The Quest for the Paperless Office Electronic Contracting: State of the Art Possibility But Legal Impossibility?

Halina S. Dziewit
James M. Graziano
Christopher J. Daley

Follow this and additional works at: http://digitalcommons.law.scu.edu/chtlj

Part of the Law Commons

Recommended Citation
Available at: http://digitalcommons.law.scu.edu/chtlj/vol5/iss1/6

This Article is brought to you for free and open access by the Journals at Santa Clara Law Digital Commons. It has been accepted for inclusion in Santa Clara High Technology Law Journal by an authorized administrator of Santa Clara Law Digital Commons. For more information, please contact sculawlibrarian@gmail.com.
THE QUEST FOR THE PAPERLESS OFFICE
ELECTRONIC CONTRACTING: STATE OF THE ART POSSIBILITY BUT LEGAL IMPOSSIBILITY?

Halina S. Dziewit†
James M. Grazianott††
Christopher J. Daleyt†††

Despite the availability of high technology in the field of electronic communication and record keeping, the business world almost exclusively relies on the generation and exchange of paper to consummate business transactions and run day to day business operations. Where is the predicted paperless office? This essay does not attempt to determine why the prediction has failed to become a complete realization. What it does analyze is the basic law of contracts in light of the available state of the art computer technology. The issues associated with electronic contracting are encountered under the Statute of Frauds and the Uniform Commercial Code: the requirement of a writing, an authenticating signature to indicate that the terms and conditions of a contract are acceptable to both parties, and document authenticity.

I. CURRENT BUSINESS PRACTICES: THE CONTRACT

Two parties meet with the intent of reaching an agreement for the sale of merchandise. The parties exchange verbal understandings. At some point these verbal understandings are put down on paper. A first draft is generated. The draft is sent by the vendor to the buyer. The buyer marks his copy and sends it back to the vendor. This process generally takes several iterations between the parties before a final written contract is approved and executed to consummate the deal.
The contracting parties depicted above may avail themselves of the existing computer technology. For example, each party probably takes advantage of computerized word processing; electronically retaining the document on magnetic media (tape or disk)\(^1\) to allow easy retrieval, modification, transmission and storage. Each party’s business, if large enough, relays documents between departments or branch offices by electronic mail to prompt comments and suggestions on the documents in real time (in actual or current time rather than at some delayed point in time). Document transmission between independent parties takes place via teletype, facsimile, or overnight mail, thereby eliminating dependency on the U.S. Postal System. Computer network arrangements such as wide area networks (WANs) can be utilized where parties not co-located can electronically exchange information from their place of business in real time, and agree upon contract terms and conditions.\(^2\) Communication may also occur via teleconferencing, either aurally or visually, to allow geographically separated people to conduct a group conference without travel and to achieve compromises and solutions expeditiously.\(^3\) The one common thread in all of the above is that the final document is always expressed in a hard paper copy, carefully “eye balled” by the signatory parties, and executed by appending a handwritten signature to the final printed document.

Although reliance on paper contracting is significant, it is obvious to most astute business observers that contracting via computers provides several advantages in the conduct of business transactions and enhances the ability of businesses to reach their goals and transact business more effectively. Computers have stepped up efficiency, automated record keeping and data retention, provided real-time communications capability, eliminated geographical obstacles and reliance on the postal system, and reduced paperwork as well as the generation of paper.

The realization of these advantages is evidenced by those businesses now taking advantage of a recognized contracting method

---

referred to as Electronic Data Interchange (EDI).\(^4\)

EDI is the electronic transfer of standard business transaction information—invoices, purchase orders, and dozens of other types of transactions—between organizations in a structured application. It is a specialized, structured subset of electronic mail. Electronic Fund Transfer (EFT), although a specialized form of EDI, is usually considered separately. EDI moves information, not money.\(^5\)

The following are examples of how EDI is or can be utilized as a standard way in which to do business:

*At Levi-Strauss, retailers must order jeans a month in advance, unless they use EDI, in which case they can order two weeks ahead. That reduces inventory costs and facilitates the operation of the business.

*The trend in the automotive industry is to deal with suppliers via electronic purchase orders and electronic invoices.

*The Department of Defense may require EDI connections with its 300,000 suppliers and contractors in the next two years. The General Services Administration hopes to issue EDI regulations soon, and has already selected a third party network to handle their EDI commitment.

