

The Legality of the PenOp® Signature

Benjamin Wright, Esq.

Published by:

PenOp Inc.
One Penn Plaza, Suite 2407
New York, NY 10119
USA
Tel: (212) 244-3667
Fax: (212) 244-1646

PenOp
Vallis House, 57 Vallis Road
Frome, Somerset BA11 3EG
United Kingdom
Tel: (01373) 452755
Fax: (01373) 452744

E-mail: info@penop.com
Web: <http://www.penop.com>

Second revised edition. Copyright © 1994 by Benjamin Wright. All Rights Reserved.
PenOp is a registered trademark of Peripheral Vision Limited.

This paper provides general information and is not intended as legal advice for any particular person or situation. It does not establish and is not part of a client-attorney relationship between the reader and any other person. If the reader needs legal advice, the reader should seek the services of a competent attorney. No warranty is given as to the accuracy or completeness of this information, and Peripheral Vision Limited, PenOp Inc. and Benjamin Wright disclaim, and do not assume, any liability for any loss or damage caused by errors or omissions in this paper, whether the result of negligence, accident or otherwise. This paper is not necessarily intended as an exhaustive discussion of the legal issues involved with using PenOp. Benjamin Wright received a fee from Peripheral Vision Limited, the developer of PenOp, to write this paper.

The Legality of the PenOp Signature

Table of Contents

Executive Summary	3
Introduction	4
System Functions	5
PenOp Applications	7
Question and Conclusions	9
PART I: LEGAL PRINCIPLES	11
The Law of Signatures Generally	12
Signatures When Required	12
Signatures as Intentional Symbols	12
Precedent for Non-traditional Signing	12
Signatures When Desired	13
Security and Evidence	13
Active Assent	15
Special Signature Laws and Documents	16
The General Law of Writings	18
PenOp Information as Evidence	20
Believing Data Records	20
Believing the Signature Verification Service	21
Legal Conclusions and Form Language	23
PART II: PRACTICAL CONSIDERATIONS	25
Data Linking	26
User Instructions	28
Archives	29
Graphic Representation of Autograph	30
Multiple Signature Attempts	31
Dual Signatures	32
Witnesses	33
Notarization	34
General Controls	36
PART III: MANAGING RISK	37
Biography of the Author	39
Endnotes	40

The Legality of the PenOp Signature

Executive Summary

PenOp is a pen-based computing software component that captures and verifies signatures (autographs) and links them to specific electronic documents. It can permit, for instance, a bank customer to view the words of a loan application on the screen of a computer and then to approve the application by inscribing his signature on the screen.

This paper analyzes the legal effectiveness of using PenOp to sign an electronic document. It concludes that a compelling argument can be made that PenOp, when used intelligently, can allow documents to be signed in a way that is just as legally effective as the traditional method of signing. This conclusion is subject to limited reservations. Some laws, such as government regulations, may be interpreted to require signing in the traditional way.

Adequately controlled records of the electronic documents signed through PenOp are likely to be roughly as useful as evidence in court as equivalent paper documents. When properly implemented, PenOp may even provide better security and evidence than is common for traditional signed documents. PenOp provides what appears to a lawyer to be an impressive set of security and evidence tools (such as act-of-signing statistics, checksums, and a timestamp).

There is no guarantee, however, that PenOp's signature verification capability will be believed in court, just as there is no guarantee that a traditional handwriting/document examiner will be believed.

If a PenOp signing is to be effective, a well-conceived program for creating and archiving records must be followed. This program is generally no more and no less difficult to follow than the program needed to create and archive paper records, but it is different. This paper offers suggestions for such a program.

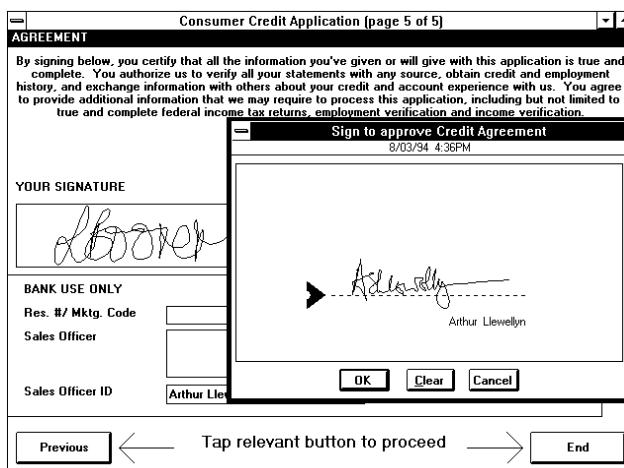
The adoption of PenOp entails benefits, risks, and costs. But the alternatives to PenOp -- including traditional paper and ink -- also entail benefits, risks, and costs. People using PenOp for signing legal documents should seek the advice of counsel, and this paper will help counsel give informed advice. But the ultimate decision whether to adopt PenOp is a decision for business managers, not lawyers.

See the full paper for details.

Introduction

The business world is beginning to wring great productivity gains from computers. Among other things, computer technology is streamlining the customs that businesses observe when they enter and record transactions for legal purposes.

A remarkable example of this technology is PenOp. Developed by Peripheral Vision Limited, PenOp is a pen-based computing software component that captures and verifies signatures (autographs) and links them to specific electronic documents. It can permit, for instance, a bank customer to view the words of a loan application on the screen of a computer and then to approve the application by inscribing his signature onto the screen.



This method of signing departs somewhat from the traditional method, where the signer manually inspects, handles, and signs, in ink, a document written on paper. The question that immediately comes to mind is whether a document signed using PenOp is legally effective. This paper addresses that question.

This paper is not a product endorsement or a legal opinion. The observations it makes do not apply to any specific situation. Rather, it is an essay that analyzes, in a general sense, the legal effectiveness of signing documents with the aid of PenOp. It is intended to assist lawyers advising current and potential users of the technology so they may make an informed assessment of its benefits and risks. The law discussed here is that generally applicable in the United States of America (federal and state law, excluding Louisiana), with references to English law.

I am a lawyer, not an engineer. In writing this paper, I have assumed that PenOp functions as I have described here and that the people who will use the product will do so intelligently.

System Functions

PenOp is a computer software component that can augment the function of other computer applications. PenOp has two primary features:

1. The *Signature Capture Service (SCS)* captures and permits the storage of certain data associated with the manual inscription of a signature on the screen of a pen-based computer. SCS must work with a "Client Application," which is software that informs the pen computer user what he is doing and prompts him when and how to do it. (Many different Client Applications can be designed to be used with PenOp.)

In coordination with the Client Application, the SCS receives information, such as a user ID, showing who the user claims to be. It then prompts the user to inscribe his signature, using a stylus (or pen), upon a window on the computer's screen. The Client Application supplies the wording of the prompt in the window, known as the "Gravity Prompt," which indicates the purpose for which the signature is being captured. The Gravity Prompt normally refers to an electronic document that is accessible to the user through the pen computer.

As the user moves the stylus across the screen, an image appears that traces the movement of the stylus. Thus he sees his autograph. At the same time, the SCS measures certain features of the inscription event, including the size, shape, and relative positioning of the curves, loops, lines, dots, crosses and other features of the signature being inscribed, as well as the relative speed at which each feature is imparted. The results of these measurements are known as "act-of-signing statistics." The user then has the option, by tapping indicated buttons on the screen, of approving the inscription event, retrying it, or aborting it.

If the user taps the approval button, the SCS calculates a checksum,¹ or a brief string of data, that represents the content of the electronic document referred to by the Gravity Prompt. This checksum is not a complete statement of the original document, and the original document cannot be derived from the checksum. But the checksum bears a mathematical relationship to the document. If the document is changed, then it can no longer be mathematically matched with the checksum.

