.C. expressly provides the presumption that attributes machine signatures to their owners, leaving it to the putative signer to produce evidence that the use of the signing device was unauthorized. N.Y. U.C.C. §3-307 (McKinney 1993). There is, however, a responsibility on the owner of a machine signature to exercise due care to prevent it coming into unauthorized hands, and negligence on the owner's part will deprive him of the defense of claiming the signature is unauthorized. N.Y. U.C.C. §3-406 (McKinney 1993).

III. Terms and Technologies: Electronic Signatures Explained

Let us now enter the modern world of paperless communications. As we leave paper behind, we find persons exchanging information by means of some computer interface. The typical ways of communicating electronically are by E-mail and by entering data on the counter-party's website. How can such messages be “signed?”

Recall that anything can be a signature if it is intended authenticate a message. Thus, when you print your name at the bottom of an E-mail, you can be said to have “signed” it if you have the requisite intent. Similarly, even when you send an E-mail that has your return E-mail address on it as pre-programmed into your E-mail browser, you could be said to have signed the document, again if you had the requisite intent. Likewise, when you type information on to a web page template and press a button that says "submit" or "I agree," there is nothing in the law of evidence that prevents those acts from being deemed “signatures.” It all depends on the signer’s intent.

When we speak of electronic signatures, we are referring to all those acts, and any others, by which the identity of the person sending the message is transmitted in such a way that it is logically linked to the message. “Logically linked” means that the computer program that delivers the message also delivers the identity of the sender in the same or in a linked file. In other words, a computer process exists such that the message and the identity of the putative signer always go together.

Digital signatures, considered below, are a special form of electronic signature. But most electronic signatures are not digital signatures, and the treatment of electronic

signatures is broader and more extensive than the treatment of digital signatures alone.

IV. The Problem of Electronic Signatures, First Part

Courtroom Vignette: The Case of the E-mail

Examination by Plaintiff's Counsel

Q: Have you seen this document, Exhibit A, before?

A: Yes.

Q: What is this document?

A: This is a copy of an E-mail that I received, which I printed out from my computer.

Q: From whom did you receive this E-mail?

A: The return address indicates it came from Mr. Jones. It says "From: jones@acme.com," which I recognize as Mr. Jones's E-mail address.

Plaintiff's Counsel: Your Honor, I offer Exhibit A into evidence.

Defense Counsel: Your Honor, may I voir dire?

The Court: Go ahead.

Q: Mr. Smith, did Mr. Jones personally tell you he sent you this E-mail.

A: No.

Q: Did you see Mr. Jones prepare this E-mail?

A: Of course not.

Q: Do you know what computer generated this E-mail?

A: No, I do not.

Q: Do you know whether the text of this document was in any way altered since it was sent?
A: Not by me.
Q: But it could have been altered by someone else without your knowledge, isn’t that so?
A: I don't know.
Q: In fact, it is true, isn't it, that someone other that Mr. Jones could have sent you this E-mail.
A: I don't know.
Q: Do you have an E-mail browser?
A: Yes.
Q: Are you familiar with its operations?
A: Somewhat.
Q: Do you know how to set the mail server preferences?
A: Yes.
Q: Would it surprise you to learn that Mr. Jones's mail server is mail.acme.com?
A: No.
Q: It is common for E-mail servers to be so designated, right?
A: Yes.
Q: And you know that Mr. Jones's username is jones, right?
A: I would assume so, since that is his E-mail address.
Q: And would it surprise you if someone else in Mr., Jones's office knew his password?
A: No.

Q: Other people know your password, right?
A: Yes.
Q: You could set your E-mail browser to use mail.acme.com as the outgoing mail server, could you not?
A: Yes.
Q: And you could make “jones” the username on your browser, could you not?
A: Yes.
Q: And if you knew Mr. Jones's password, you could send E-mails through Mr. Jones's mail server, could you not?
A: Yes.
Q: And to a recipient, those E-mails would look just like those sent by Mr. Jones, wouldn't they?
A: Yes.
Q: So it is possible, isn't it, that this E-mail, Exhibit A, was not sent by Mr. Jones?
A: Yes, it's possible.
Q: And other than the addressee line on the E-mail, you have no way of knowing who actually did send it.
A: No.
Defense Counsel: Your Honor, I object to the document. This witness is in no position to testify that this E-mail came from Mr. Jones. No authentication.
Plaintiff Counsel: Your honor, people in the real world routinely rely upon the remittance identifiers

of E-mails to determine who sent them. Counsel posits an unusual situation in which someone deliberately forges an E-mail. That can happen with any communication, and there is no evidence that it happened here. That such a forgery could happen is not enough to prevent authentication. Rule 901 only requires some reasonable evidence that the E-mail came from Mr. Jones, and the identification placed on the E-mail by the sender's computer is sufficient.

Defense counsel: Your Honor, Rule 901 requires reliable evidence to establish authenticity, not just some evidence. Even with holographic signatures, it is not enough that a document be signed. Even there, some witness must testify whose signature it is. Here, this witness has said nothing more than that the E-mail had Mr. Jones's return address on it. I do not know of any case that permits even a signed document to be admitted on the testimony that it bears a return address, much less an E-mail whose sole clue to its sender is a return address. To say so is tantamount to saying that E-mails are self-authenticating, since all E-mails have return addresses. But Rule 902 specifies what documents are self-authenticating and E-mails are not on the list.

Also, as this witness well testified, E-mail return addresses are easily tampered with. Do you remember the "Lovebug" virus that circulated last

month? It was attached to E-mails sent without the owners' knowledge or consent. I received a half dozen of them myself, each one appearing to be an E-mail from a colleague, with that person's return address on it just like Mr. Jones's on Exhibit A. By counsel's logic, I could introduce each of those virus bearing E-mails against the return addressees, when they had nothing to do with them.

Plaintiff Counsel: Counsel makes a good point, but he overlooks that if his computer has been tampered with, Mr. Jones is in a better position to produce evidence of it than we are. Mr. Jones can always produce evidence that he did not author the E-mail.

Defense counsel: That is not so. Someone could have sent the E-mail using Mr. Jones's return address without Mr. Jones being aware of or able to prove any tampering with his computer. And anyway, since when do we require people to prove a negative, making Mr. Jones prove that he did not send an E-mail. Plaintiff has the burden of proof, both of producing evidence and persuading the jury that Mr. Jones sent the E-mail. That is why he is required to authenticate documents before they can be admitted. If he wants to admit Exhibit A to prove that Mr. Jones adopted the contents of that E-mail, he is going to have to come up with something more that Mr. Jones's return address on it to prove that Mr. Jones

authored it.

The Court: I have to agree with Defense Counsel. A mere return address on an E-mail is not sufficiently reliable to be a basis for authentication. Plaintiff will need to come up with some better evidence that Mr. Jones sent this E-mail. Objection sustained.

Last month's Lovebug virus dramatically showed the weakness of E-mails. Once launched, the virus began sending E-mails, all very legitimate looking, from the infected computer, with the owner being none the wiser. If some teenagers in the Philippines whom you have never met could get your computer to send out E-mails in your name, what do you suppose a disaffected employee or co-worker within your own company could do?

The point is that just because the E-mail says it came from you, does not necessarily mean it did. Accordingly, our judge is within his rights not to permit the E-mail into evidence without some other proof of its authorship besides the return address.[10] This is not to say that the E-mail can never be admitted; only that, like any other machine signature, it cannot be admitted as easily as a holographic signature.

The proponent faces the following practical problems:

First, unlike with a holographic signature, the evidence needed to authenticate will never be entirely within the proponent's control. Often, the proponent can himself

---

[10] *See Parma Tile Mosaic & Marble Co. v. Estate of Short*, 87 N.Y.2d 524, 663 N.E.2d 633 (1996).

recognize a handwritten signature. If not, he can obtain an authentic copy of a signature during discovery and authenticate the disputed signature by showing the two to an expert or just to the judge if they are sufficiently the same. Never can an E-mail be introduced with such ease.

Second, the authentication of an E-mail may depend upon evidence that is exclusively within the control of the opponent. It is possible to trace from neutral sources what computer network an E-mail came from, but generally not the machine itself. Even if the sender's server is a public Internet service provider, like AOL or Earthlink, all you will get is evidence of whose account was used to send the message. In either case, in the absence of witnesses, any proof that the sender of the E-mail was actually the person whose name appears on it will be exclusively within the putative signer's control. The availability and reliability of such evidence may be problematic.

If one goal of the legal system is to ensure the efficient and economical resolution of disputes, these kinds of problems in admitting E-mails into evidence cut right against it. E-mails are great tools for non-dispositive communications, but their convenience is counterbalanced by the insecurity and greatly increased legal expense they entail if one has to depend on them alone to resolve a dispute.

V. The Problem of Electronic Signatures-Second Part

Courtroom Vignette: The Case of the Click Wrap Agreement.

Plaintiff's Counsel's Examination:

Q: What is this document, Exhibit A?

A: This is a copy of our standard form customer agreement.
Q: Was this agreement delivered to Mr. Jones?
A: Yes, it was.
Q: How?
A: It resided on a page of our Website when Mr. Jones opened his account with us, and Mr. Jones accessed that page as part of the application process.
Q: How do you know that he did?
A: Our website is designed so that one cannot complete the application process without first viewing that page and clicking on a button that says "I accept and agree to the above terms" So, since Mr. Jones completed the application and submitted it, he had to have viewed this page and clicked that he agreed to its terms.
Q: Will you please describe the application process?
A: Yes. Upon visiting our website and navigating to the application page, the customer is required to fill in a template with such things as name, address, E-mail address, social security number, investment objective, investment experience, financial information, and so on. To complete the application, the customer must click on a button that says "continue." Clicking that button brings up the customer agreement page I just spoke of. clicking the "I Agree" button on the customer agreement page

brings the customer back to the sign in page, where a new button appears that says "Submit Application." If the Customer clicks that button, the application is submitted. All of this must be done during one session. If the customer leaves our website before completing the process, the entire process is canceled and the customer must reapply from the beginning when he or she signs on again. At the end of a completed session, the customer is given an account number and a temporary password.