*In the wholesale drug industry (average profit margin: less than 1%), manufacturers receive 95 percent of all purchase orders via EDI. More than 80 percent of the orders from druggists to distributors use EDI. In the drug business, EDI is the rule, not the exception.

*Banks that started using EDI in the last year now exchange information on-line with 5 percent of their trading partners. That figure may rise to 80 percent in the next three years.\(^6\)

It is predicted that EDI will be a $1.9 billion business by 1992 and that one-third of all business documents will move via EDI by 1995.\(^7\) Today, however, only an infinitesimal fraction of all documents are transferred electronically.

Despite the availability of these technological advances and system implementations by some of the significant industry leaders, there still remains a paper proliferation. Paper copies continue to


\(^5\) Id. at 21.

\(^6\) Id. at 20.

\(^7\) Id.
serve as the standard and accepted way of contracting. Why the dependency on paper? Perception. The nature of electronic expressions raises issues of security, tangibility, reliability, authentication, longevity and validity. To change this perception, the parties must realize that electronic contracting is a legal and technological possibility. In fact, electronic contracting eliminates many of the problems spawned by paper contracts such as the "battle of the forms" and the "mailbox rule".

Since it appears that more problems may be raised as electronic contracting becomes a reality, a discussion of the relevant elements of the law of contracts with respect to the Statute of Frauds, the Uniform Commercial Code and case precedent follows. In particular, significant legal issues arising from electronic contracting will be considered: the requirement of a writing, the need for authenticating signatures demonstrating that the terms and conditions of an agreement are truly acceptable to both parties, and the question of document authenticity.

II. THE REQUIREMENT OF A WRITING

The Statute of Frauds

Under the Statute of Frauds, if the contract takes longer than one year to perform or involves a monetary sum greater than $500, it must be in writing. The writing must specify all the terms and conditions of the contract. Mutual assent to these terms and conditions must be demonstrated by an authenticating mark, typically the signatures of both parties. The rationale behind the Statute of Frauds is to "provide a writing which will afford a basis for believing that the oral evidence offered rests on a real transaction and to ensure the valid existence of a contract." Thus, a writing is required to provide evidence of a valid agreement between the parties.

The writing requirement of the Statute of Frauds can be satisfied by handwritten or typewritten versions of a document or by telegram. A telegram is generated by microwave transmissions or as signals transmitted over electric wires. A transmission which generates a telegram is clearly an intangible method of exchanging

12. ANDERSON, supra note 10, at § 2-201:72.
information to produce a human readable document — a printout. A computer transmission is another intangible method of exchanging information to produce a human readable document. Both the telegram and computer methods of contracting should satisfy the Statute of Frauds in that both can be reduced to a human readable document.

The computer media on which an electronic contract is stored as data provides a permanent record to which a court can turn in the event of a dispute. The lifetime of computer media and the state of the art in storing this media not only ensures the existence of a representation of the parties’ understanding, but endures beyond the lifetime of paper. Should the contents of an electronic contract be brought into question, the data comprising the terms and conditions is immediately retrievable and transformable to a human-readable document.

Further arguments in support of computer contracting can be found in the works of American Jurisprudence. American Jurisprudence on the Statute of Frauds states that “no particular form of language or instrument is necessary to constitute a memorandum or note in writing under the Statute of Frauds, where the Statute does not require that the contract itself be reduced to writing.”13 The only requirement necessary to have a valid contract is mutual assent or a “meeting of the minds”.14 To establish mutual assent, an “objective test is generally to be applied... in determining whether the parties possessed the necessary intention to contract.”15 Therefore, if the parties agree that their intentions are to be expressed on computer media, and that the media is to serve as a reflection of their intent to contract, the Statute of Frauds does not vitiate an interpretation of the above statement. In fact, the language contemplates the existence of an agreement stored in a machine readable language on a computer storage medium from which a printout of the medium’s contents can be generated at any time.

Uniform Commercial Code

The Uniform Commercial Code (UCC) provides an interpretation of what constitutes a writing. Under the UCC, a writing includes “printing, typewriting or any other intentional reduction to tangible form.”16 The “intentional” limitation in the definition “re-

---
15. Id.
lates only to the intending that there be a tangible representation of the intelligence or information" that comprises the subject matter of a contract. Computer storage media, such as floppy or hard disks, are a tangible form that comprise "intelligence" or "information." The data is expressed in machine readable form that can be translated to human readable form, such as a printout. This printout constitutes a tangible representation of the intelligence or information, i.e., contract terms and conditions.