Next, the SCS compiles the following data and computes a second checksum from it:

- * the first checksum
- * the act-of-signing statistics
- * the date and time of signing (as represented by the computer operating system under which the SCS is operating)
- * the identity of the particular machine on which the signing occurred (based on identity information programmed earlier in the SCS)
- * the claimed ID of the user
- * the words that appeared in the Gravity Prompt
- * (optionally) data reflecting the graphic image of user's signature

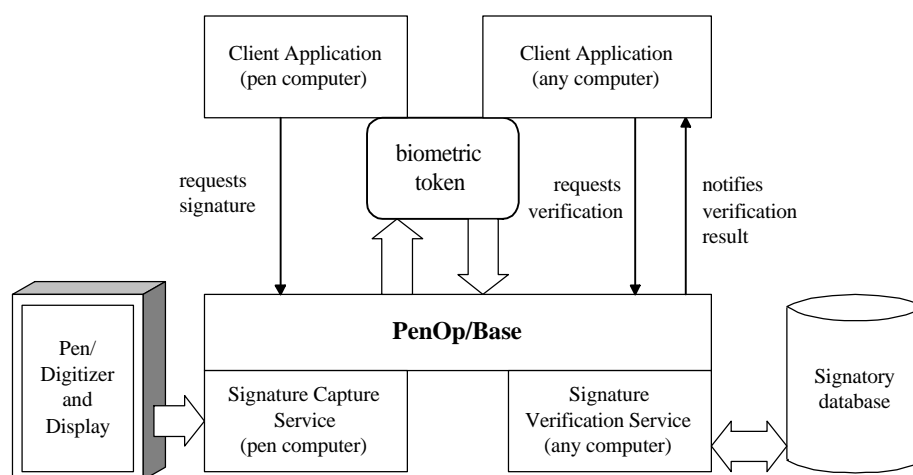
The SCS then encrypts all of this data, together with the second checksum. This encrypted string of data -- called the "Biometric Token" -- represents the inscription event.

The Legality of the PenOp Signature

2. The *Signature Verification Service (SVS)* reports the probability that a particular signature is authentic. First, in authorized enrollment sessions, the SCS captures and the SVS holds, in a database, act-of-signing statistics for a user who has been identified to the SVS.

Later, the SVS may be presented with a particular Biometric Token and directed to evaluate whether the token is a product of an authentic inscription of the signature belonging to the user identified in the token. The service decrypts the token and then compares the information therein with the signature statistics stored earlier in its database. Based on this comparison, it issues a "signature match percentage", e.g., 50 percent or 72 percent, and reports this percentage to a Client Application (software configured to make use of the report). The SVS applies scientific principles deemed relevant by PenOp's developers.

PenOp System Diagram



These two functions of PenOp, SCS and SVS, might be incorporated into many different types of computing environments. The SCS might, for example, inhabit a fleet of portable pen-based computers, while the SVS might reside on a single host computer. The portable computers might capture numerous Biometric Tokens over time and then transmit them to the host for verification.

I am not qualified to assess how reliably the PenOp technology captures and evaluates data. I am also not competent to assess how secure the PenOp technology is against abuse. In part, reliability and security will depend on whether the technology is implemented by competent computer professionals using appropriate equipment.

See Part II: Practical Considerations.

PenOp Applications

PenOp might be used in any number of ways. This paper focuses on the use of PenOp to facilitate the legal "signing" of documents such as contracts, expense reports, or medical records. The discussion is limited to the following two applications of PenOp (recognizing that other applications are possible):

A. *Attachment of Biometric Token.* In this application, one seeks merely to attach a Biometric Token to an electronic document, such as a medical report, for the purpose of achieving a legal "signing" of the document. To start, a Client Application within a pen computer is configured to display to the computer user the data within the document in question (text, graphics, and so on, all in digital format).

The Client Application then calls the SCS to write a Gravity Prompt, inviting the user to "sign" the document by inscribing his signature within a window on the computer screen. The SCS also presents the user a button for approving the inscription. If the user inscribes and approves, SCS captures the necessary data and creates a Biometric Token. The SCS delivers the Biometric Token to the Client Application for storage in a way that identifies the token as being related to the signed document. If, at a later date, a third party such as a court wishes to verify that the user did "sign" the document, that party could obtain the PenOp SVS, introduce the user to it, and use it with the help of an expert to verify (to the degree possible) that the Biometric Token represents an inscription by the user. A test could also be made (using the checksum in the Biometric Token) to establish whether the document to which the token is linked is the exact document used at the time of the token's creation. Under this application A, signature verification would occur only on rare occasions.

B. *Attachment and Verification of Biometric Token.* In this application, one seeks to verify and record that a particular user did sign a document, such as a medical report. First, sometime before the document is created, the user is introduced to the PenOp SVS, which stores in a database the user's act-of-signing statistics. Later, when the document is created, a Client Application within a pen computer is configured to display to the user the data in the document (text, graphics, and so on, all in digital format), including a simple identification of the user such as a user ID.

The Client Application then calls the SCS to write a Gravity Prompt, inviting the user to "sign" the document by inscribing his signature within a window on the computer screen. The SCS also presents the user with a button for approving the inscription. If the user inscribes and approves, the SCS creates a Biometric Token. The Client Application next creates an archive of the Biometric Token and delivers the data from the token to the SVS, which then evaluates whether the token derives from the identified user. The SVS issues a "signature match percentage", e.g., 50 percent, and reports this percentage back to the Client Application. The application then makes a record whether the signature match percentage did or did not exceed a pre-designated threshold (e.g., 75 percent) and identifies that record as being related to the document in question. This record shows in effect whether the identified user signed the document. The record is available to a third party, such as a court, as positive or negative evidence of signing. In addition to this record, an archive of the Biometric Token is also kept for analysis in the future.

The Legality of the PenOp Signature

In this paper I refer to the "PenOp method of signing" as meaning a competent implementation of either application A or B above. The PenOp method of signing might be applied to any number of legal transactions. It might be used to sign a loan application that is kept as a computer archive. It might be used to sign an e-mail or electronic data interchange (EDI) message that authorizes a bank to make an electronic payment. Or, it might be used to sign a photograph, stored in digital format as a computer file.

Question and Conclusions

The question: are the foregoing applications legally effective? In other words, if an electronic document is signed with the PenOp method of signing, is the document just as legally effective as if a signature had been affixed in the traditional way to an equivalent paper document?

The following discussion analyzes this question in three parts. Part I looks at law as a set of principles. It concludes that a compelling argument can be made that PenOp, when used intelligently, can allow documents to be signed in a way that is just as legally effective as the traditional method of signing. As explained later, however, this conclusion is subject to limited reservations. Some laws, such as government regulations, may be interpreted to require signing in the traditional way.

Part I further concludes that adequately controlled records of the electronic documents signed through PenOp are likely to be roughly as useful as evidence in court as equivalent paper documents are. It points out, however, that there is no guarantee that PenOp's signature verification capability will be believed in court, just as there is no guarantee that a traditional handwriting/document examiner will be believed.

Part II examines what I mean by "using PenOp intelligently" and having "adequately controlled records." It looks at the practical process of gathering and preserving legal evidence, observing that if a PenOp signing is to be effective, a well-conceived program for creating and archiving records must be followed. This program is generally no more and no less difficult to follow than the program needed to create and archive paper records, but it is different. Part II offers suggestions for such a program.

Finally, Part III considers the risks involved with using PenOp for legal transactions and compares it to other legal risks taken in business.

The Legality of the PenOp Signature

PART I: LEGAL PRINCIPLES

The affixing of a "signature" is a customary way of showing approval of a legal document. Signing is oftentimes required by law in order to make a document legally effective.

The consummate example of a signature requirement is the statute of frauds, a commercial law that appears in different forms in the laws of almost all the American states. The statute generally provides that certain types of contracts, such as a contract for the sale of goods for more than \$500, are not enforceable unless there exist "signed writings" to evidence the contracts.²

Even if there is no law such as the statute of frauds mandating that a document be signed, it may still be customary that the document be signed as a way of evidencing assent. As evidence of assent to the assumption of risk of injury, for example, the patron of an amusement park may sign a release document. This assumption of risk does not necessarily require a signature to be effective, but the signature is a convenient and well understood device for evidencing that the patron knew the risk and that he assented to the assumption of it.

Signatures are often used as a means of security. To a limited degree, for instance, the signature on a check is a form of security; drafting an unauthorized check often requires forging a signature on the check. As explained later, however, a legal requirement for a signature is not necessarily a requirement for security.

Often, government regulations require that people sign this or that document, a tax return for example. The purposes of the signing requirement can differ from one regulation to the next, but they can be interpreted to include the desire to obtain evidence that a certain person actually saw a document, completed it, or assented to it.

This Part I will consider each of these ways in which one might wish to use the PenOp method of signing, i.e., to satisfy the statute of frauds, to achieve security, to evidence assent, and to satisfy a particular regulation. It will also consider whether a document signed with the PenOp method of signing is a legal "writing" and whether PenOp-supported information is admissible as evidence in court.