Q: Is the account opened at that time?

A: No. We do not open accounts or accept orders for 48 hours. During that time, we send an E-mail to the customer's address to confirm the information received. If we receive no notice of any error, we open the account.

Q: Can the customer then begin trading?

A: In theory, yes. However, the customer first needs to know his permanent password. The temporary password cannot be used to make trades. We send a permanent password by mail to the address given to us. Included in the package is a copy of the account agreement, and certain required disclosures. The mailing is the only way a customer can get a permanent password, so if a customer uses the password by making an online trade, we know the mailing got to him. The permanent password must

first be activated by the customer, who logs on to our website, accesses a password verification page by using his temporary password. At that point, if there is money in the account, the customer can begin trading.

Q: Let me show you this document, Exhibit B. What is this document?

A: This is a copy of the sign-in page from our website, as completed by Mr. Jones. You can see there Mr. Jones's name and address and E-mail address and other information, all as typed in by the user.

Plaintiff's Counsel: Your Honor, I move exhibits A and B into evidence.

Defense Counsel: Your Honor, for what purpose are they offered?

Plaintiff's Counsel: To prove that Mr. Jones agreed to the terms of the customer agreement.

Defense Counsel: In that case, may I inquire?

The Court: Yes.

Q: Sir, can your system identify who specifically is accessing your site?

A: No. We can tell what computer network the inquirer is operating on, but not the person itself?

Q: And what system was used to make this communication?

A: America Online.

Q: And how many users does America Online have?

A: I don't know. Many millions, I think.

Q: So you do not have any direct knowledge that Mr. Jones actually logged on to your website, do you?
A: I know the information given to us, including Mr. Jones's E-mail address, to which we sent a confirming E-mail, and his address, to which we sent a permanent password that was thereafter activated and used.
Q: But it is true is it not, that all you know about the owner of this account is what has been told to you?
A: I would not agree with that. The verification procedures also tell us that the account was opened in the normal course. We know as much about the identity of Mr. Jones as we would had he personally signed a customer agreement.
Q: If he had personally signed a customer agreement, you would have a handwritten signature, would you not?
A: Yes.
Q: And if there was a dispute about who's signature it was, we could test that signature couldn't we?
A: I guess.
Q: We could compare it to other things the real Mr. Jones had signed, couldn't we?
A: Yes.
Q: We could have the signature analyzed by an expert?
A: Yes.
Q: We cannot do that here, can we?
A: Not in that way.
Q: Not in any way.

A: Well, you could see if Mr. Jones used the same E-mail address in other communications.

Q: Have you done so?

A: No.

Q: In fact, sir, you cannot testify of your own knowledge that it really was Mr. Jones who opened an online account with your firm, can you?

A: No.

Defense Counsel: Objection Your Honor. No foundation has been laid for these documents. This witness cannot testify conclusively that it was really Mr. Jones who agreed to the customer agreement. Also, your honor, I object because this document is not signed. Signed documents can be admitted into evidence if there is proof of the identity of the signer. But this document bears no signature. As such it is mere hearsay, and not admissible.

Plaintiff Counsel: Your honor, Counsel reads the signature requirement too strictly. At common law, and under the UCC, to be signed a document merely needed to bear a mark indicating assent to its terms, and the mark could be anything. In fact, if the whole document was handwritten, you don't need a signature at all. If a classic handwritten signature is relevant anywhere, it would only be with respect to a contract that falls within the statute of frauds, which requires documents to be subscribed,

that is signed at the bottom. Brokerage customer agreements are not within the Statute of Frauds.

The Court: Isn't there an NASD rule that requires customer agreements to be signed?

Plaintiff Counsel: Yes, but that is only a regulatory requirement of the NASD. It does not serve to invalidate agreements as a matter of contract law. It is not like a statute of frauds that requires agreements to be "subscribed." My point, Your Honor, is that the law is flexible enough as it stands to let a party's clicking an "I Accept" button on a computer be a mark signifying an intent to be bound to the same extent as a handwritten signature.

The Court: Counsel, I agree with you that clicking a button on a computer could be a signatory mark. However, under the law of evidence, to have such a document admitted against a party as a signed instrument, you still need to lay a foundation by competent evidence that the person who clicked the computer is the same person whom you seek to use the document against. Perhaps you can do so in this case, but you have not done so through this witness. The objection is sustained.

Click wrap agreements can generally be more reliable than E-mails, and might be

more easily admitted into evidence. They are better because (a) they rest control of more indicators of the signer's act within the hands of the proponent of the document, and (b) they generally create a series of security gates that collectively decrease the probability that an imposter acted in the place of the putative signer. In doing so, click wrap schemes set up a *"security procedure,"* whose use makes the signature more trustworthy.

Our example above is a close call. The website design ensures that the person who filled out the name and address was the same person who clicked the “I agree” button, and all that evidence is within the proponent's control. An E-mail confirmation was sent to the E-mail address given, and was not replied to, and all that evidence is within the company’s control. A real-life mail package was sent to the physical address given and was not returned as undeliverable, and the permanent password was activated and used, and all that evidence is within the proponent's control.

And yet, there is a missing link. There still is no direct proof that the person who entered all the information on the screen and used the account is the flesh and blood person who is sought to be held liable. An imposter could have logged on the website and given the information as well as clicked the “I Agree” button. Since the imposter provides the E-mail address to which the confirmation was sent, it is no surprise that a confirming E-mail to that address is not disputed. Since the imposter provides the mailing address to which the permanent password was mailed, it is no surprise that he received the package. A determined and not even that ingenious crook could accomplish all that with ease.

Still, one can argue that, in our example, the judge could have admitted the

evidence, and left it to the defense to rebut.[11] The defense could do so by proving, for example, that the defendant does not use the E-mail address given on the website, or that the address to which the confirmatory package was sent was not his, or that he was not near a computer when the website was accessed. But this is all problematic, and we generally do not require a defendant to disprove essential allegations of a case against him unless the contrary has already been established by the plaintiff.

And so again we face the classic problem of machine signatures: their use does not inherently prove the physical act of the real human being in whose name they are invoked. Although click wrap agreements might be admissible under existing law, I would not bet on doing so solely with evidence in the proponent's control. Even in the best of circumstances, resolution of a dispute over authentication of a click wrap agreement will be longer and costlier than it could have been had the agreement borne a simple holographic signature.

VI. Terms and Technologies: Digital Signatures Explained

Digital signatures are a special kind of electronic signature. Indeed, they are more a security device than a true signature.[12] Using sophisticated cryptography methods, a digital signature attempts to imbue electronic communications with as many of the attributes of non-repudiation as holographic signatures provide for paper documents.

---

[11] Indeed, several courts have held click wrap agreements enforceable. *See, e.g., Caspi v. the Microsoft Network and Microsoft Corporation,* 323 N.J. Super. 118, 732 A.2d 528 (1999), *Hotmail Corporation v. Van Money Pie, Inc., et al.,* 1998 U.S. Dist. LEXIS 10729, 47 U.S.P.Q.2d 1020 (1998).

[12] *See,* Illinois Electronic Commerce Security Act §5-105, definition of "Digital Signature," 5 Ill. Comp. Stat. 175/1-101 *et seq.* (1997 Illinois House Bill 3180).

In some respects, a digital signature provides even greater security than a holographic signature. Indeed, a digital signature is more akin to a handwritten document than to a traditionally signed one. More so than other electronic signatures, a digital signature cannot exist except in connection with a message. A digital signature is created out of the content of the message itself in a way that makes it unique not only to the signer but also to the message. To understand this, one must examine how digital signatures work.

Digital signature technology depends on two mathematical techniques. The first is called *asymmetric cryptography*, also known as *paired key encryption*. Using asymmetric cryptography, it is possible to create two mathematical values so related that, by using them in a properly designed algorithm,[13] each can be used to encode messages that can only be decoded by using the other. Such paired values, typically just unusually large prime numbers, are commonly called "keys," and the two paired keys comprise a *private key* and a *public key*. As the name implies, only I would possess my private key, while my public key can be freely distributed. One cannot[14] derive my private key from knowing my public key. By using my private key, I can encode a message and send it to

---

[13] An algorithm is just a fixed sequence of mathematical instruction designed to solve a problem. An algebraic formula is an algorithm. A computer program is the embodiment of one or more algorithms in a language of commands that a computer can follow. *See* "Algorithm," H. Newton, *Newton's Telecom Dictionary* (14th ed. 1998).

[14] When I use the terms "only," or "cannot" to describe what can or cannot be done with keys or hash functions, I risk the ire of technological purists. Because these are mathematical functions, there is always a theoretical possibility that a private key can be derived from a public key, or that two different messages will yield the same hash result (see below). However, the odds of those events happening are so remote (that is, it would take a supercomputer several hundred years to accomplish the task) that it is termed "computationally unfeasible." It is more likely that a forger will perfectly mimic your holographic signature than that someone will derive your private key from your public key. For practical purposes we will just say that it cannot be done, and leave it at that.

you; by using my public key, you (or anyone else) can decode my message. Since only my public key will decode a message encoded by my private key, you have some measure of confidence that it was really I who sent the message.[15]

The second is the development of mathematical algorithms that, when applied to a message, generate a fixed set of unintelligible characters unique to that and only that message. Such algorithms are called "hash functions," and their result is called a "hash result" or, in less whimsical terms, a "message digest."[16] A hash function provides a one-way trip. A hash result cannot be transformed back into the message from which it was generated.[17]

When we apply a digital signature to a document, we do nothing as simple as putting some electronic code at the end of the page. The process is two-stepped:

First, we run a hash function on the message to be sent to obtain a hash result.