Support for computer contracts as writings is persuasive. Similar to the Statute of Frauds, the UCC provides contracting parties the freedom to express their understanding in whatever form they choose, as long as the chosen form is mutually agreeable to both. UCC Section 2-204 allows "a contract for the sale of goods [to be] made in any manner sufficient to show agreement, including conduct by both parties which recognizes the existence of such a contract," and UCC Section 2-206 states that an offer may be accepted "in any manner and by any medium reasonable in the circumstances (emphasis added)." Therefore, as long as the method and medium are sufficient to show an agreement, or demonstrate that an understanding specifying the terms and conditions of an agreement was achieved, electronic contracting should qualify.

Therefore, the requirements of a valid and enforceable contract may be satisfied by any type of physical computer storage media, where a tangible printout of the media's contents can be generated and the parties intend the media and any printout generated therefrom to be a representation of their contractual terms and conditions. "Temporary visual picturizations" represented on a computer screen, however, are not included within the UCC's "writing" definition, because they are not a "tangible form" of expression and are not permanent.

There are, however, arguments that computer storage media, such as floppy or hard disks, are not incorporated within the writing definition of the UCC because these forms of expression fail the ejusdem generis rule. This rule would "limit the phrase 'or any

---

17. ANDERSON, supra note 10, at § 2-201:71.
19. Id. at § 2-206(1)(a).
21. Id. at Sec. 1-201:380. See BLACK'S LAW DICTIONARY 464 (5th ed. 1979): Of the same kind, class, or nature. In the construction of laws, wills, and other instruments, the "ejusdem generis rule" is that where general words follow an enumeration of persons or things, by words of a particular and specific mean-
other intentional reduction to tangible form' to methods of reduc-

Consequently, computer storage media would not fall within the writing definition because they are not readable by the unaided human eye as are typ-
ing and printing. Further, if magnetic storage media had been intended to be included within the writing definition, "the final 'or' clause would have been drafted to read 'or any intentional reduction to or preservation in any tangible form or on any substance.'" Because the definition does not read in this manner, an interpreta-
tion might be construed to exclude computer storage media. To date, no reported decisions have declared a particular writing insuf-
ficient to satisfy the Statute of Frauds solely due to its form. Therefore, computer storage media containing machine readable in-
formation which can be translated to human readable form should qualify as a writing.

The Statute of Frauds' inclusion of a "telegram" in the defini-
tion of a writing can be further developed by focusing on the UCC's definition of telegram. Under the UCC, a telegram includes "a message transmitted by radio, teletype, cable, any mechanical method of transmission, or the like." This definition has been inter-

It would seem that unless the Code expressly requires that there be a "writing" in a particular case, there is no objection to giving the term telegram an application sufficiently broad to include methods of communication which provide only a temporary visual image and do not make a permanent record.

It appears that Anderson would accept temporary visual expres-

---

22. See supra note 20, at § 1-201:379.
23. Id.
24. Id.
25. See, e.g., ANDERSON, supra note 10, at § 2-201:73.
26. U.C.C. § 1-201(41).
27. ANDERSON, supra note 20, at § 1-201:376.
28. Id.
sions of a contract provided that the parties agreed on this mode of expression to consummate their deal. Although the visual display can be fleeting, it may also be captured in the computer memory. The memory contents can then be generated as a printout at any time following the transaction.

On January 1, 1988 the participants attending the Convention on Contracts for the International Sale of Goods (CISG) preempted the UCC in certain areas. In particular, the CISG documentation provides that "a contract of sale need not be concluded in or evidenced by writing. . . It may be proved by any means, including witnesses." Such an open-ended provision clearly contemplates the admission into evidence of contracts stored on computer storage media in machine readable form, or possibly, contracts expressed as visual displays on computer screens, provided that the courts find such evidence credible to establish the parties' intent to contract and the existence of a contract.

As an aside, the CISG addressed the "mirror image rule", which mandates that each party have identical contracts at the time of consummation. Present computer technology enables the computer to verify the identicalness of the contents of each parties' contract at each user's computer station prior to contract execution. A unique software program would be capable of accomplishing this function. The risks presented by this type of software are indistinguishable from those existing in the manual comparison of paper copies. Clearly, a computer verification as to the identicalness of documents addresses the "meeting of the minds" concern under the Statute of Frauds.