The Law of Signatures Generally

Signatures When Required

The traditional concept of a signature envisions that a person grasping an ink pen writes an autograph on a sheet of paper. This, however, is only one of the many concepts accepted under the law of signatures. As argued later, the legal word "signature" is generally broad enough to include the PenOp method of signing.³

Signatures as Intentional Symbols

Legally speaking, the essence of a signature is the **intent** to use it (whatever "it" happens to be) to adopt or approve a writing. Under Uniform Commercial Code Section 1-201(39), for example, "'Signed' includes any symbol executed or adopted by a party with present intention to authenticate a writing." U.C.C. Section 1-201 Official Comment 39 explains:

The inclusion of authentication in the definition of "signed" is to make clear that as the term is used in [the U.C.C.] a complete signature is not necessary. Authentication may be printed, stamped or written; it may be by initials or by thumbprint. It may be on any part of the document and in appropriate cases may be found in a billhead or letterhead. No catalog of possible authentications can be complete and the court must use common sense and commercial experience in passing upon these matters.

If one assumes that a document signed with PenOp is a "writing" (an assumption to be discussed later), then a compelling argument can be made that PenOp can, under the foregoing definition, be used to "sign" it. The argument is that if the PenOp user intends the autograph he inscribes on the screen of a pen computer to be his symbol for authenticating a writing, then the autograph is his legal signature.

Precedent for Non-Traditional Signing

Extensive precedent exists for non-traditional methods of signing. Indeed, commercial law has proven to be flexible as new means for creating signatures have emerged. *Beatty v. First Explor. Fund 1987 and Co.* (a noteworthy British Columbian case) confirmed that an autograph on a fax was indeed a signature. The court observed:

The law has endeavored to take cognizance of, and to be receptive to, technological advances in the means of communication. . . . The conduct of business has for many years been enhanced by technological improvements in communication. Those improvements should not be rejected automatically when attempts are made to apply them to matters involving the law. They should be considered and, unless there are compelling reasons for rejection, they should be encouraged, applied and approved.⁴

The compelling reason for approving the PenOp method of signing is that it can provide a record that is roughly as useful as a traditional written and signed paper record, if not more useful. Of course, the PenOp system must be intelligently implemented, just as paper and ink must be used intelligently if they are to create a useful record.

The Legality of the PenOp Signature

The U.S. Securities and Exchange Commission now interprets the word "signed" to include simply the characters of a name (e.g., "John Doe") transmitted in an electronic filing to the Commission.⁵ Further, the U.S. Internal Revenue Service interprets the statutory requirement that a tax return be "signed" as being satisfied when a taxpayer leaves a "voice signature" on an interactive telephone system. This interpretation was made in temporary regulations issued for purposes of a pilot test.⁶

Many judicial decisions have held that simple typewritten names on telegrams and telexes are signatures for purposes of the statute of frauds. One of the most famous, *Howley v. Whipple*, made clear that the traditional method is not the only effective way to sign a writing:

[W]hen a contract is made by telegraph . . . that constitutes a contract in writing under the statute of frauds; . . . it makes no difference whether [the telegraph] operator writes the offer or the acceptance . . . with a steel pen an inch long attached to an ordinary penholder, or whether his pen be a copper wire a thousand miles long. In either case the thought is communicated to the paper by the use of the finger resting upon the pen; nor does it make any difference that in one case common record ink is used, while in the other case more subtle fluid, known as electricity, performs the same office.⁷

In one potent respect, the PenOp method of signing is closer to the traditional method than signing via telegram or telex is. PenOp involves the manual inscription of an autograph -- one that visually appears to the signer to be almost identical to the signer's traditional ink and paper autograph. This similarity between the PenOp and the traditional method helps to clarify the signer's intent when he signs with PenOp. Because the PenOp method looks so much like the traditional method, the intent to make a legal "signing" is unambiguous.

Signatures When Desired

Security and Evidence

Under the statute of frauds and many other commercial laws, the requirement for a signature does **not** demand that the symbol serving as signature have any level of security, reliability, or forensic value whatsoever. The definition of signature in U.C.C. Section 1-201(39) (printed earlier) does not say that a signature must be secure.⁸ Further, *Hessenthaler v. Farzin*⁹ held that a mere typewritten name on a mailgram was a signature. Anyone could have typed that name; still, it was a signature under the statute of frauds.¹⁰

Security, reliability, and forensic value do nevertheless play a role in the practice of making signatures. Often, one party or another involved with a transaction wishes to create or obtain some proof that the signer really did something, that he actually saw a particular document and approved it.

This desire for proof is not a statute of frauds or commercial law concern. Rather, it is an evidence concern. As an evidentiary matter, the signer wishes to mark the documents he approves so as to distinguish them from all the documents in the world that he has not approved. Conversely, the receiver of a document wishes to have some evidence that could, if necessary, be taken to court to show that the signer approved the document.

The Legality of the PenOp Signature

One of the popular ways for making this evidence is the traditional signature. But despite its popularity, the traditional signature performs the job of gathering evidence very poorly. A thumbprint would do a far better job of gathering the desired evidence, but people seldom authenticate legal documents with thumbprints -- simply because thumbprints are not the custom.

Traditional signatures are weak. They can be forged. They can be so difficult to decipher that a handwriting expert cannot determine whether they are authentic. They can also be disguised: A signer of a document who, with deceitful intent, wants the ability to repudiate the document can deliberately scribble his name with his left hand rather than his usual right hand.¹¹ Rarely in commercial dealings (some financial transactions being the exception) do the recipients of signed documents rely on a comparison of legal signatures with verified specimen signatures.

So if traditional signatures are so weak, how are paper documents proven in court? Despite what one may infer from watching courtroom-based television shows, the origin and genuineness of most documents are not proven on the basis of signatures. Much more often, origin and genuineness are proven from all the facts and circumstances -- the full relationship of the people involved - - the time, the place, the related transactions and discussions, the purpose and content of the documents, not just the signature. Much more often than not, the origin and genuineness of documents are not in dispute, and the parties simply stipulate that the documents are what they purport to be.

These problems aside, a traditional signature can provide a modicum of evidence on who is responsible for a document. A trained document examiner, for example, can sometimes -- but not always -- make a reasonable assessment whether a traditional signature is authentic. As explained later, however, the practice of assessing the authenticity of traditional signatures and documents is an inexact science. The document examiner's success depends on many factors, including the extent of his training, the quality of the specimen signatures he is given to compare, and the effectiveness of the particular testing techniques he employs. These factors are largely outside the control of the signer and receiver of a document; thus, at the time of signing, the parties have at best only a murky idea whether the signature will provide any valuable evidence of authenticity.

So what about PenOp? The user must judge for himself whether the PenOp method of signing -- as implemented in the user's particular application -- provides an adequate level of security and evidence. PenOp's developer promotes and sells the technology as a security device, though I am not qualified to pass on that aspect of the technology.

The user might bear in mind, however, that the technology PenOp replaces (the traditional signature) sets the baseline for adequate security and evidence at a very low level. When properly implemented, PenOp may well provide greater security and evidence than is common for traditional signed documents. PenOp provides what appears to a lawyer to be an impressive set of security and evidence tools (such as act-of-signing statistics, checksums, and a timestamp). Adequately controlled records of the electronic documents signed through PenOp are likely to be roughly as useful as evidence in court as equivalent paper documents, if not more useful. Part II of this paper offers suggestions that could enhance PenOp's security and evidence collection abilities when it is implemented in a particular application.

Active Assent

Another reason the receivers of documents prefer they be signed is that traditional signing entails some *action* on the part of the signer. The action helps make clear that the signer intended to assent to the document.

The PenOp method of signing replicates perfectly this function of the traditional signature. PenOp requires just as much action by the signer as traditional signing does.

Special Signature Laws and Documents

Myriad laws and regulations, issued by federal, state, and local authorities, require signatures, and this paper cannot address all of those laws and regulations.

Despite the arguments above for why the PenOp method of signing should be legally effective, it is possible that some specific laws or regulations could be interpreted to permit only signatures created in the traditional way. The risk arises not from any imperfection of PenOp. Rather, the risk is that some who interpret laws (judges or government administrators) will hold a different or more rigid view of what a "signature" is.