Second, we encrypt the hash result with our private key.

The result would look something like this:[18]

---

[15] Using keys in this manner does not necessarily provide confidentiality, since anyone possessing my public key can decode my message. I can provide confidentiality by encoding the message using your public key, which you alone, holding your private key, will be able to decode, but then you will not know with certainty who sent it since it could have been sent by anyone having your public key.

[16] Several hash functions have been developed. In 1996, the then standard, MD5, betrayed certain weaknesses when it was almost broken by a German cryptographer. The one commonly used today, SHA-1 (Secure Hash Algorithm-1), a federal standard developed by the National Security Agency, is considered extremely well designed and secure. Network Associates, Inc., *PGP for Personal Privacy User's Guide (Version 5.5 for Windows 95/NT),* at 100-110 (1998).

[17] *See*, Illinois Electronic Commerce Security Act, §5-105, definition of "Message Digest Function," Comment 3.

[18] Shamelessly borrowed from Illinois Electronic Commerce Security Act §5-105, definition of "Digital

```
---------BEGIN SIGNATURE------
owHtWX1sU1UUP+91G+22ysbHhDHcBeZAvmq7L9iAuNJ2UuhX2soUs
paufVoftu8tby1kUXTGsGhAgsEBGNSELGpiNEFM5A80xIzEoPiPSE
iMRFbPfR/ajW7rlBjR/ZbfOeed9+5999177j3endS9CW/cI/qe3Df
lw45vOjb5zYvRmy2drFnZKT17a/97nTt11d8dNmyvqV12K7jt8Lxf
Vr9We2jHyk
--------END SIGNATURE-------
```

Then we send the original message, together with the encrypted hash result of that message that is the digital signature, to the intended recipient.[19]

The recipient runs the same hash function on the message he receives to obtain his own hash result. He then decrypts the second part of the message using the sender's public key to obtain the sender's hash result of the message. Since any message will yield only one unique hash result, if the hash result generated by the recipient matches that generated by the sender, then message received is *ipso facto* the message sent.

This technique can be, in theory, uncannily effective at providing all the necessary attributes of traditional signatures. Because the encrypted hash result can only be decrypted by a public key linked to the sender, one can establish the identity of the sender. Because only the same message can generate matching hash results, there is reliable evidence of non-alteration. And, because only by an overt concerted act of the

---

signature," Comment 4.

[19] The original message can also be encrypted using the encryption keys, but does not need to be in order to

sender can effect the process of generating, encrypting, appending and sending a hash result that comprises the digital signature, there is strong circumstantial evidence of adoption. The system is elegant and ingenious, appearing to solve all elements of the signature problem at once.[20]

But, for all that, digital signatures are still a kind of machine signature, with all the attendant problems of a machine signature, as we see below.

VI. The Problem of Digital Signatures

Courtroom Vignette: The Case of the Digital Signature

```
Examination by Plaintiff's Counsel
Q:    I show you what's been marked for identification as
      Exhibit A, and I ask if you can describe it.
A:    Yes.  It is a copy of a trading authorization
      received by our broker by E-mail, giving him
      discretion to execute trades in Mr. Jones's account.
      I personally printed it out from our E-mail server.
Q:    What is that at the bottom of the page?
```

---

be digitally signed.

[20] For a more detailed and technical treatment of digital signature theory, *see,* W. Ford & M.S. Baum, *Secure Electronic Commerce*, at 93-117 (1997); *Digital Signature Guidelines*, A.B.A Sec. Sci. & Tech., Information Security Comm., at 9-20 (1996); Network Associates, Inc., *PGP for Personal Privacy Users Guide (Version 5.5 for Windows 95/NT)*, at 95-132 (1998).

A: That is a computer-generated confirmation that the message was sent by Mr. Jones.
Q: Do you know how that confirmation is derived?
A: Yes I do. Attached to the E-mail that contained the authorization was a string of characters. The characters represent what's called a hash result, but encrypted by one of a pair of asymmetric encryption keys. The way those work, the sender used a private key to encrypt a hash result. We used Mr. Jones's public key, which we have on file, to decode the message and retrieve the hash result that was sent. We then ran our own hash function on the original message and compared our result to the one we decoded from the digital signature. If the two hash results match then our system reports back that the message is verified as having been sent by Mr. Jones. If the two hash results did not match, then either the message was not sent by Mr. Jones or the message content was altered in transit. Either way, the computer would reject the message as unverified.
Q: How do you know that Mr. Jones sent the message?
A: Because only a particular person's public key can decode a message encoded by that person's private key. The public key used to successfully decode the message to extract the correct hash result is registered to Mr. Jones. We have a notarized certificate from VeriSign, the company that issued

the pair of keys in question, attesting that Mr. Jones is the owner of the public key we used to recover the hash result.

Q: Do you know whether the E-mail was altered after it was sent?

A: My understanding is that it was not altered, because the hash result that was sent with the message matched the hash result that we generated ourselves from the message. Hash functions produce a unique hash result for any given message. If the message had been altered since it was sent, then our hash function would have yielded a different hash result, and there would have been no match with the one sent with the original E-mail. Because the two hash functions matched, we know that the message received was identical to the message sent.

Q: I show you what has been marked as Exhibit B for identification. What is that document?

A: This is an original certificate, duly signed and notarized, from VeriSign, certifying that the public key we used on this communication was duly issued by VeriSign to Mr. Jones, and had not been revoked as of the date of this E-mail.

Plaintiff Counsel: Your honor, I offer Exhibit B, the VeriSign certificate, in evidence to prove that the public key was registered to Mr. Jones.

Defense Counsel: Your honor, that certificate is clearly

hearsay, and it lacks foundation.

Plaintiff Counsel: Your honor, we can bring someone in from VeriSign to testify to the same thing if we have to. We are trying to save time. In any event, I think the existence of a notarial acknowledgement on this certificate classifies it as self-authenticating under Rule 902.

Defense Counsel: Your Honor I appreciate counsel's position. We don't want to waste the Court's time unnecessarily, so we will waive the hearsay objection.

The Court: Very well. Exhibit B is received.

Plaintiff Counsel: At this time, I offer Exhibit A, the trading authorization, into evidence.

Defense Counsel: What is the purpose of the offer?

Plaintiff Counsel: To prove that Mr. Jones gave the broker discretion to trade the account.

Defense Counsel: May I inquire, Your Honor?

Examination by Defense Counsel:

Q: Sir, do you have a pair of encryption keys issued to you?

A: Yes.

Q: How do you access your private key?

A: We use Microsoft Outlook as our E-mail program, and it has a function that permits me to attach a digital signature to a document.

Q: Do you use E-mail often?

A: Constantly.
Q: So Outlook is always on your desktop, isn't that right?
A: Yes.
Q: Do you need to enter a password every time you send an E-mail?
A: No.
Q: Do you need to enter a password every time you attach a digital signature to a document?
A: You can set up your browser to require that, but I do not. I do it so often that it just became cumbersome.
Q: Do you turn your computer off in the middle of the day?
A: Not usually.
Q: Do you have a password that you need to enter when you start your computer?
A: Yes.
Q: Do you travel much?
A: Fairly often.
Q: Who checks your E-mails when you are out of the office?
A: My secretary does.
Q: He has your password, isn't that so?
A: Yes.
Q: Do you know where your secretary keeps his copy of your password?

A: No.
Q: Are you sometimes out of your office during the day?
A: You mean for meetings in other people's office?
Q: That, or to go to lunch, or the men's room or for any other reason.
A: Yes, of course.
Q: And your computer is usually on during those time, is it not?
A: Yes.
Q: And Microsoft Outlook is on the desktop of your computer at those times, is it not?
A: Yes.
Q: And during those times when you are away from your office, anyone could enter your office and use your computer, isn't that right?
A: My secretary would spot such a person.
Q: Not if your secretary was also out to lunch, though.
A: No, not then.
Q: And if someone used your computer while you were out, that person could send a message on your E-mail system, isn't that so?
A: I suppose so.
Q: And that person could also attach your digital signature to a message, isn't that so?
A: I suppose so.
Q: Turning now to Mr. Jones, do you know where his private key is stored?

A: No.
Q: Do you know whether he, like you, keeps his computer on all day?
A: No.
Q: Do you know whether he, like you, has given his password to his secretary or someone else.
A: No.
Q: So for all you know, his secretary could have sent this message, isn't that right?
A: He or she could have.
Q: For all you know, the janitor could have sent this message, isn't that right?
A: It's possible.
Q: Indeed, from all the information available to you, you cannot say definitively that this communication came from Mr. Jones, can you.
A: I guess not.
Defense Counsel: Your Honor, it is clear that this witness cannot authenticate this communication. He cannot of his own knowledge say that Mr. Jones actually authorized the transmission of this E-mail. We do not dispute that it was encoded using Mr. Jones's public encryption key issued by VeriSign. But this witness cannot testify that Mr. Jones actually authorized the use of his key on this occasion. I object to the document.
Plaintiff Counsel: Your honor, a foundation for

admission of a signed instrument requires only some proof that the document was authored by the party to be charged. The way in which this document was received, digitally signed using Mr. Jones's public encryption key, is sufficient evidence that Mr. Jones sent it for purposes of authentication under Rule 901. Also, the matching hash result proves that the document was not altered in transit. This is the best we can do in authenticating an electronic communication like this.