Case Law

Prior case law addressing electronic contracting does not exist. Precedence, however, does exist to uphold the contracting method and medium chosen by the parties to consummate a transaction. In Western Tire v. Skrede, the court states a general rule of contracts: "the offeror can require notice of acceptance in any form that he pleases and may specify the manner in which notice is to be given." In Zamore v. Whitten the court held that under common law, an acceptance must be communicated in the same medium as

---

30. CISG Rule (Art. 11), reprinted in Haarer, supra note 29.
31. Haarer, supra note 29, at 5.
the offer. Therefore, if two parties agree to contract via their computers, the legal framework governing contract intent and expression would not inhibit this agreement. Clearly, EDI subscribers have the intent to use electronic data exchanges to express their commitments. The courts would be hard pressed to disallow this form of contracting where such a result would contradict the intent of the code.

Under the common law, the courts have also upheld the use of contracting via telegrams as valid. In Miller-Crenshaw Co. v. Colorado Mill and Elevator, the Eighth Circuit concluded that the Statute of Frauds was satisfied by the issuance of a telegram. In this case, Miller, through a broker, wired the plaintiff milling company and offered to buy 2,000 barrels of flour. Plaintiff accepted by telegram as expressed in a telegram displaying his signature in typewritten form. The court held that the telegraph acceptance, transaction and signature satisfied the Statute of Frauds.

Similarly, in State Highway Dept. v. Wright Contracting Co., the Georgia Court of Appeals restated the ability of parties to contract via telegrams. The court noted that "[t]here must be mutual assent of the parties, and they must assent to the same thing in the same sense." The phrase "in the same sense" implies that contracting parties, whether they contract by telegraph or computer, must communicate in the same mode as long as both parties agree on the mode.

It is clear that the elements of a writing have surpassed the literal requirement of a penned piece of paper scribed with the terms and conditions of an agreement between parties who have an intent to contract. An electronic expression of contractual terms and conditions stored on computer media appears to be a reasonable extrapolation of the writing requirement. The courts have recognized a variety of contractual expressions as technology has advanced beyond the quill pen, provided that the contracting parties' mutual intent was present and the medium chosen was agreeable to them. It is absurd to believe the courts would now fail to appreciate the current state of the art, and disallow electronic ex-

34. 87 F.2d 457 (8th Cir. 1937).
35. Id. at 458.
36. Id.
37. Id. at 460.
pressions to serve as contractual expressions when the contracting parties do appreciate the available technology and make use of it to conduct business transactions in today's world.

III. THE REQUIREMENT OF AN AUTHENTICATING SIGNATURE

The Statute of Frauds

The Statute of Frauds requires a signature by the person to be charged. This requirement clearly merits discussion in regard to electronic contracting. *American Jurisprudence* on the Statute of Frauds states that:

> [T]he signature must be made or adopted with the declared or apparent intent of authenticating the writing relied upon as a memorandum, and not by way of mere recital or identification. Especially if the signature is affixed by means other than the hand of the signer . . . it is essential that the act be done with intent to authenticate the instrument.

Again, the intent of the parties governs the acceptability of the authenticating “signature.” The Statute of Frauds clearly contemplates the use of something other than a hand-scribed signature as acceptable for authentication.

The Uniform Commercial Code

The UCC adopts a similar definition as that of the Statute of Frauds. The UCC defines “signed” to include “any symbol executed or adopted by a party with present intention to authenticate a writing.” The term “authentication” is included in the definition to “make it clear that a complete handwritten signature is not required.” A signature appended to a contract establishes an “evidentiary connection to the signatory.” The state of computer technology does not preclude the ability to authenticate “a writing” in the context of electronic contracting. The existing laws may be interpreted to encompass computer technology authenticating methods.

Case Law

Case law provides precedent for the requirement of an authen-

---

41. *Id.* at § 362.
42. *U.C.C.* § 2-201 (1972).
43. *Id.* at § 1-201(39).
44. *Anderson, supra* note 20, at § 1-201:295.
45. *Id.* at § 1-201:304.
ticating signature, regardless of whether a written or type-like signature exists. In Kohlneyer & Co. v. Bowen, a standard fill-in form which contained labeled spaces for appropriate information was held to be a contract. This form did not include signature spaces. The court concluded that industry usage and custom provided the requisites needed for signature authentication. The court stated that:

In conformity with the spirit behind the broad definition of "signed", the courts have looked to the writing as well as to the attendant circumstances to determine whether the symbol was executed or adopted by the party with present intention to authenticate, and in the great majority of cases the requisite intent has been found notwithstanding the fact that irregularities appeared on the writings or the niceties and formalities of manual signatures were lacking.