An example of this rigid view comes from the case *Gilmore v. Lujan*,¹² where a person vying for a federal oil and gas lease submitted a document via fax machine. Bureau of Land Management regulations, however, specified that the document could only be a "writing" that was "holographically signed in ink". BLM deemed the fax and the signature on it invalid. Although this rigid interpretation of a signature requirement is out of step with modern business practices, BLM had the authority to interpret its regulations in this way. Other government agencies may occasionally take similar positions.¹³

Most or all signing requirements are likely, eventually, to accept modern, computer-based methods. The Food and Drug Administration announced in 1992, for instance, that it is undertaking a massive effort to overhaul its regulations to accommodate new, electronic methods of signing.¹⁴

One would expect that in many cases authorities will be open-minded and will consider the PenOp method of signing to be acceptable. One feature of PenOp that may appeal to authorities is that, depending on how it is implemented, PenOp can provide more reliable evidence of signing than a traditional signature does. Judges and administrators will intuitively feel more comfortable with a method of signing if they perceive that it creates reliable evidence.

But there is the risk that some authorities will conclude that the PenOp method of signing does not produce a legal signature. (There is also the risk that they will not be persuaded of the technical reliability of PenOp or a particular implementation of it.) In those cases, usually what will be needed to have PenOp accepted is not necessarily a change in laws or regulations, but rather a change in the thinking on the part of the authorities who interpret them.

Given the risk, counsel must help clients judge whether it is prudent to use PenOp when a specific regulation requires a signed document. The intellectually easy choice will be to advise against using PenOp. But to do his job, counsel must work harder and be more practical. The risk that the PenOp method will not satisfy an authority must be weighed against benefits (convenience and savings in time and money) the client enjoys by using PenOp.¹⁵ See Part III.

In evaluating risk, counsel should recognize that a proper use of PenOp is not deceitful. The spirit behind the PenOp method of signing is the same as the spirit behind the traditional method. Just as with traditional signing, the person who properly employs PenOp views the words of the document to be signed, and takes physical action to cause the image of his handwritten signature to be associated with the document. In each case, the signer actively takes responsibility for the document, understanding that a record is being made.

The Legality of the PenOp Signature

The PenOp method is not an automatic event initiated by a computer. It is, like the creation of a traditional signature, an event driven by the hand of the signer. Because PenOp is a new device that functions very similarly to the traditional ink pen, very few if any regulations have been explicitly written or interpreted not to permit the PenOp method of signing.¹⁶ When using PenOp to satisfy a legal requirement for a signature, the signer has an honest and substantial argument that he has complied with both the letter and spirit of the law.¹⁷

The General Law of Writings

Beyond the question whether it can provide for a legal signature, PenOp raises two additional legal issues. The PenOp method of signing contemplates that the signed document be recorded in electronic media rather than on paper. An electronic record faces the questions whether it is a "writing" and whether it can be admitted as evidence in court. The outlook for each of these questions is generally optimistic.

Oftentimes particular statutes and regulations require that legal information be "written" or "in writing". The statute of frauds, for example, sometimes requires that a contract be supported by a writing.¹⁸ The question then is whether a document signed with the PenOp method of signing is "written" for purposes of a given law. The answer depends on the law's interpretation and purpose. There is no universally understood definition of what constitutes a writing, and the term carries different meanings in different contexts.

The ambiguity of the word "written" is illustrated by two counter-intuitive judicial decisions. In the first case, *Common Carrier Motor Freight Assn. v. NCH Corp.*,¹⁹ information that was written into a public tariff filed on paper was deemed by the court not to be "in writing" because the people the information was meant to protect did not have adequate notice of it. In a literal sense, the information was written, but it still did not achieve the purpose of the law requiring it to be "in writing".

Compare the second case, *Opinion of Justices*,²⁰ in which the court ruled that voting with the aid of a voting machine did constitute voting by "written ballot" because the machine served the same purposes under the law (secrecy and integrity) as a conventional written ballot. In a literal sense, there was no written ballot, but the mechanical method of voting achieved all the purposes of a written ballot.

The interpretation of the words "written" and "signed" can be influenced by a statement from a relevant party. Thus, for purposes of the statute of frauds, if the signer declares that the document is written and signed, it is very difficult for the signer later to argue that the document is not written or signed. A similar declaration is commonly made in the so-called trading partner agreements employed by users of electronic data interchange (EDI), an electronic messaging technology used to form paperless contracts.²¹ See the later section titled "Legal Conclusions and Form Language", which suggests a form statement to the effect that a document signed via PenOp is "written" and "signed".

A growing body of legal authority does support the notion that the word "written" includes information stored on computer media.²² In *People v. Avila*²³ the question was whether a magnetic recording of data on a computer disk constituted a "written instrument" under a forgery statute. The statute defined "written instrument" as "any paper, document, or other instrument containing written or printed matter or the equivalent thereof" The court held that data on a computer disk satisfy that definition.

Copyright law has also come to recognize computer disk recordings as "writings". Under the U.S. Constitution, Congress has power to extend copyright protection to "Writings". Congress has interpreted that word "Writings" to include computer disk recordings and now extends copyright protection to works in that medium.²⁴

The Legality of the PenOp Signature

The U.S. Securities and Exchange Commission now interprets the word "written" in the Securities Act of 1933 to include "magnetic impulses or other forms of computer data compilation."²⁵ The SEC reached this conclusion in connection with its program to receive securities filings via electronic transmission.

Hence, a substantial argument can be made that a document signed by the PenOp method of signing is indeed "written" under many different laws. The argument is strongest if (a) the PenOp signing is being applied to a text-based document (rather than, say, a computer file containing sound data) and (b) the purpose of the law in question either is to ensure that the signer has taken serious, deliberate action or is to ensure that there is a record made of the action. If the user can read the text of the document, and if that text is then recorded, it satisfies many of the traditional purposes of a writing. That text is controlled, symbolic information. It is functionally very similar to text printed on paper. In many instances it should be interpreted to be a writing.

The trend in American law is to interpret the words "in writing" and "written" to include electronic documents, like those signed through PenOp, and this trend very likely will grow.

Nevertheless, there may be some instances in which a document signed through PenOp does not satisfy a legal requirement for a "writing." An electronic document may not serve all the statutory purposes of a writing. A consumer protection statute may, for example, require that a consumer be delivered a copy of a "written" document, such as a loan agreement. The purpose is to ensure that the consumer possesses a record that is convenient for him to keep and use. An electronic document may not satisfy this purpose (depending on the sophistication of the consumer). Thus, for purposes of this particular statute, the word "written" may not include an electronic document, and PenOp may not be appropriate for transactions regulated by that statute.

If the user is concerned that an electronic document may not be considered "written," the practical solution may simply be to print the document on paper. Depending on the circumstances, it may be best to print the document at the time it is signed, or it may be enough to make printing available on demand. Proper use of printing bolsters the argument that a "written" document is created as required by the law.

PenOp Information As Evidence

The use of PenOp information as evidence in court raises two issues: 1. whether the records of relevant data -- such as the contents of an electronic document -- are admissible and credible as courtroom evidence; and 2. whether the Signature Verification Service (SVS) is to be believed.

Believing Data Records

Another way of stating the first issue is whether the computer system in question should be allowed to report the data recorded in it and whether those data should be believed once they are reported. The general answer is that American courts will admit into evidence, and will likely believe, reliable computer records.²⁶ (To allow evidence to be "admitted" is to allow the trier of fact -- which in the classic sense is the jury -- to learn of and consider the evidence.)

A large and growing body of judicial case law, dating back to the mid-1960s, shows that courts have generally been receptive to computer records into the courtroom, so long as the trustworthiness of those records can be demonstrated.²⁷ Such a demonstration can be made by showing the **controls** in place that make the data and the records thereof trustworthy. In other words, if a computer system has appropriate protections against error and abuse, then relevant records in the system are likely to be admissible as evidence.²⁸ Further, if computer records are shown to be reliable, they are likely to be believed by the trier of fact (the jury).

Thus, records of electronic documents signed through PenOp are likely to be useful as courtroom evidence if the process for creating and storing the records is well-controlled.

Any number of controls might be in place over a computer system in which PenOp is installed. The primary control would likely be that the system is used in business, for business purposes (or in government, for government purposes). Recognizing that businesses keep records for serious purposes, courts generally defer to records kept in the ordinary course of business.²⁹ Common sense says that a business is unlikely to use a computer system -- including PenOp -- if it consistently makes recordkeeping errors.