The Court: Counselor, I appreciate it may be the best you can do, but I can see defense Counsel's point. All you have established is that the message was sent using Mr. Jones's encryption key, a fact which your adversary concedes. But you haven't established that Mr. Jones actually sent it. You might be able to do so if you can show that only Mr. Jones had access to his encryption key when message was sent, but you haven't done that yet. The objection is sustained.

This shows the Achilles' heel of the entire digital signature scheme. Digital signatures have two fundamental weaknesses that can be exploited by the unscrupulous, and which complicates the problem of using them as a basis for admitting documents into evidence.

1. Encryption keys, although unique, are not self identifying. Unlike Queequeg's

tattoo, encryption keys are not naturally linked to their owner, and so by themselves do not serve to prove the identity of their user.

2. Encryption keys are still machine signing devices. Even if you establish beyond dispute who owned the private key used to digitally sign a document, there still is no direct proof that person actually used that private key in the case at issue, and there is no natural basis for presuming that he did so.

A putative digital signatory could therefore deny that (a) he is the owner of the encryption key used, or (b) he used the key on the message sent. In denying either, he can repudiate the document.

Admittedly, the first problem is easily surmountable. A notarized document from the issuer of the key to the effect that the key was issued to Mr. Jones and has not been revoked is admissible as a self-authenticating document under Federal Rule of Evidence 902 and comparable state rules. Proving the ownership of encryption keys is the purpose of the development of a ***Public-Key Infrastructure*** ("PKI").

PKI is built on the activities of private or public organizations, such as VeriSign, Inc., referred to in the above example, which would undertake to generate key-pairs for subscribers and also certify to third parties, either directly or by reposing a public-key in a publicly available repository, that any particular public key is part of a key-pair issued to a named subscriber and still is in effect. Such organizations are called generically ***Certification Authorities***, and the issuance of ***Certificates*** as to the ownership of keys is their pivotal role in a PKI.[21] The credibility of a certificate issued by any Certification

[21] In order to shorten the dialogue in the above vignette, the nature of the certificate offered is suggested to

Authority ultimately depends on how securely the Authority does its job, including how much physical security surrounds its computers, what protocols it follows in issuing and certifying keys, the nature and limitations of its employees, and generally how difficult it would be for someone to cause a false certificate to be issued. The sum total of all of those factors is encompassed in the word "***Trustworthy***," which is also used in the literature to describe security procedures. In short, the more Trustworthy are the processes of a security procedure or of a Certification Authority, the more reliable will be deemed the result of the procedure or the certificate of the Authority. How a Certification Authority maintains its security, upon which a determination of Trustworthiness may be made, is usually described in a document called a ***Certification Practice Statement*** ("CPS"). VeriSign's CPS runs almost 100 pages.[22]

Within the limits of Trustworthiness as documented in its CPS, a Certification Authority can identify the owner of a digital signature with even greater reliability than even an expert can identify the owner of a holographic signature. One *can* establish with relative ease and certainty whose key created any digital signature.[23]

---

be a paper document. In actuality, certificates generally are themselves electronic documents, and they are digitally signed by the Certification Authority so as to ensure non-alteration of the content of the certificate. See Illinois Electronic Commerce Security Act §5-105, definition of "Certificate," at Comment 3 (5 Ill. Comp. Stat. 175/1-101 *et seq.* (1997 Illinois House Bill 3180)). Who, you may ask, certifies the digital signature of the Certification Authority? This raises a whole other subject, that of Certification Paths and Hierarchies, also an important part of PKI, which I will leave for another day. For those really interested, see, W. Ford & M.S. Baum, *Secure Electronic Commerce*, at 193-314 (1997).

[22] *See, VeriSign CPS (Certification Practice Statement, Version 1.2),* (May 15, 1997), available at http://www.verisign.com.

[23] There is an interesting idea being studied to further strengthen the link between a key pair and a person, and that is the "CyberNotary." A CyberNotary would be an attorney who actually undertakes the identification, through normal means, of a person applying for an encryption key pair, and then certifies that identity to the authority issuing the keys. For high level security, a CyberNotary could also perform background and financial responsibility checks. See, T.S. Barassi, *The CyberNotary: Public Key*

But the second problem, that of ensuring that only the putative signer actually used his encryption key on the occasion in question, is not nearly so tractable, for the reasons that plague all machine signatures. This leaves the law in a quandary. If digital signatures, with their elegant ability to ensure the identity of the sender and the integrity of the document, might not be enough to sufficiently authenticate documents under the rules of evidence, then the goal of contracting entirely on-line remains elusive.

VIII. The Trouble with Electronic and Digital Signature Legislation

Enter the national and international movement towards the drafting and enacting of electronic and digital signature legislation, which we can now survey from a vantage point informed by the problems of admissibility highlighted above.

Most states have enacted some legislation concerning the legal effect of electronic and digital signatures.[24] Several bills have been introduced in Congress over the past few years, though only legislation authorizing electronic filing of certain documents have been signed into law. In addition, model laws and guidelines have been considered and adopted by such diverse groups as the American Bar Association,[25] The National

---

Registration and Certification and Authentication of International Legal Transactions (ABA Science & Techn. Section, Information Security Comm., http://www.abanet.org/scitech/ec/cn/cybernot.html).

[24] As of early this year, only Massachusetts, Michigan, New Jersey, South Dakota and Vermont had not enacted any laws dealing with electronic and digital signatures. Alabama only permits electronic filing of tax returns, but does not use the term "electronic signature."

[25] *See*, American Bar Association, Information Security Committee, Electronic Commerce and Information Technology Division, Section of Science and Technology, *Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce* (August 1, 1996).

Conference of Commissioners on Uniform State Laws,[26] the United Nations,[27] the European Community,[28] and the International Chamber of Commerce.[29] To survey these scores of laws and would-be laws is to be struck by the variety of ways considered to deal with the issues.

In broad terms, the legislative ideas coalesce around three strategies.[30]

A. Authorizing electronic signatures for specific types of documents.

This is the simplest type of legislation. A number of states have authorized the use of electronic or digital signatures only for specific purposes, usually to make governmental filings or to communicate with public agencies. Such statutes permit state agencies to use electronic or digital signatures when communicating with each other or when filing state records (*e.g.*, Delaware,[31] Maryland,[32] Rhode Island[33]) and permit

---

[26] *See*, National Conference of Commissioners on Uniform State Laws, *Uniform Electronic Transactions Act* (1999).

[27] *See*, United Nations Commission on International Trade Law (UNCITRAL), *Model Law on Electronic Commerce* (December, 1996).

[28] *See*, Christopher Kuner, *Draft Convention on the Mutual Recognition of Digital and Electronic Signatures*, at http://www.mbc.com/ecommerce/legis/convention-kuner.html.

[29] *See*, International Chamber of Commerce World Business Organization, *General Usage for International Digitally Ensured Commerce (GUIDEC)* at http://www.iccwbo.org/home/guidec/guidec.asp.

[30] Most if not all existing and proposed legislation on electronic and digital signatures, as well as the leading government and private sector initiatives, are well collected and catalogued in the website of the Chicago law firm McBride Baker & Coles at http://www.mbc.com/ecommerce. The McBride website should be the first stop for anyone doing serious research into the existing state of electronic and digital signature legislation. I acknowledge my reliance on their efforts, and I do not intend here to duplicate them.

[31] *See*, Del. Code. Ann. Tit. 29, §§. 2706(a), 5942(a).

[32] *See*, Maryland Digital Signature Pilot Program, 1998 Md. Laws 482 (1998 Md. House Bill 523).

[33] *See*, Rhode Island Electronic Signatures and Records Act, General Laws of Rhode Island Annotated §42-127-1 *et. Seq.* (1997 RI House Bill 6118).

acceptance of such signatures in public filings by members of the public (*e.g.*, New Mexico[34]), in documents filed with state agencies (*e.g.*, Arizona,[35] Idaho,[36] Indiana,[37] Maine,[38] Montana,[39] Nevada,[40] North Carolina,[41] North Dakota,[42] Texas,[43] and Wyoming[44]), or in court filings (*e.g.*, Hawaii[45]). A few states have given the green light to use electronic and digital signatures in maintaining medical records and in transmitting health care authorizations (*e.g.*, Connecticut,[46] Louisiana,[47] and Ohio[48]). Usually any

---

[34] *See,* Electronic Authentication of Documents Act New Mexico Statutes Annotated § 14-15-1 *et seq.* (1996 NM House Bill 516); 1999 NM Senate Bill 146.

[35] *See,* Ariz. Rev. Stat. Ann. § 41-121; 1998 AZ House Bill 2518 (Amends Ariz. Rev. Stat. Ann. § 41-121 and § 41-132).

[36] *See,* Idaho Electronic Signature and Filing Act (1998 ID Senate Bill 1496); Idaho Code § 3-1-140 (1997) (1997 ID House Bill 221).

[37] *See,* Electronic Digital Signature Act – West's Ann. Indiana Code Title 5, Art. 24 (1997 IN Senate Bill 5a, 1997 IN House Bill 1945).

[38] *See,* Maine Revised Statutes Annotated, Title 29-A, Chapter 11, Subchapter IV, §§ 1401, 1405, and 1410 (1997 ME Senate Bill 473).

[39] *See,* Montana Code Annotated §§ 2-15-401 and 2-15-404 (1997 MT House Bill 468).

[40] *See,* 1997 NV SB 42; Nevada Revised Statutes Title 14 § 171.103 (1997 NV AB 386).

[41] *See,* 1997 NC House Bill 1356.

[42] *See,* 1997 ND Senate Bill 2071.