Several judicial determinations support the finding that an actual signature is superfluous, and that any authenticating mark is sufficient to enforce a contract. No court has held an electronic authenticating signature to be unenforceable, except where the parties have expressly agreed that a written signature was necessary. Consequently, an electronic authorization or "electronic signature" appended to an electronic expression of contractual terms and conditions between two parties may sufficiently bind each party. The intent of the parties or the industry custom provides the basis for recognizing an authenticating signature. Thus, an EDI environ-

47. Id. at 404.
48. Id.
49. See Siverton & Co. v. Lolmaugh, 63 Ill. App. 3d 724, 380 N.E.2d 520 (1978) (any mark or symbol with intent to authenticate); Bell v. Washington, 373 So.2d 865 (Ala. Civ. App. 1979) (mutual assent can be shown in ways other than signature); Sanders v. DeWitt, 579 S.W.2d 707 (Mo. Ct. App. 1979) (mutuality of assent may be shown in ways other than signature); Porter v. General Boiler Casing Co., 284 Md. 402, 396 A.2d 1090 (1979) (a signature is not always required to form a valid contract); Rogin v. Dimensions South Realty Corp., 153 Ga. App. 75, 264 S.E.2d 555 (1980) (a promissory note does not require a signature, other forms of assent valid); Hershey Foods Corp. v. Ralph Chapek Inc., 828 F.2d 989 (3rd Cir. 1987) (letters without signatures coupled with actions equals a valid contract, n.5); Manes Organization, Inc. v. Standard Dyeing & Finishing Co., 472 F. Supp. 687 (S.D.N.Y. 1979) (acts of performance replace signed agreement); Ragge v. Bryan, 249 Ark. 164, 458 S.W.2d 403 (1970) (typed initials on an insurance policy equal to a signature if intended as such); Executive Leasing Assoc. v. Rowland, 30 N.C. App. 590, 227 S.E.2d 642 (1976) (silence, signature or conduct equals sufficient manifest intent to accept); Lynge v. Kunstmann, 94 Ill. App. 3d 689, 418 N.E.2d 1140 (1981) (signature not only way to show mutuality or assent); Webb v. Duke, 211 So.2d 722 (La. Ct. App. 1968) (unusual signature raises question of intent to execute).
50. See generally note 49.
The court's acceptance of signatures in any form which indicates an intent to authenticate is clear. In fact, custom in the industry is sufficient to demonstrate acceptance. Signatures, therefore, need not be written where an intent to authenticate is demonstrated. "Electronic signatures" are easily created and appended to electronic contract documents, and an intent to authenticate can be technically demonstrated. The industry custom is established if reliance on a standard electronic procedure, acceptable to both parties as a method of performing business transactions, exists. EDI is an acceptable industry standard which is rapidly becoming the industry norm rather than the exception.

IV. DOCUMENT AUTHENTICITY

The Statute of Frauds

In terms of electronic contracting, the most significant requirement of the Statute of Frauds is document authenticity. Is the document credible? Does this document contain all the true terms and conditions agreed upon by the parties, and thereafter, is the document verifiable by an authenticating signature? Have there been alterations, modifications or even forgery? Can we detect the alterations and the forgery?

In the paper contract world, science has offered and accepted verifiable methods to detect alterations, e.g., ink and paper dating, fingerprint lifting. Signature analysis and "forged" signature detection are sciences in and of themselves. These sciences boast accepted and distinguished world-wide experts on the subject of handwriting analysis. The courts readily admit such scientific evidence to authenticate a written document as being "true." The longevity of handwriting analysis as a recognized science and the court's familiarity with the technical details of the procedure have led to its acceptance as a reliable method of validation. Can the court, however, believe that the electronic expressions of 1's and 0's are an accurate representation of the terms and conditions agreed upon by the contracting parties at the time the authenticating signa-

52. See U.C.C. § 2-202(a) (1976).
54. Id.
ture was appended? Can the contracting parties demonstrate that 1’s and 0’s now under review have not been altered?