The secondary controls in a PenOp-based system would be all the technical and operational features that make the system a reliable recordkeeper -- the configuration of the hardware, the writing of the software, the function of the algorithms included therein, the maintenance of the system, and so on. The reader must judge for himself whether his PenOp-based system is a reliable recordkeeper. He might note that PenOp is marketed as a security technology; then he might take steps to confirm for himself how secure the technology truly is. He can gain comfort by observing whether the system functions properly over a period of time and by ensuring the system is operated and maintained by competent computer professionals. He can gain greater comfort -- at greater expense - - by engaging an independent system auditor to evaluate the system's reliability as a recordkeeper.

See Part II, which suggests controls that might be implemented with PenOp.

Believing the Signature Verification Service

It is one thing for a court to believe that a computer is faithful in the rote task of capturing and storing data in records (such as the words in a contract). It is another thing for the court to believe the computer has correctly interpreted or evaluated data. The PenOp SVS interprets and evaluates data when it judges the authenticity of a signature inscription.

Sometimes courts will rely on complex scientific processes like that executed by SVS, and sometimes they will not. There is no guarantee that, in any particular lawsuit, the court will rely on or believe the results of the SVS. But then again, there is no guarantee that the court would rely on the scientific process that the SVS replaces -- traditional handwriting/questioned document analysis.

The PenOp SVS technique is, essentially, an application of a scientific theory about handwritten signatures. Whether a party in court can use results from the application of a scientific theory depends on the party's persuasiveness in showing the validity of the theory and the aptness of the application.

In some courts, some well-recognized scientific techniques, such as some types of fingerprint analysis, are more readily accepted than others. In those courts certain techniques are so well accepted (as a result of "judicial notice" or legislative recognition) that the proponent need not do much to show the validity of the techniques. Yet the recognition of specific techniques varies from one court to the next, and one cannot predict in which court a particular issue will be litigated.³⁰ It is also hard to predict the relative persuasive skills of the parties (and their lawyers) who might be contesting a scientific technique some day.

The PenOp user must judge for himself whether the PenOp SVS is a scientific technique likely to be persuasive and useful in court. But that issue is not as bewildering as one might think. An equivalent issue faces the user of traditional ink and paper. He must judge whether traditional handwriting/questioned document analysis will be persuasive and useful in court. Sometimes it is; sometimes it is not.

Courts do not uniformly follow a rigorous system for determining the authenticity of traditional signatures. Some courts rely only on testimony from a qualified forensics expert, but some others will rely on testimony from a non-expert (e.g., the signer's spouse).³¹

Further, experts vary in their reliability. A traditional expert document examiner might use any of a number of different techniques: ink analysis, comparison of handwriting specimen, microscopic examination of pen strokes, and so on. Some techniques are better than others. Whether a court will admit into evidence (and believe) testimony resting on any particular technique depends on the proponent's success in showing the effectiveness of the technique. A court will sometimes bar or ignore the testimony of a document expert.³²

The reliability of the testimony can also depend on the expert's qualifications. Until quite recently, when certification became available, there was little in the way of uniformity in the qualifications courts would accept for a document examiner.

Thus, the forensic value of paper documents has always been uncertain. Nevertheless, commercial parties rarely think twice about relying on signed paper documents. As a practical

The Legality of the PenOp Signature

matter, they are little worried about this issue. It is enough for them to know from common experience that there is a modicum of forensic value around traditional signatures and documents. The PenOp user may be able to sense at least equivalent forensic value simply by observing and testing PenOp.

In sum, there is no black or white response to the questions whether any given document or signature will be believed as authentic and whether any particular technique for evaluating authenticity will be accepted in court. These questions have always been with us and they are likely to follow us into the electronic age. In the long run the PenOp SVS may prove to be more controlled, systematic, and therefore reliable than traditional handwriting/questioned document analysis, and courts may so recognize. But I cannot predict.

Legal Conclusions and Form Language

Asking the question whether the PenOp method of signing is legally effective is a bit like asking whether flour is bread. Flour is not itself bread; but if properly employed flour can become bread.

When used intelligently, the PenOp method of signing an electronic document should in many cases be just as legally effective as the traditional method of signing a document printed on paper. Persuasive legal precedent supports the concept of an electronic signature, and the PenOp method of signing fits well within this precedent. Precedent goes so far as to approve of signing by telegraph and telex even though the signature made thereby is just a typed or printed word. The PenOp method of signing, in contrast, is much more like traditional signing: with PenOp, the signer sees a graphic image tracing the motion of the signer's hand as he grasps a pen-like object.

A substantial argument can be made that an electronically-recorded document is a "writing". An exception might apply if the law requiring a writing is intended to protect consumers or help others who are incapable of dealing with electronic documents.

Further, considerable precedent supports the use of computer records, such as those of electronic documents signed through PenOp, as evidence in court. And, although there is no guarantee that the SVS will be believed in court, there is no guarantee in any particular case that a traditional document examiner will be believed either.

For these reasons, the case in favor of the PenOp method of signing is strong, though not absolutely airtight.

As explained, this conclusion is subject to reservations related to special laws and documents that might be understood to require only traditional signatures. Ultimately, the question whether to use the PenOp method of signing for any particular legal document is one for the user to make with the advice of informed counsel. The question requires judgment, which must weigh the practical benefits of using PenOp against the risk that someone might consider a PenOp document legally deficient.

Given the risk, some may feel more comfortable if the signer makes his intent in signing a document more explicit. Accordingly, counsel could recommend that the document (or the Gravity Prompt) contain the following statement (or selected parts of it):

The person signing this electronic document does so with the aid of a pen-based computer software component known as PenOp. [He or she] understands that a record of the document and [his or her] signing of it will be stored in electronic code. [He or she] intends both the signature [he or she] inscribes with PenOp and the electronic record of it to be [his or her] legal signature to the document. [He or she] confirms that the document is "written" or "in writing" and that any accurate record of the document is an original of the document.

The reason for confirming that an accurate record is the "original" is to preclude any suggestion that the image of the document displayed on the pen computer held by the user is the only original of the document.

The Legality of the PenOp Signature

PART II: PRACTICAL CONSIDERATIONS

I described earlier the inherent weaknesses of the traditional method of signing as a means for achieving security and gathering evidence. In view of these weaknesses, lawyers have employed various techniques to enhance the traditional method. For example, sometimes documents are set up so that signatures from two different people (e.g., a clerk and a manager) are necessary to make the documents effective.

Given the myriad procedures that might be employed to enhance a signature, knowing which to use, and when, requires judgment. There are no hard and fast guidelines. A trade-off must be made between security and convenience. One can always devise another procedure to deter error and abuse, but each additional one makes the use of a document more difficult.

The PenOp user faces the same trade-off. This Part II describes procedures to make the PenOp method of signing more secure and effective, but each procedure can make use of the system more cumbersome. The user must strike a balance between security and ease-of-use, based on the user's understanding of risk and tolerance of inconvenience.

The effective creation and long-term archiving of electronic documents requires skill and resources. It is a project not to be undertaken lightly. The same can be said, however, about the effective creation and long-term archiving of paper documents.

Data Linking

PenOp is not a stand-alone product. It is a software component intended for use in tandem with a Client Application. PenOp provides a method for signing; then, in coordination with the Client Application, PenOp ties or links the act of signing to something that is meaningful (such as an electronic expense voucher). Thus, the proper interaction between PenOp and its Client Application is critical to the legal effectiveness of the PenOp method of signing.

The Client Application has three primary responsibilities. First, it must make clear to the signer what is being signed. Second, it must inform the PenOp SCS what is to be signed. Finally, it must create an effective archive showing what was signed and what the evidence of the signing is. The archive is effective only if it is meaningful to a third party such as a court or an auditor.