[43] *See,* Tex. Bus. & Com. Code § 2.108 (1998 TX House Bill 984); Tex. Gov't Code § 403.027 (1997 TX Senate Bill 645); Tex. Transp. Code § 201.931 (1997 TX Senate Bill 370).

[44] *See,* Wyoming Statutes § 9-1-3069-1-306.

[45] *See,* Hawaii Revised Statutes Annotated Title 14 § 231-8.5 (1995 HI Senate Bill 2401).

[46] *See,* Conn. Gen. Statutes § 19a-25a (1997).

[47] *See,* West's Louisiana Revised Statutes Annotated §40:2144 (1995); West's Louisiana Revised Statutes Annotated §40:32 (1998) (1997 LA House Bill 1605); West's Louisiana Revised Statutes Annotated § 40:2145 (1998) (1997 LA Senate Bill 609); West's Louisiana Revised Statutes Annotated §13.3733.1 (1997 LA House Bill 294).

[48] *See,* Ohio Revised Code Annotated § 3701.75 (1997 OH House Bill 243).

kind of electronic signature is permitted, but some require certain authentication attributes (Idaho and Maryland) and others accept digital signatures only for some or all purposes (Indiana, New Mexico).[49]

The impetus here is not so much to foster electronic commerce, but to ease the burden of paperwork faced by government and quasi-governmental agencies and the taxpayers who deal with them. Usually the permission to use electronic signatures in governmental filings is the tail wagging the dog, that being the computerization of state records. Unless the state has converted its own records to electronic form, the acceptance of electronically signed documents makes no sense. These statutes should be seen, therefore, as efforts by the state to discourage the use of paper in the state's own governmental processes. From an evidentiary point of view, a duly certified state document will be deemed self-authenticating and admissible, but only to the extent of the purpose of the public filing. These statutes will not of themselves foster the wide-scale use of electronic signatures.

B. Recognizing the Legal Validity of Electronic Signatures.

The next level of legislation includes those statutes that attempt to give equal legal effect to electronic signatures, but without directly solving the evidentiary problems raised by them. The text of the Uniform Electronic Transactions Act ("UETA") is

[49] In reading all existing legislation, one must take care to review the definitions. Some statutes use the term "digital signature," but define it in such a way that any electronic signature would fit the definition. Generally, "electronic signature" could be defined as anything from a simple electronic signature as we have used the term, to such a signature with specific authentication attributes, to a full digital signature using encryption keys.

typical: "If a law requires a signature, an electronic signature satisfies the law."[50] The UETA has already been adopted by some states,[51] and may well be on the books in many others before too long, so it is worth looking at. Statutes with similar effect have already been enacted in other states.[52] Most states now appear to grant equivalency with holographic signatures only to digital signatures or electronic signatures that have other specified indicia of reliability similar to those of digital signatures.[53] That may become

---

[50] UETA §7(d), (1999). The definition of "electronic signature" follows the UCC formulation: "an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record." *Id*., §2(8).

[51] **California**: *see*, The Uniform Electronic Transactions Act: California Civil Code (adding Title 2.5 (commencing with §1633.1) to Part 2 of Division 3) and California Financial Code (amending §18608) (1999 CA Senate Bill 820); California Civil Code (adding §1633) (1999 CA Senate Bill 1124); 1997 CA AB 521; 1997 CA AB 721 (amends §§25003, 25100, 25101, 25110, 25120, 25130, 25161, 25164, 25165, 25203, 25216, 25230, 25234, 25237, 25240, 25241, 25245, 25300, 25301, 25532, 25608, 25612.5 and 25619 of Title 4 of the Corporations Code, relating to securities; Online Disclosure Act of 1997; Title 9 Political Reform, Chapter 4.6, §84600 *et seq.* (1997 CA Senate Bill 49); 1995 CA AB 2755 (amends §§102370, 102875, 103535, 102875, 103535, and 103641 of the Health and Safety Code, relating to vital statistics.); CA Government Code § 16.5 (1995 CA AB 1577). **Pennsylvania**: The Electronic Transactions Act (Pennsylvania Consolidated Statutes, Titles 12 and 18) (1999 PA Senate Bill 555); 1997 PA Senate Bill 1385.

[52] **Florida**: Amends Fla. Stat. § 117.20 (1997 FL House Bill 1125); Electronic Signature Act of 1996 – Fla. Stat. § 282.70 *et seq.* (1997), (1996 FL Senate Bill 942); Fla. Stat. § 117.20 (1997) 1997 FL House Bill 1413. **Georgia**: Georgia Electronic Records and Signatures Act O.C.G.A. §10-12-3 (1998) (1997 GA Senate Bill 103); 1997 GA Senate Bill 433 (amends Georgia Electronic Records and Signatures Act O.C.G.A. §10-12-3 (1998) and Information Technology Policy Act O.C.G.A. §59-29-12 (1998); Amends Title 40, Motor Vehicle and Traffic of the Georgia Code (1997 GA House Bill 487); O.C.G.A. §48-2-32 (1998) (1997 GA House Bill 479); O.C.G.A. §16-9-121 (1998) (1997 GA House Bill 513); 1999 GA Senate Bill 62). **Oregon**: Electronic Signature Act, Oregon Revised Statutes §192.825 *et seq.* (1997 OR House Bill 3046); Oregon Revised Statutes §709.335 (1997 OR Senate Bill 125). **Tennessee**, 1997 TN Senate Bill 525; Tennesee Code Annotated §16-1-115 (1997 TN House Bill 1718). **Virginia**, Va. Code. Ann. §§59.1-467 to 469 (1997 VA Senate Bill 923); 1998 VA Senate Bill 153; 1998 VA House Bill 794 (amends §17-83.1.4 and creates §17.1-258); 1998 VA Senate Bill 808; 1998 VA Senate Bill 819. **West Virginia**, 1998 WV House Bill 4293; WV Code §30-3-13; and **Wisconsin**, 1997 WI AB 811; 1997 WI AB 100.

[53] **Alaska**, 1997 AK Senate Bill 232; **Arkansas**, The Information Network of Arkansas (1999 AR Senate Bill 378); 1999 AR House Bill 1167. **Colorado**, Colorado Revised Statutes, adding 24-71.1, amending 24-71-101, 24-30-1604(1) and (1)(b), adding 13-25-134, 22-32-110(1)(kk), 30-11-107(1)(gg), 31-15-201(1)(h), and 32-1-1001(1)(o) (1999 CO House Bill 1337); Colorado Revised Statutes, adding 24-71-101, amending 24-30-1603, 24-30-1604(1) and (1)(b), 4-9-413, 4-9-404(1), 4-9-405(2) and 4-9-406 (1999 CO House Bill 1079); Colorado Revised Statutes, adding 24-37.5, repealing 24-1-128(7)(m), amending 16-

less restrictive as more states adopt the UETA.

These provisions directly affect substantive law. Their effect is to make electronic signatures as good as holographic signatures, *whenever the law requires a signature*. As we have said, however, the law rarely requires a signature, so these provisions are usually of limited applicability in general commercial or securities matters.

These types of statutes generally also contain a provision stating that electronic signatures otherwise admissible will not be denied admissibility solely because they are electronic.[54] This is a logical procedural counterpart to the substantive recognition of electronic signatures. Surely, if an electronic signature is recognized as a legal "signature," then the state's courts should not exclude such signatures from evidence just because they are electronic.

Such statutory provisions are a necessary first step in dealing with electronic signatures, but they tend to gild the lily, solving a problem that, given the common law's widely sweeping definition of what may be considered a signature, probably does not

---

20.5-102(2.3), and repealing and relocating 24-30-17 to 24-37.5 (1999 CO House Bill 1372); Department of Health Care Policy and Financing Staff Manual, Volume 8: Medical Assistance Agreements 8.130-8.130.8 (state rules concerning Medicaid); C.R.S. 4-9-413 (1997); 1997 CO Senate Bill 155. **Kansas**, Kansas Digital Signatures Act – Kansas Statutes Annotated §60-2616 (1997 KA House Bill 2059). **Kentucky**, 1998 KY House Bill 708; 1998 KY Senate Bill 390. **Mississippi,** Digital Signatures Act of 1997, Miss. Code 1972 Ann. §25-63-1 *et seq.* (1997) (1997 MS House Bill 752); 1997 MS House Bill 1314 (amending Title 79. Corporations, Associations and Partnerships – Chapter 4. Mississippi Business Corporation Act; chapter 11. Nonprofit, Nonshare Corporations and Religious Societies; Chapter 12. Partnerships; Chapter 14. Mississippi Limited Partnership Act; and Chapter 29. Mississippi Limited Liability Company Act. **New Hampshire**, 1997 NH House Bill 290; 1997 NH Senate Bill 472; New Hampshire Digital Signature Act – RSA 294-D:1 *et seq.* (1997 NH Senate Bill 207). **Nebraska**, 1997 NB LB 924; The Geologists Regulation Act (1997 NB LB 1161); Nebraska Revised Statutes §81-3437 (1997 NB LB 622). **New York**, Chapter 57A of the Consolodated Laws: The State Technology Law (includes Article I: the Electronic Signatures and Records Act) (1999 NY Senate Bill 6113). **Oklahoma**, 1997 OK House Bill 3287; **Rhode Island**, Rhode Island Electronic Signatures and Records Act, General Laws of Rhode Island Annotated §42-127-1 *et seq.* (1997 RI House Bill 6118).