Again, science provides a method to deal with document authenticity in the electronic environment. New technology, however, means new authenticity processes, procedures and methods which must be admitted and accepted by the courts. Such processes, procedures and methods are unfamiliar and complex in view of existing scientific methods of paper authenticity. The courts must become knowledgeable as to what demonstrates an original, unaltered electronic expression, and as to what qualifies as competent computer evidence.

The Rules of Evidence

The concept of computer generated documents as credible evidence has been broached in statutes and case law. In 1975, for example, the Federal Rules of Evidence (FRE) were enacted to provide uniformity in dealing with the various items offered for evidence. "The courts have not distinguished computer generated documents any differently than other hand created documents, subsidiary records or reports."55 Further, computer illiteracy has "aided the courts in retaining old principles and applying those rules to computer generated documents and reports."56 The basic criteria for the admissibility of evidence is that it: (1) is reliable; (2) is relevant and credible; (3) is authentic; (4) is in conformance with privacy laws; (5) is not prejudicial; (6) was obtained from an eyewitness or authentic record of the act, condition or event being tried; and (7) is not redundant or representative of prior admitted evidence or rejected evidence, i.e., Best Evidence Rule.57 It is within this framework that computer generated evidence is examined. As of this writing, no case law exists on point with respect to what constitutes competent evidence of electronic contracting.

FRE 1002, titled "Requirement of Original", states that "to prove the content of a writing, recording or photograph, the original writing, recording or photograph is required. . ."58 A "writing or recording" is defined as "letters, words or numbers, or their equivalent, set down by . . . magnetic impulse, mechanical or elec-

56. Id.
57. Id. at 9.
58. FED. R. EVID. 1002.
tronic recording, or other form of data compilation." This definition is expanded in an advisory note to this rule which states:

Present day techniques have expanded methods of storing data, yet the essential form which the information ultimately assumes for usable purpose is words and figures. Hence the considerations underlying the rule dictate its expansion to include computers, photographic systems, and other modern developments. Under this interpretation of FRE 1002, magnetic computer storage media would satisfy the requirements of an original or the "best evidence." Where the physical media is unreadable by humans, the courts have permitted computer printouts to meet the "original" requirement. To confirm this interpretation, FRE 1001(3) defines "original" as "any printout or other output readable by sight, shown to reflect the data accurately, is an 'original.'"

The Business Records Exception

Case law has expanded the concept that computer printouts constitute "original" documents by developing the Business Records Exception to the hearsay rule. Under traditional rules of evidence, a computer cannot be a witness at a trial. Thus, all printed documents and reports should be classified as hearsay. Exceptions to the hearsay rule, however, have been made when there is reason to believe the evidence, although hearsay, is still reliable. The hearsay rule exception applied to computer generated reports is known as the Business Records Exception. This doctrine states that during the regular course of business, entities must consistently maintain reliable records. FRE 803(6) defines "Records of Regularly Conducted Activity", in relevant parts, as:

A . . . data compilation . . . made . . . from information transmitted by . . . a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the . . . data compila-

59. FED. R. EVID. 1001(1).
60. Id. advisory committee's note.
61. See FED. R. EVID. 1001(3). (Emphasis added.)
64. FED. R. EVID. 803(6).
tion, unless the source of information or method or circumstances of preparation indicate lack of trustworthiness.

Thus, the "statements" reflected as printed reports and documents are not deemed to be those of the computer, but rather the statements of the individuals that programmed the computer, input the data, and maintained the programs, equipment, and data. The computer printouts are statements that were supplied to the computer, and the printed reports are the assertion of the truth of such statements.  

The Business Records Exception presents five areas of concern. First, the evidence must be a record. As FRE 803(6) states, a record can be magnetic or electronic images expressed as a data compilation. Second, a qualifying witness must attest to the validity and reliability of the records, reports, documents and equipment. The witness need not be responsible for data input, editing or ensuring data integrity; such person need only be skilled and knowledgeable about the data and procedures followed. The third concern involves identifying the mode of preparation of the record, and the degree of reliance a business organization places on their record. For example, nonuse of the record precludes a Business Record's exception to the hearsay rule. Fourth, the report preparation must be timely. If a report is generated solely for trial, it will be scrutinized carefully for trustworthiness. The final concern is trustworthiness of the records. Adequate safeguards must be utilized to prevent haphazard or intentional entry into the computer record, and assure the credibility of the data's integrity, either with respect to errors or tampering. In particular, there must be controls and safeguards over data preparation, data conversion, error detection and verification, data storage devices, data security and computer accessibility, user and operator training and knowledge, equipment reliability, programming and system capability of computer operation, and data input and output controls.