If the Client Application did not perform its responsibilities faithfully, one can imagine the following types of problem:

1. Suppose an assistant hands a pen computer to the president of a company, advising the president that in order to approve a certain contract, he should sign on the Gravity Prompt that appears on the computer's screen. But suppose the screen and prompt present a confusing jumble of information, little of which relates to the contract. If the president is foolish enough to sign this anyway, his action would be ambiguous at best. It would be unclear whether he understood that he was signing a contract, and it would be unclear what the terms of the contract were.
2. Suppose in the same example that the screen and the prompt make very clear to the president that he is signing a specific contract and the screen allows him to see all parts of the contract. He signs on the computer screen, and the PenOp SCS computes a Biometric Token. But suppose that when the Client Application informed the SCS of the content of the contract, the procedure it used was unreliable. Consequently, when the SCS computed the checksum representing the contract, the checksum did not match with the true contents of the contract. It would be unclear whether the Biometric Token matched with the contract.
3. Suppose in the same example that the Client Application competently informs the SCS what the content of the contract is and the SCS creates a sound Biometric Token to memorialize the event. Suppose further that the Client Application archives that token but fails to make a protected archive of the content of the contract. It simply records the Biometric Token and a notation that the token relates to a particular computer file -- which file over time becomes unidentifiable as the computer's records are changed. Obviously, in the event of a legal inquiry, it might be difficult or impossible to show what the president agreed to. The archive does not effectively connect the record of signing with the content of the contract. The content cannot be recreated from the Biometric Token.

These examples point out the urgency of these issues: (a) the integration between PenOp and its Client Application; (b) the security of the environment in which PenOp and its Client Application operate; (c) the logical, unambiguous, controlled, and verifiable operation of PenOp and its Client Application; (d) the systematic and secure creation, cataloging, and long-term protection of the

The Legality of the PenOp Signature

archives showing what was signed, by whom, and when. Each of these issues affects the extent to which the PenOp method of signing would be effective in a practical sense.

Each of these issues also has an analog in the traditional world of paper and ink. Conscientious lawyers instinctively take pains to ensure that traditional documents are well-organized, clearly written, properly paginated, stapled, cataloged and archived, as well as protected from loss, tampering, or damage. A paper document that is not intelligently prepared and preserved is not as effective as it could be, even though it may have a "signature" on it somewhere. Sloppy documents beget ambiguity and misunderstanding.

For traditional documents, paper provided the structure in which to capture, link and preserve legal evidence. For electronic documents signed with the PenOp method, the Client Application must perform an equivalent service. If the application is well conceived and implemented, then it will intelligently gather the relevant information and interact with PenOp. If it is not, then the system is unsound.

When a particular Client Application is united with PenOp, for the purpose of facilitating legal transactions, the system developer would be wise to seek advice of a skilled business lawyer. The lawyer should help the system developer ensure that the electronic data are captured, interrelated, and stored in meaningful ways, just as he would help a client ensure that paper documents are properly composed, paginated, organized, stapled, signed, and archived.

In rendering this advice, the lawyer must be practical. Evidence of a given transaction can be collected *ad infinitum*; more security procedures can always be imposed on records. There are no absolute limits. But there is a practical limit, and to discern it requires good judgment.

User Instructions

Another feature the Client Application should have is sensible, on-line user instructions. Displayed on the computer screen, these would inform the signer how to use the Client Application and how to sign the document the right way at the right time. They would show, for example, how to view all of the pages and parts of the document, where to inscribe the signature, and how to approve or abort a particular inscription. The instructions need to be logical and intuitive. If they are not, the signer may be confused and the practical value of the signer's action declines.

Archives

Ideally, archives created by the Client Application would preserve the Biometric Token for each signing, even if the token has already been verified with the SVS. The archive of the token would allow a third party independently to verify the signing. Although logically it may not be necessary for a third party to verify the signing after it has been verified by the SVS, the ability to verify at a later date will appeal to a jury or other authority evaluating a signing.

The PenOp user needs to develop a comprehensive, cradle-to-grave, program for archiving signed documents. The program should ensure that the archives are protected, retrievable, and understandable for the necessary duration (possibly many years). It might incorporate such features as off-site backup of archives, periodic checking of archive media for deterioration, and documentation of system design, control, implementation, and maintenance.³³ The documentation should thoroughly describe all relevant aspects of the PenOp implementation, including such things as the assignment of identifications (IDs) to users, the systematic enrollment of users with the SVS, the algorithms used to compute checksums and to encrypt Biometric Tokens, and the scientific principles on which PenOp is based. This documentation should provide an independent expert everything he would need to confirm the results of a particular signing many years after the fact.

Graphic Representation of Autograph

Technically speaking, it is not required in the computation of a Biometric Token that data reflecting the graphic appearance of the signer's autograph be included. But practically speaking, the inclusion of that graphic data would be wise. The graphic data could have an emotional appeal to judges, juries, or auditors. It is easier to persuade a skeptic that a legal "signing" really occurred if the skeptic can be shown an image that looks like a traditional autograph.

Multiple Signature Attempts

Each inscription of an individual's signature is different from every other inscription of a signature by that individual. Thus, the PenOp SVS cannot verify every inscription with absolute accuracy. Some inscriptions are more verifiable than others; the authenticity of some Biometric Tokens will therefore be more certain than for others. The user should evaluate whether signers should be asked to sign documents more than once so that multiple Biometric Tokens would be available as proof of signing. Multiple tokens, created by the same signer for the same document, increase the likelihood that the signer's inscription of the document can later be proven by the SVS.

Of course, the user should note that this same practice could be applied to signatures on paper documents. It might be easier to verify the authenticity of paper documents if signers signed multiple times. Yet rarely if ever are paper documents signed more than once. For many transactions, proof of the signature is just not perceived as being so important.

Dual Signatures

Another procedure to enhance PenOp's effectiveness is to require dual signatures. An electronic medical record, for instance, might require a signature by both a physician and an attending nurse. Dual signatures make authenticity more certain.

However, the need for dual signatures is no greater and no lesser with PenOp than it is with traditional signing methods.

Witnesses

Yet another practical procedure to make PenOp more effective is the signature witness. (Notaries, discussed in a later section, can also serve as signature witnesses.)

As part of a traditional signing of a document, a lawyer might recommend that one or two witnesses sign the document to show simply that they observed the signer affix his signature. Occasionally, signatures from witnesses are mandated by law (as is common with the signing of wills), but commonly lawyers recommend the use of witnesses even when it is not legally mandated. In these cases, the decision to recommend witnesses is purely a matter of practical judgment. The lawyer makes the recommendation on the basis of his perception of how important it is to obtain reliable evidence that the original signer truly signed the document.

The practice of using witnesses can be applied to PenOp. First, if a witness's signature is required by a statute, the lawyer must interpret the particular statute in light of the considerations outlined in the earlier section titled "Special Signature Laws and Documents". The lawyer might conclude that the witnessing of a signature made through PenOp is satisfactory under the statute.

Second, a lawyer may wish to use a witness for purely practical reasons -- simply to secure more evidence of who signed the document and under what circumstances. A lawyer might recommend that a witness apply the PenOp method of signing in connection with the following representation:

My name is [fill in name of witness]. I witnessed [fill in name of original signer], a person who is known to me, sign the electronic document to which this representation is linked. [He or she] applied [his or her] signature by writing on the screen of a pen-based computer, just as I now do.

Signed: _____

Notarization

Society assigns special status to documents that have been notarized.³⁴ Various federal and state statutes and regulations provide that documents notarized in accordance with certain standards be more readily admitted into courtroom evidence or be accepted by government agencies.³⁵ For example, only those documents that have been acknowledged before a notary may, under some state laws, be recorded in public land records. Laws may even forbid any recognition of certain documents that have not been so acknowledged.

A notary is a public official having certain authority under the laws of a jurisdiction such as a state. In practical terms, the purpose of acknowledging or verifying a document before a notary is to enhance the reliability of the evidence contained in the document. The action of the notary helps confirm the identity and intent of the person signing the document. Usually, the notary is required to take certain steps (such as reviewing identification cards) to confirm the signer's identity.

Unfortunately, the laws on notarial acts are not uniform across the country. Although a Uniform Law on Notarial Acts has been published, it has been adopted by only a handful of states. This lack of uniformity, coupled with the novelty of PenOp, makes it difficult to predict the extent to which notarial acts aided by PenOp would be recognized in any particular case.

Normally, a person acknowledging or verifying a document before a notary must physically present himself to the notary. And normally, the notary must physically observe and sign (and sometimes seal with an inkstamp or perforation stamp) the document being acknowledged or verified. If a person wants the acknowledgment or verification to be recognized as a "notarial act", it may not be wise to depart from these norms. PenOp may not be advisable.