[54] *See* UETA §13 ("evidence of…signature may not be excluded solely because it is in electronic form").

even exist. If any mark can be a "signature" under common law, then it is hard to see why the creation of an electronic mark would not be considered such a signature, and if it is so considered, why a court would exclude it from evidence solely because it is in electronic form. Certainly, I am aware of no cases that have so held. The common law has never been as inflexible as these provisions suggest. Yet the elimination of any bias against electronic formats is the sole purpose of these provisions.[55]

These recognition statutes generally say little about how electronic signatures will be received in evidence. The UETA, for example, touches obliquely upon the subject of authentication by stating that "An electronic . . . signature is attributable to a person if it was the act of the person."[56] Thus, under the UETA, electronic signatures have no practical meaning unless one first proves they are the act of the party sought to be charged. One can make the showing "in any manner, including a showing of the efficacy of any security procedure applied to determine the person to which the . . . electronic signature was attributable."[57] "Security procedure" is defined to include any method used to verify that an electronic signature belongs to a person, including but not requiring the use of encryption keys and hash functions.[58] Under the UETA, therefore, the use of a digital signature using an encryption key owned by a person can be circumstantial evidence that the digitally signed document is "the act" of that person. This does not change existing law at all. Whether such evidence will be enough in any given case to

---

[55] *Id*. §7, Comment 1.

[56] UETA, §9(a).

[57] *Id*.

sufficiently attribute the document to the owner of the encryption key used to create the signature for purposes of authentication is open to question. Regardless, to a litigator it sounds like a lot of work, and an expensive task.

Showing that a signature is the act of a person is the very problem that the common law presumption of attribution from mere ownership so neatly solves for holographic signatures. No such easy solution exists for electronic signatures under the recognition statutes.

C. *Affording Evidentiary Presumptions to Digital Signatures.*

The third category of legislation, however, actually changes existing law by providing that, under certain circumstances, a digital signature is *presumed* to have been affixed by the owner of the encryption key used to create it. Such a presumption gives to digital signatures exactly the same evidentiary advantage that holographic signatures have always enjoyed. But while no one feels uncomfortable when that presumption is applied to holographic signatures, creating such a presumption for digital signatures makes us queasy, and properly so. The statutes that provide such a presumption reflect that disquiet, for they adorn the grant with qualifications, collateral obligations and conditions.

There is scant uniformity in the legislation. Recently enacted digital signature statutes in Minnesota, Illinois and Pennsylvania illustrate three variant approaches to the problem.

---

[58] UETA, §2(14).

The Minnesota Electronic Authentication Act[59]

This is among the most straightforward attempts to make digital signatures as useful as holographic signatures. It deals specifically with digital signatures created using key pairs and hash functions. Similar statutes have been enacted with minor variations in Missouri,[60] Utah,[61] and Washington.[62]

The architecture of the Minnesota Act is easy to follow. The Act provides first for the regulation of Certification Authorities.[63] Then the act regulates and imposes duties upon both the issuer and the recipient of encryption keys issued or certified by such Certification Authorities.[64] Finally, the act describes the consequences of using such certificated keys.[65] All in all, the statute is concise and well organized. Its strength, however, is also its limitation. Since it is specifically crafted for existing digital signature technology, it will need to be amended or augmented as newer technologies become available.

The provisions relating to the licensure and regulation of Certification Authorities are intended to ensure that any entities issuing and certifying encryption key pairs operate

---

[59] Minnesota Electronic Authentication Act (Minn. Stat. Anno. §325K *et seq.*

[60] Missouri Digital Signature Act (1998 MO Senate Bill 680), 1998 MO Senate Bill 844, Vernon's Annotated Missouri Statutes §130.57 (1997 MO Senate Bill 16).

[61] Utah Digital Signature Act (Utah Code Ann. §46-3-101 *et seq.*); Utah Stat. Ann. §46-1-16 (1998 UT Senate Bill 107); 1996 Utah Senate Bill 73; 1996 Utah Senate Bill 188; 1998 Utah Senate Bill 1.

[62] Washington Electronic Authentication Act (Chapter 19.34 RCW).

[63] Minnesota Electronic Authentication Act at Minn. Stat. Ann. §325K.05-09.

[64] *Id*. at §325K.10-18.

[65] Minnesota Electronic Authentication Act, Minn. Stat. Ann. at §§325K.10-19-25.

sufficiently secure facilities and processes to obviate any concern that issued keys can be compromised at their source. This obviously is a necessary first step to ensuring reliably that only the owner of a key pair can create a digital signature using those keys. Only keys certificated by licensed Certification Authorities are entitled to the act's benefit.

The basic requirement of a licensed Certification Authority is that it use a "trustworthy system" in its operations and disclose its CPS.[66] In issuing certificates, a Certification Authority must confirm the identity of the key-holder and the accuracy and effectiveness of the key pair issued.[67] A Certification Authority makes certain statutory warranties to subscribers and third parties who reasonably rely on its certificates, which makes it liable as a sort of guarantor of a certificate's accuracy.[68] This reflects the core role of Certification Authorities in maintaining the PKI upon which public reliance on digital signatures must rest. The Act imposes upon licensed Certification Authorities the onus of making sure that their certificates are reliable.

Having established a framework for PKI, the Act then imposes duties on the users of certificated encryption keys. By accepting a certificate, a user warrants its accuracy to all who reasonably rely on it. If the subscriber is an agent (like an officer of a corporation), he or she warrants that he or she has the authority to sign on behalf of the principal. The subscriber further agrees to indemnify the Certification Authority for any

---

[66] *Id*. at §325K.09. "Trustworthy system" is defined as computer systems that "are reasonably secure from intrusion and misuse; . . provide a reasonable level of availability, reliability, and . . . are reasonably suited to performing their intended functions." *Id*. at §325K.01(39). This accords with our discussion of Trustworthiness above.

[67] *Id*. at §325K-10.

[68] *Id*. at §325K-11.

losses incurred by the Authority to third parties relying on a certificate issued on the basis of information fraudulently supplied by the subscriber.[69] In addition, the holder of a certificate "assumes a duty to exercise reasonable care to retain control of the private key and prevent its disclosure to a person not authorized to create the subscriber's digital signature."[70] What consequences flow from a failure to do so is not said.

The benefits of complying with these strictures attendant to issuing and accepting certificates are several, but not unlimited. The Act recognizes certificated digital signatures as equal to holographic signatures "where the law requires a signature," but only if no affected party objects to it by refusing to accept it, if it is established that "the digital signature was affixed by the signer with the intention of signing the message and after the signer has had an opportunity to review items being signed," and if the recipient has no notice that the signer breached some duty as a subscriber or is not entitled to use the private key that created the signature.[71] As noted above, this only affects documents required by law to be signed, which are relatively few.

For other signed documents, the benefits are greater. Although the recipient of a digital signature must be reasonable in his reliance thereon (and assumes the risk of forgery if he is not[72]), a message that bears a validly certificated digital signature is "as

---

[69] Minnesota Electronic Authentication Act, Minn. Stat. Ann. at §325K.12.

[70] *Id*. at §325K.13.

[71] Minnesota Electronic Authentication Act, Minn. Stat. Ann. at §325K.19.

[72] *Id*. at §325K.20.

valid, enforceable, and effective as if it had been written on paper. . . ."[73] But what really gives the Act its force is its presumptions:

> In adjudicating a dispute involving a digital signature, a court of this state presumes that:
>
> * * *
>
> (c) If a digital signature is verified by the public key listed in a valid certificate issued by a licensed certification authority:
>
> (1) that digital signature is the digital signature of the subscriber listed in that certificate;
>
> (2) that digital signature was affixed by the subscriber with the intention of signing the message; and
>
> (3) the recipient of that digital signature has no knowledge or notice that the signer:
>
> (i) breached a duty as a subscriber; or
>
> (ii) does not rightfully hold the private key used to affix the digital signature.[74]

Thus, the Act creates for digital signatures exactly what common sense and law provides for holographic signatures, a presumption that the owner of the signature is the same person who affixed the signature on the document in question. Unlike with holographic signatures, this presumption does not apply to every situation. But for users of certificated key-pairs, the Act makes digital signatures fully the equals of holographic signatures.

---

[73] Minnesota Electronic Authentication Act, Minn. Stat. Ann. at §325K.21.

[74] Minnesota Electronic Authentication Act, Minn. Stat. Ann. at §325K.24(1)

The Illinois Electronic Commerce Security Act[75]

The Illinois statute is more comprehensive than the Minnesota Act, and is intended to provide a flexible framework for facilitating commerce by electronic means, without regard to what technology is used. While largely a recognition statute,[76] it does "provide enhanced evidentiary presumptions designed to give legal assurances to persons engaged in electronic commerce that their transaction documents will be provable and enforceable."[77] It has been well received and has been used as a model by the drafters of the UETA and by UNCITRAL in promulgating its Uniform Rules on Electronic Signatures, and is being considered for adoption by other states. Similar statutes are on the books in Iowa[78] and South Carolina.[79] It has broad similarities to the Minnesota Act, but also important differences.

The key difference is that where Minnesota rests its structure on the licensure of Certification Authorities, Illinois instead rests its on the concept of a "qualified security procedure." Security procedures are any method or procedure used to verify the identity of the creator of an electronic record or signature, and that the record has not been altered since its creation.[80] Security procedures become "qualified" if the parties agree to them

---

[75] Illinois Electronic Commerce Security Act; 5 Ill. Comp. Stat. 175/1-101 *et seq.* (1997 Illinois House Bill 3180).

[76] *See, id.* at §§5-110, 5-115, 5-120, 5-125, and 5-130.

[77] *Id*. at §1-102, Comments.

[78] Iowa Electronic Commerce Security Act (1999 Iowa HF 624).

[79] South Carolina Electronic Commerce Act (1997 SC Senate Bill 1167).