Note: Sometimes people use notaries when they are not legally required. A notary makes for a superior witness to the signing of a document. See the earlier discussion of witnesses. Because a notary is a public official who (normally) keeps public records of his actions,³⁶ the action of a notary can add to the credibility of a document, even if the notary's action does not satisfy the official requirements of a notarial act. Thus, if a PenOp user chooses to have a document witnessed solely for the sake of making the document more believable, the user might consider using a notary as the witness rather than a layperson.

Following is a generic certificate for use with PenOp when a notary is acting solely as a witness. It is for use by a notary who is in the presence of an original signer acting in an individual capacity.

General Controls

As suggested in the section titled "PenOp Information as Evidence," any electronic recordkeeping system should be supported by adequate controls. Controls are the full range of technical, procedural, and environmental factors that ensure an information system is properly designed, implemented, functioning, and protected from abuse. These include, for example, employment of competent professionals to configure and implement the system, testing procedures that confirm the system functions as designed, physical and logical barriers that prevent unauthorized people from accessing and changing software or archives, and backup archives to protect against loss or abuse. Obviously, the credibility of a PenOp-based system is undermined if it would be easy for an unscrupulous person to create a false Biometric Token.

A system is more likely to be well-controlled if it is implemented and maintained by professionals who know what they are doing. Not only do they need to be trained, but they need to be given adequate procedures to follow, such as steps for enrolling new users to the system.

PART III: MANAGING RISK

The creation and storage of a legal record -- any legal record -- is inherently risky. The record might some day be misunderstood by a judge or a jury, even if its words are carefully composed. The record might be susceptible to alteration, even if it resides on paper. The record might be lost, destroyed, or corrupted with time, even if it is controlled by a professional document management firm. The signature on the record might not be verifiable, even if it is penned in longhand with ink. Thus, a legal actor such as an architect who signs a contract or an insurance company that receives a signed release cannot avoid risk. The best that can be done with risk is to manage it.

Risks and benefits must be balanced in any system for creating and storing legal evidence. Obviously, some records -- contracts involving major financial transactions for example -- warrant greater attention and security than do other records -- such as employee expense vouchers.

The benefits of an electronic document system, supported by PenOp, could be considerable. Compared to an equivalent paper-based system, the electronic system could be much more convenient, efficient, and cost effective. The handling, copying, transmitting, cataloging and storing of paper are all expensive, labor-intensive tasks.

Suppose, for example, that a hospital has historically kept patient records on paper. Physicians have approved these records with traditional ink signatures. The hospital spends a fortune every year creating the records, shuffling them from place to place, protecting them from loss, corruption, or unauthorized disclosure, storing them in warehouses, and so on. The hospital could determine that computerized patient records are far more effective than paper records. The electronic records can more efficiently be created, tracked, sent from one physician or nurse to the next, warehoused, and so on. Electronic records can also be copied easily, which facilitates the keeping of protected, off-site backups.

When the hospital decides to adopt electronic records, it must find a new way for physicians to sign records. Any method of signing that the hospital might consider will necessarily entail risks. The PenOp method will entail the risks outlined in this paper, and the reader should seek the advice of counsel. But the significance of those risks is unknowable until they are compared with the risks associated with other options. PenOp's risks may, for instance, be minor when compared with the risks associated with continuing to use paper and ink, which may include the risk that the hospital will devote too much resources to records management.

In this age of rapid technological change, it is common for institutions to employ advanced information technology to make legal records, even when the law's application to the technology is less than crystal clear. An example is optical imaging. Although few legal authorities have categorically stated that optical images of paper documents will be accepted in court or regulatory proceedings, many institutions today do make optical images of their paper archives. And a growing number are destroying the original paper. This practice does carry risk. But some have decided the risk is well worth taking given the tremendous savings realized by discarding bulky paper.

The Legality of the PenOp Signature

In fall 1993, the Association for Information and Image Management held a nationwide videoconference in which the legality of optical storage was discussed by users and lawyers, including Robert Hoagland, Assistant Vice President and Managing Attorney at Property and Casualty Counsel for the USAA insurance company in San Antonio, Texas.³⁷ Mr. Hoagland told the conference that his company had for years been optically imaging the vast majority of its paper documents and then (within 60 days of original receipt) destroying them.

Mr. Hoagland was asked whether USAA had been concerned about the legality of optical images. He responded that USAA had studied the question very carefully. On the one hand, it knew it could save enormous sums of money and achieve vast improvements in service if it imaged and then destroyed documents. On the other hand, it examined the relevant evidence laws and recordkeeping regulations, finding that most were written broadly enough that they could, arguably, be interpreted to allow optical images, even though no authority had ever made such an interpretation. The company concluded that, if it implemented its optical recordkeeping system with adequate controls, it would possess a substantial argument that its records would be legally effective for courtroom and regulatory purposes. It recognized that the images might from time to time be challenged, but rather than recoil from that risk, USAA chose to accept it and manage it. It prepared, with the assistance of its counsel, to meet the challenges if ever they arose.

Since implementing its system, USAA's experience has been better than anticipated. It has on numerous occasions admitted optical images into courtroom evidence, and not once has admissibility been challenged.

USAA's story reflects a mature approach to the legality of new technology like PenOp. USAA's lawyers did not simply say there was a risk and it should be avoided; rather, they helped their client understand the risk, as well as the methods available to minimize it. The business managers at USAA were then in a position to weigh the risk against the benefit. The decision whether and how to use information technology ultimately rests with the client, not the lawyer.

Biography of the Author

Benjamin Wright is the author of *The Law of Electronic Commerce: EDI, Fax and E-mail*, a comprehensive book on the legality of electronic transactions, published by Little, Brown and Company, Boston (tel: +1-800-331-1664 or +1-617-227-0730; fax: +1-617-890-0875). He is also editor of *EDI Forum: The Journal of Electronic Commerce*, published by EDI Group, Ltd. (tel: +1-708-848-0135; fax: +1-708-848-0153). He is a frequent speaker at industry and professional conferences, and he regularly teaches seminars on the law of electronic commerce.

An independent attorney practicing in Dallas, Texas, Wright earned his law degree in 1984 from Georgetown University. He welcomes comments on this paper.

Benjamin Wright
3431-1/2 Granada Ave.
Dallas, TX 75205-2233
U.S.A.
Tel: (214) 526-5254
Fax: (214) 526-0026
Internet: Ben_Wright@compuserve.com

Endnotes

¹ Following is a discussion of checksum, as used in PenOp, written by CPK Smithies, Technical Director of Peripheral Vision:

A checksum is a number computed electronically from a relatively large amount of computer data. Computer data are always stored as sequences of numbers, and the crudest form of checksum amounts merely to adding all these numbers up together. Checksums are used as evidence whether two sets of data are identical. The advantage of using a checksum is that it is a good deal smaller than the original data. Given an original set of data D, and a checksum of those data C, it is possible to compute a second checksum C2 on a second set of data D2, and by comparing C2 with C it is possible to say with what probability D2 is identical to D. Modern checksumming algorithms, as used within [PenOp], can offer a probability of error of about one in two-to-the-power-of-eighty, or about one in ten to the power of 24. This compares favorably with the probability of error in any currently available forensic test.

² Uniform Commercial Code Section 2-201 provides:

[A] contract for the sale of goods for the price of \$500 or more is not enforceable by way of action or defense unless there is some writing sufficient to indicate that a contract for sale has been made between the parties and signed by the party against whom enforcement is sought.

³ The conclusion in the text applies to American law. A similar conclusion appears likely to apply under English law. In his thoroughly researched book *Paperless International Trade: Law of Telematic Data Interchange* (Singapore: Butterworths Asia 1992) at 83-84, Toh See Kiat observes:

It is clear . . . that English law has very few rules about what a 'signature' should be. Except where statute stipulates otherwise, a signature is any mark placed anywhere on a document which points to a person who has intention to be bound by it. . . . [A] telematic signature is undoubtedly possible in English law.

⁴ 25 B.C.L.R. (2d) 377 (S.C. 1988).

⁵ 17 C.F.R. Section 232.302, as amended by 58 Fed. Reg., Mar. 18, 1993, 14628 at 14674.

⁶ 58 Fed. Reg., Jan. 13, 1993, 4079.