[80] Illinois Electronic Commerce Security Act §5-105, definition of "Security procedure," 5 Ill. Comp. Stat. 175/1-101 *et seq.* (1997 Illinois House Bill 3180).

or, in the absence of agreement, if the Illinois Secretary of State certifies them as being qualified.[81] In doing so, however, the Secretary's role is only to ascertain whether the scientific community has evaluated and determined that a given security procedure is capable of verifying the creator and non-alteration of a record in a "trustworthy manner."[82] In this way, Illinois opts for flexibility. Existing digital signature technology clearly would be a qualified security procedure, but any new methods that come in the future will also qualify if the scientific community finds them Trustworthy.

Any electronic signature verified by a qualified security procedure as being the signature of a specific person is deemed a "secure electronic signature," if the security procedure was "commercially reasonable under the circumstances, . . . applied by the relying party in a trustworthy manner, and . . . reasonably and in good faith relied upon by the relying party."[83] Once given the status of secure electronic signature, the presumption attaches: "In resolving a civil dispute involving a secure electronic signature, it shall be rebuttably presumed that the secure electronic signature is the signature of the person to whom it correlates."[84] Since signature is defined as a mark made with intent to authenticate, the presumption would have the effect of authenticating a document by proving the secure electronic signature.[85] And a strong presumption it is,

---

[81] *Id*. at §10-110(b).

[82] *Id*. at §10-135. "Trustworthy manner" has much the same meaning as in Minnesota. *See, id*, at. §5-105, "Trustworthy manner."

[83] Illinois Electronic Commerce Security Act §10-110(a), 5 Ill. Comp. Stat. 175/1-101 *et seq.* (1997 Illinois House Bill 3180).

[84] *Id*. at 10-120(b).

[85] *Id*. at §5-105 definition of "sign or signature."

too, shifting both the burden of producing evidence and the burden of persuasion to the opponent of the signature to show that the secure electronic signature was not authorized.[86]

Certification Authorities are not entirely ignored. The Act has an entire article devoted to digital signatures, but digital signatures are used in support of secure electronic signatures, not as the main event. Thus, the Act provides that a digital signature created by an encryption algorithm certified by the secretary of state shall be deemed a qualified security procedure for purposes of finding that an electronic signature is a "secure electronic signature," but only if it was created during the operational period of a certificate, and the certificate itself is "trustworthy" because either it was issued in accordance with rules and standard to be promulgated by the Secretary, or is otherwise found to be by a court.[87] There are the expected prohibitions against issuing certificates known to be false,[88] but no wholesale regulation of Certification Authorities beyond establishing criteria to measure when certificates should be considered sufficiently trustworthy to merit the heightened presumption. In fact, the Act's commentary expressly rejects regulation for any other purpose (such as quality control or revenue generation).[89]

Where Minnesota dealt narrowly with digital signatures created under existing technology, Illinois deals instead with security concepts that can be met by any

---

[86] *Id*. at §10-120(c) and Comment 3.

[87] Illinois Electronic Commerce Security Act §§15-105 and 15-115, 5 Ill. Comp. Stat. 175/1-101 *et seq.* (1997 Illinois House Bill 3180).

[88] *Id*. at §15-205.

[89] *Id*. §15-115, Comment 2.

technology. The availability of certificates makes digital signatures easily encompassed in the "secure electronic signature" designation that gives rise to the heightened presumption. However, if the requirements for a qualified security procedure are met, there is no reason why other forms of electronic signatures, such as click wrap agreements, could not also be so treated. But note the number of conditions that need to be met before a security procedure can be deemed "qualified," and the circumstances under which a signature created by such a procedure can be deemed "secure." All are grist for litigation before the presumption can be invoked. It is not nearly so simple as authenticating a document with a holographic signature.

Pennsylvania's Electronic Transactions Act[90]

Pennsylvania's Electronic Transactions Act is one of the most recently enacted statutes, and can be seen as providing a minimalist approach. It basically adopts the UETA for Pennsylvania, but adds to it a chapter expressly providing enhanced evidentiary protection under certain circumstances. Now that the UETA is in final form, efforts like this are likely to appear in other states that wish to eschew the specificity of the Minnesota model, but are not ready to embrace the sweeping scope of the Illinois model.

The Pennsylvania Act bases its treatment of electronic signatures on the UETA's definition of a "security procedure" as it may be adopted by agreement of the parties.[91]

---

[90] The Electronic Transactions Act (Pennsylvania Consolidated Statutes, Titles 12 and 18) (1999 PA Senate Bill 555).

[91] "A procedure employed for the purpose of verifying that an electronic signature . . . is that of a specific person or for detecting changes or errors in the information in an electronic record." The Electronic Transactions Act at §103, definition of "Security procedure" (Pennsylvania Consolidated Statutes Titles 12

The Pennsylvania Act simply enhances the UETA's normal attribution rule[92] in those cases where "the parties agree to use or otherwise knowingly adopt a security procedure to verify the person from which an electronic signature has been sent . . . ."[93] Where a security procedure has been so agreed to or adopted, then, provided the procedure was commercially reasonable and was reasonably relied upon, an electronic signature "is attributable to the person identified by the security procedure. . . ."[94] By the same token, an electronic record will be deemed unaltered if an agreed upon, commercially reasonable and reasonably relied upon security procedure so indicates.[95]

This enhanced attribution is subject to rebuttal when there is no independent showing that the electronic signature was the "act of the person." If the electronic signature is not attributable under the UETA'a normal attribution rule, but would be under the enhanced attribution rule, then attribution can be defeated if the putative signer can prove that the signature was issued by an unauthorized person, or by a person misusing the security procedure.[96]

Thus, without even mentioning digital signatures, Certification Authorities or certificates, the Pennsylvania Act provides all the evidentiary features of the Minnesota and Illinois presumptions for those parties who have agreed upon any security procedure

---

and 18) (1999 PA Senate Bill 555).

[92] "An electronic . . . signature is attributable to a person if it was the act of the person." *Id*. at §305(a).

[93] *Id*. at §701(2).

[94] *Id*.

[95] *Id*. at §702.

[96] The Electronic Transactions Act at §701(3) (Pennsylvania Consolidated Statutes, Titles 12 and 18) (1999

to govern their electronic communications. The Act essentially privatizes the availability of presumptions favorable to electronic and digital signatures. If the parties agree to use a security procedure to create electronic and digital signatures under the Act's provisions, then the Act will provide the attribution rules that will give swift procedural effect to their transactions, regardless if the security procedure specifies a digital signature or not. If there is no agreement or adoption of a security procedure, then the law gives no special protection.

As you can see, there is not much uniformity in how states deal with electronic and digital signatures, not even among those states that have provided presumptions in favor of their use to authenticate documents. Minnesota's straightforward treatment, Illinois' elegantly engineered solution and Pennsylvania's *laissez faire* approach reflect legitimate but divergent ways of looking at the state's proper concerns in facilitating the use of this new technology. Pennsylvania's Act is, perhaps more than the others, cognizant of the present lack of consensus, and simply leaves it to private parties to agree or not on how to manage their electronic affairs. In decreeing by legislative fiat that the owner of a certificated encryption key, or the sender identified by a security procedure, is therefore presumed to have actually sent the message, these statutes ultimately depend on a *non-sequitur*, that because we can with certainty identify the owner of an electronic signature, therefore that owner must have signed the document we seek to authenticate. One, however, does not follow from the other. These statutes accomplish by brute legislative force what in the common law evolved naturally from common sense. That is

---

PA Senate Bill 555).

why they all seem so contrived, and why Pennsylvania's, which does the least, may be the best.

IX. Special Considerations for Securities Transactions

Securities transactions are not fundamentally different from other commercial transactions, and so everything said so far applies equally to them. Aspects of the securities business that could and do take electronic form are:

The on-line filing of registration and blue sky forms with regulators.

The on-line solicitation for the purchase and/or sale of securities.

The on-line delivery of prospectuses and other selling documents.

The receipt of subscription agreements and other purchasing documents in on-line non-broker sales of securities.

The opening of brokerage accounts on-line.

The transmission of brokerage instructions on-line.

On-line record-keeping by broker-dealers.

Most of the issues surrounding these on-line activities do not involve the peculiar evidentiary problems of electronic and digital signatures that we have been discussing, and to the extent they do, most of the issues are generic and dealt with above. In this section, rather, I want to focus on three specific topics deserving special mention.

1. Using Electronic and Digital Signatures to Track On-Line Deliveries of Offering Documents

When selling securities, either by a broker-dealer or the issuer or its placement

agent, it is often important to be able to prove the delivery of a prospectus or offering memorandum. When dealing with private offerings exempt from registration, initial public offerings and additional offerings of securities of already public companies, it may be unlawful to sell the security without first delivering a selling document to the potential investor. With regard to private offerings that are exempt from registration, it may be necessary to prove that an offering memorandum was not widely distributed in order to take advantage of a registration exemption. For whatever reason, keeping track of who receives an offering document is often important and may be crucial to maintain the integrity of the offering.

Under existing and developing SEC rules, it is possible, and will in the future become more common, to distribute offering memoranda on-line, either through a web-site or through delivery as an E-mail attachment. When delivery of offering material occurs on-line, electronic and digital signatures can be used as means of tracking recipients.

However, this form of record-keeping does not require the level of security provided by secure electronic signatures and digital signatures. It should be enough for the broker-dealer or issuer simply to retain a record of the E-mail address of the recipient, which can easily be archived off any E-mail program. If delivery is by download from a website, then the recipient should be required first to fill in a template with his or her name and address, which would then become the record of delivery.