⁷ 48 N.H. 487, 488 (1869). Other cases hold that simple codes or names on telegrams and telexes can be signatures. See, e.g., *Hillstrom v. Gosnay*, 188 Mont. 388, 614 P.2d 466 (1980); *Joseph Denunzio Fruit Co. v. Crane*, 79 F. Supp. 117 (S.D. Cal. 1948). See generally, W. Jaeger, *Williston on Contracts*, Section 587 (3d ed. 1961); *Electronic Messaging Services Task Force, The Commercial Use of Electronic Data Interchange - A Report*, 45 Bus. Lawyer 1645, 1688 n. 177 (June 1990); B. Wright, *The Law of Electronic Commerce*, Section 16.4 (1991). One solitary American case stands in contradiction to the proposition that a code or name on a telegram can be a signature. In reaching this anomalous holding in *Pike Industries, Inc. v. Middlebury Associates*, 398 A.2d 280 (Vt. 1979), the Vermont Supreme Court failed to analyze the issue carefully or to consider any of the many other decisions on the matter. No reported case has ever cited *Pike Industries* as support for the proposition that a name on a telegram cannot be a signature. See, B. Wright, *The Law of Electronic Commerce*, Section 16.4.1 (1994 supp.).

⁸ Some observers may disagree with the proposition that a legal signature need not be secure or carry forensic value, and in support of their disagreement they might cite the anomalous case *In re Carlstrom*, 3 U.C.C. Rep. Serv. 766 (Callaghan) (D. Me. Bankr. 1966). It holds that to be a signature under U.C.C. Section 1-201(39), a symbol must be "susceptible of evidentiary connection to the signatory." *Id.* at 773. This is a confusing and misguided standard. See, B. Wright, *The Law of Electronic Commerce*, Section 16.4.4, n.35. Be that as it may, this standard would appear to be satisfied by the PenOp method of signing because it generally captures some of the same type of evidentiary information that a traditional signing does.

The Legality of the PenOp Signature

⁹ 388 Pa. Super. 37, 564 A.2d 990 (1989).

¹⁰ See, B. Wright, *The Law of Electronic Commerce*, chap. 16 (1991).

¹¹ Despite the phenomenal weaknesses of traditional signatures, the commercial world is not awash with signature fraud. Two reasons: First, most business people are honest most of the time. Second, evidence of who is responsible for a document comes from much more than the signature. It comes from all the facts and circumstances that surround the document (the time, place, related transactions, content of the document, and so on).

¹² 947 F.2d 1409 (9th Cir. 1991).

¹³ In the Gilmore case BLM no doubt believed it was looking out for the best interests of the government. BLM likely believed that its traditional signature requirement served the purpose of ensuring that BLM gathered adequate evidence of who submitted the bid in question. Yet a traditional signature gives little more than the illusion of evidence. A traditional signature can be forged, it can be disguised, and it can be difficult to prove in court. Evidence of the authenticity of a document like a bid is much more often proven through all of the facts and circumstances surrounding the document than it is through a signature.

¹⁴ 57 Fed. Reg. 32,185 (July 21, 1992).

¹⁵ Counsel must help its client realistically understand the magnitude of the risk. Counsel should ask questions: Is the authority enforcing the regulation likely to take a hard stand against PenOp? Given the pervasiveness of computer technology in our society today, the answer could well be no. Further, is the authority likely to invest much law enforcement effort on this issue? If the client is acting honestly and responsibly, the more likely answer is no, again.

¹⁶ A regulation might, however, require that a signature be affixed to a physical object, such as a driver's license. Obviously, PenOp method of signing would normally not be suited for satisfying this regulation.

¹⁷ The exception would be if the regulation explicitly required the signature to be "in ink."

¹⁸ See footnote 2 above.

¹⁹ 788 S.W.2d 207, 209 (Tex. Ct. App. 1990).

²⁰ 114 N.H. 711, 327 A.2d 713 (1974).

²¹ See, for example, Section 3.3 of the Model Electronic Data Interchange Trading Partner Agreement and Commentary published by the American Bar Association, 45 Bus. Law. 1717 (1990). Despite the theoretical risk associated with relying on EDI rather than traditional signed paper documents, many thousands of companies confidently use EDI to form contracts. Experience shows that their confidence is warranted, for there have yet to be any reported lawsuits challenging the legality of EDI contracts.

²² Toh See Kiat argues, under English law, that the word "writing" can include data stored on computer media. Toh See Kiat, *Paperless International Trade: Law of Telematic Data Interchange* (Singapore: Butterworths Asia 1992) at 66. As support he cites, among other cases, *Grant v. Southwestern & County Properties Ltd* [1975] 1 Ch 185, 197 (holding that information recorded in microfilm is "written") and *Kelly v. Charmer* (1856) 23 Beav 195, 53 ER 76 (holding that easily erasable information recorded in code is "written").

If, however, a statute requires that a document be "written in ink" or the like, then it will be more difficult to conclude that the required document could be electronic. Rarely do statutes contain such words.

²³ 770 P.2d 1330 (Colo. Ct. App. 1988).

²⁴ B. Wright, *The Law Electronic Commerce*, Section 16.4.2a (1994 supplement).

²⁵ 17 C.F.R. Section 230.405, as amended by 58 Fed. Reg., Mar. 18, 1993, 14628 at 14670. The Securities Act of 1933 defines "write" or "written" as including "printed, lithographed, or any means of graphic communication." 15

The Legality of the PenOp Signature

U.S.C. Section 77b(9) (1988). The Commission maintains that the words "any means of graphic communication" are broad enough to embrace computer methods.

²⁶ The law of evidence in England, while a bit more murky than American law, also generally provides for the admission of reliable computer records. Toh See Kiat, *Paperless International Trade: Law of Telematic Data Interchange* (Singapore: Butterworths Asia 1992) at 224-250. "Despite the difficulties, there are probably many types of computer-printed and computer-created (i.e. computer-compiled) records which are admissible under" Section 4 of the Civil Evidence Act 1968. *Id.* at 243. See also, Rob Bradgate, "Evidential Issues in EDI," Chapter 2 in *EDI and The Law*, Ian Walden, ed., (London: Blenheim Online Publications, 1989), at 23.

²⁷ See, e.g., *Transport Indemnity Co. v. Seib*, 178 Neb. 253, 132 N.W.2d 871 (1965); *King v. State ex rel. Murdock Acceptance Corp.*, 222 So. 2d 393 (Miss. 1969); *United States v. Vela*, 673 F.2d 86 (5th Cir. 1982). See generally, B. Wright, *The Law of Electronic Commerce*

²⁸ It is not enough just to have records admitted. To be effective in court, they must also be believed. But believability depends on the same thing as admissibility: control. The better the control, the more believable the computer records.

²⁹ *United States v. Vela*, 673 F.2d 86 (5th Cir. 1982); *People v. Lugashi*, 205 Cal. App. 3d 632, 252 Cal. Rptr. 434 (1988). See generally, Brockett, *Evidence and Trial Advocacy: The Erosion of the Hearsay Objection to Computer Generated Evidence*, 26 Crim. L. Bull. 357 (July-Aug. 1990).

³⁰ P. Giannelli & E. Imwinkelried, *Scientific Evidence* (The Michie Company 1986) at 1-35.

If the scientific technique is novel, the party wishing to use it in court must put on evidence to show its reliability. In judging this evidence of reliability, some courts (those following the famous decision *Frye v. United States*, 293 F. 1013 (D.C. Cir. 1923)) are concerned with whether the technique is generally accepted in the scientific community. Other courts (those following the so-called relevancy approach) are concerned more with whether the technique is more likely than not to provide reliable evidence about the matter in question. Giannelli & Imwinkelried, above, at 9-35.

³¹ P. Giannelli & E. Imwinkelried, above, at 837-838.

³² *Id.* at 792-839. See *United States v. Bruno*, 333 F.Supp. 570 (E.D. Pa. 1971) in which the court refused to allow expert testimony based on the chemical analysis of a document because the court was not convinced the method of analysis was reliable.

³³ See generally, B. Wright, *The Law of Electronic Commerce* Section 6.3.

³⁴ This discussion of notarization is limited to wholly domestic transactions within the United States.

³⁵ 58 Am Jur 2d Notaries Public Section 43.

³⁶ Notaries normally keep log books recording their actions. These books are public records that often can be researched in the event of an investigation whether a particular person appeared before a particular notary on a particular date.

³⁷ To obtain a videotape of the conference, contact Association for Information and Image Management, 1100 Wayne Ave., Suite 1100, Silver Spring, MD 20910, USA, +1-301-587-8202. Ask for the videotape titled *Legal Requirements for Document Imaging Systems*.