For private placements that depend upon limited distribution to avoid a registration requirement, however, E-mail should be the preferred method. Even if a

prospective investor inquires or requests an offering memorandum through a web-site, the actual delivery should be by directed E-mail. The problem is that because of the wide accessibility of documents posted on a web-site, making restricted offering memoranda downloadable risks their being called a public offering.

None of this, however, brings true electronic and digital signature issues into play, except for the submission of offers to purchase and, especially, investor qualification and subscription forms. For Regulation D private offerings under Rule 505 all but 35 purchasers must be "accredited," and under Rule 506, no more than 35 can be "sophisticated" and all the rest must be "accredited". The usual way to determine whether purchasers are sophisticated or accredited is to have all potential investors fill out and certify a questionnaire about their income, assets, and investment history. The certification must, of course, be signed. If the questionnaire is on-line, or being delivered by E-mail, then the seller of the security who is relying on it to ensure that an exemption from registration is not jeopardized should demand a secure electronic or digital signature. An on-line questionnaire would need to have at least the security attributes of a click wrap agreement.

In the absence of federal legislation, various state law provisions will need to be looked at to determine the efficacy of the electronic or digital signature used. And, of course, in determining whether to accept electronically signed investor qualification certificates, you should keep in mind the issues raised here concerning the authentication of the electronic certificate, should it come to that. As a practical matter, except in those states that grant an express presumption of authenticity to secure electronic or digital

signatures issued in strict compliance with their statutes, one always runs a risk, in accepting an electronic signature, that it will not be deemed valid or that it might not be proved it court. Caution should be the watchword.

2. Using Electronic and Digital Signatures to Open Brokerage Accounts

With on-line brokerage firms proliferating, many would like to be able to sign customers up on-line, before they have time to consider a competitor. The father of on-line brokerage services, E*Trade Securities, Inc., trying to accomplish this goal, sponsored and lobbied the State of California to pass a law in 1999 that by its terms makes a brokerage account application bearing either an electronic or digital signature "a fully executed, valid, enforceable, and irrevocable written contract."[97] Interestingly enough, however, as of last August, E*Trade still required account applications to be holographically signed. Reviewing the California statute in light of our prior discussions, one is not surprised.

The California broker-dealer statute is strictly a recognition statute. It carries no presumptions that assist in finding that the owner of the electronic or digital signature is the person who actually signed the document. So, in having an electronically signed document, a broker-dealer may have a valid contract; but without any security measures to determine the identity of the signer, and no presumptions to assist in enforcement, the broker-dealer faces uncertainty in holding any particular person liable. Moreover, the California law only applies in California, and other states do not treat electronic and digital signatures uniformly. Even if a brokerage agreement states that California law

[97] Cal. Civ. Code §1633(a) (1999 CA Senate Bill 1124).

will apply, one can make a very good argument that such a provision presupposes that the agreement was signed, and that the question whether or not it was must be determined by the law of the place of contract, generally where the customer is. Thus, the California broker-dealer law cannot induce much confidence in the use of electronic signatures to open customer accounts.

While the California law was making its way through the legislature, a similar bill was introduced in the United States Senate (S.921), seeking much the same thing.[98] S.921 also provides that mere electronic signatures[99] may be relied upon by registered broker-dealers in accepting account applications, and that such signatures "shall not be denied legal effect, validity or enforceability solely because it is an electronic signature."[100] Again, this is a classic recognition statute, which probably does not change existing law anywhere, and which does not assist a broker-dealer in proving to a court that the signature on its account form was the authentic act of the party it seeks to hold liable. S.921 is still pending.

In the final analysis, there is no uniform guidance on whether electronic signatures are a safe way for brokers to open customer accounts. In the absence of uniformity, a broker-dealer, which inevitably has customers in several jurisdictions, is best advised to stick to paper and holographic signatures to open accounts.[101]

---

[98] S.921, 106th Cong. (April 29, 1999).

[99] Defined simply as "an identifying sound, symbol or process attached to or logically connected with an electronic record," I*d*. at §4(4), with no requirement of any attributes of authenticity.

[100] *Id*. at §5(a)(1)(i).

[101] Of course, once the account is opened by conventional means, nothing prevents the parties from

3. Fulfilling Broker-Dealer Record-keeping Requirements with Electronic Records

The NASD, stock exchanges and the SEC have various record-keeping requirements that broker-dealers need to comply with. As more and more brokerage activity becomes on-line, the question arises how to ensure compliance with these record-keeping requirements when all records are electronic.

At present there are no express regulatory provisions governing electronic record-keeping. The NASD's position is that records and signatures may be kept in any manner acceptable under SEC Regulations (*i.e.*, C.F.R. §240.17a-3 and §240.17a-4). While we did not deal directly with electronic records in this article, the principal issue with records is how to assure that they are not tampered with. Digital signature technology, by use of hash functions, can provide the needed assurance of non-alteration.

However, state laws do not deal well with the issue of electronic records. The UETA, for example, only provides recognition to electronic records, stating simply that where the law requires records to be maintained, an electronic record will satisfy the requirement if it accurately reflects the original information and remains accessible for later reference.[102] But an "electronic record" is defined simply as storable and retrievable information "created, generated, sent, communicated, received, or stored by electronic means."[103] There is no provision for security with the UETA and hence no requirement

---

contracting privately to provide recognition of electronic signatures in future correspondence.

[102] UETA §12.

[103] *Id*. at §§2(7), 2(13).

that electronic records be protected from tampering or kept in a way such that tampering can be detected. By strict operations of these provisions, an electronic record satisfies a record retention requirement so long as it is unadulterated; if, however, it is tampered with, then it ceases to satisfy the requirement. But how does one know whether any tampering occurs? The UETA is silent.[104]

Whether this perfunctory treatment will ultimately satisfy SRO and SEC requirements remains to be seen. The lack of state uniformity about the effect of electronic records and signatures is also a concern for any broker-dealer subject to the Blue Sky Laws of several states.[105] Again, entities needing to retain records should proceed cautiously.

X. Problems, Problems. Where's the Solution?

None of today's efforts towards making electronic signatures as legally effective as holographic signatures fully succeeds. None can, because all must contend with the root problem that all electronic signatures, including digital signatures based on the most

---

[104] The SEC has attempted to solve the problem by enacting comprehensive and detailed rules governing the keeping of records on "electronic storage media" Reg. §240.17a-4(f) (CCH 3/22/00). However, the SEC rules are very restrictive, requiring, among other things, that "electronic storage media must. . . preserve the records exclusively in a non-rewriteable, non-erasable format …" Reg. §240.17a-4(f)(2)(ii)(A) *et seq.* (CCH 3/22/00). In a similar vein, the NASD has issued interpretive letters to the effect that a registered principal may approve the opening of a customer account electronically rather than by manual signature if the approval is somehow made a permanent part of a read-only optical disk record of the customer account application. AMERICAN EXPRESS FINANCIAL CORP., NASD Interpretive Letter (Nov. 26, 1997; AMERITRADE, INC., NASD Interpretive Letter (Oct. 26, 1999). This is a different concept of record-keeping, focusing on the nature of the physical media (e.g., non-re-writeable, read-only optical disks), as opposed to using digital signature technology to identify if alteration has occurred.

[105] U.S. Senate Bill 921 would permit records to be kept as insecure electronic records, which does not make much sense until you factor in the SEC's rulemaking authority, which would no doubt strengthen the security requirements.

sophisticated and secure encryption key technology, exist separate and apart from the human beings that use them. Unlike with a simple holographic signature, there is no way to be sure that any given electronic signature was truly authorized by the person who owns it. None of the legislative solutions can create, even in theory, a mechanism that completely emulates the natural presumption that the owner of a holographic signature is the same person who signed the document bearing that signature. In place of the ease, simplicity and comfortable acceptable of that presumption, electronic and digital signature legislation imposes complexity. Add to that the lack of uniformity from state to state and country to country, and it becomes safe to say that the effect of electronic and digital signatures will almost always be litigated with less certainty of outcome, and more effort and expense, than would holographic signatures under similar circumstances.

There are technological solutions that will in time change this. These attempt to make it impossible, or at least unfeasibly difficult, for someone other that the owner of a private key to use it, to the same extent or more than it is unfeasibly difficult for someone to forge a holographic signature. The best solution will be a security procedure that requires some form of biometric confirmation of identity as a precondition to creating a digital signature. For example, your computer may deny you access to your encryption key unless you first present it not only with a password and/or an access card, but also, through a scanning device, digital camera or microphone, with the fingerprint, handprint, voiceprint, face profile, retinal scan or even, I suppose, holographic signature on a stylus pad that matches the one on file for the authorized subscriber.

In invoking biometrics, we come full circle. A holographic signature is nothing

but a simple biometric identifier. Its legal authority derives from the fact that it can only be created by the flesh and blood person who owns it. A biometrically secured electronic signature is, unlike today's machine-based models, a true analogue of the holographic signature, and indeed can be made even more secure because biometric identification is more reliable than graphology. It is reasonable to think that the use of a reliable biometric security procedure will become such unshakable evidence that the owner of a signature actually used it on the document in dispute that a presumption to that effect will arise in fact if not in law. Then, but only then, it can be said that electronic signatures are just as good as handwritten signatures.

In the meantime, Pennsylvania gives a clue on how best to advise clients seeking to do business electronically. Parties are always free to contract their own personal solutions to these problems, to govern their own transactions. The UETA specifically permits parties to deviate from its provisions.[106] Until a uniform law evolves, clients are well-advised, if they wish to conduct business electronically, to enter into an agreement (holographically signed) specifying the respective rights and obligations of the various parties insofar as reliance on electronic communications are involved, including express provisions specifying what effect, substantive and evidentiary, will be given to electronic and digital signatures, and under what circumstances.

---

[106] UETA at §3(d).