*The Best Evidence Rule*

In light of the Business Records Exception, the most significant impact on computer evidence stems from the Best Evidence Rule.

---

66. *Id.* at 10.
67. *Id.*
68. *Id.*
69. *Id.*
70. *Id.*
Case law sets forth a number of foundation elements to establish the veracity of a computer printout, and further, to determine the competence of the electronic contract. The relevant elements are:

1. the reliability of the data processing equipment;
2. the manner in which the contract was entered into the computer;
3. the measures taken to insure the accuracy of the contract's contents;
4. the method of storing the electronic document (e.g. floppy disks) and the safety precautions taken to prevent loss of the data while in storage;
5. the reliability of the computer programs and encryption methods used to process the contract's contents;
6. the measures taken to verify the proper operation and accuracy of these programs; and
7. the time and mode of preparation of the printouts of the electronic contact.

To supplement these elements, the testimonies of the person who entered the contract and the computer's custodian are presumably the best evidence.

An electronic contract appears to be admissible as evidence if the printout of the contract is deemed an original and a proper foundation can be established to prove its veracity. The issue of competent computer evidence is not untenable in light of the above discussions. The competency of the evidence, however, must be demonstrated through existing, but complex, computer technology. Judges need to educate themselves and expand their mindset to admit and accept computer technology authenticity procedures and methods as they once learned to admit and accept scientific paper authenticity procedures and methods.

V. COMPUTER TECHNOLOGY: AUTHENTICITY SAFEGUARDS

As any competent hacker knows, access to and alteration of computer files is no problem. Tracing the hacker's source of infiltration can be difficult where unauthorized modifications to computer media expressions are not easily detectable. Computer document authenticity safeguards must be instituted to ensure that the document has not been altered. To satisfy the authenticity re-

---

71. 14 Proof of Fact 2d, Computer-Generated Evidence § 17.
72. Id.
quirement for electronic contracts and meet competent evidence standards, an analogy to paper contract safeguards must be demonstrated to prove the credibility of the electronic contract. This analogy provides the court with a more tangible, realistic, familiar and acceptable basis on which to make a determination as to the credibility of the computer evidence presented.

To satisfy the computer evidence standards, the physical computer and its peripheral equipment must emulate the locked file cabinet. In addition the electronic representation of the contract, whether on computer storage media or a printout, must emulate the paper contract. The authenticity requirements include a demonstration of: identical terms and conditions in the documents held by each party, an authenticating “signature” verifying the consent by both parties to the contents of the contract, and an assurance that no physical alteration, modification, tampering or forgery has occurred at any time during, upon or following the execution of the contract. The document is particularly vulnerable to data tampering during the process of exchanging data transmissions between the contracting parties, and following contract consummation when the computer representation is stored for reference at some later time.

Physical Hardware Safeguards

The first step to ensuring proper document authenticity is to physically restrict access to the computer, i.e., maintain the locked file cabinet. By simply locking the doors to the computer system and its associated terminals, a modest security procedure is in place. Computer access, however, can be achieved via telephone lines by any average computer hacker, thus circumventing physical access restraints.

A variety of hardware and software applications are available to ensure that the locked file cabinet equivalent exists. For example, a call-back modem can provide additional security from intruders. This device responds to a person attempting to gain access to

---

77. Id.
78. Id. at CS40-760-117.
the computer by requesting identification.79 The computer disconnects the call, and telephones a predesignated telephone number stored in the computer's memory and associated with the identified caller.80 This type of security arrangement, although more sophisticated than a locked room, is still subject to circumvention. Fortunately, the state of the art offers more sophisticated methods of preventing access to the computer and computer files stored on computer disks or other computer media.

**Electronic Software Safeguards**

Passwords are typically used to verify the identity of the user attempting to access the computer system.81 The computer software prompts the user to enter a password, which is theoretically known only to the user. Once entered, the password must be verified by software operations before access to the computer's files is granted.82 Password protection attempts to limit access to a single valid user.83 Obviously, several levels of password protection can be utilized and the frequency of password changes can enhance security, making access more difficult and the system more dynamic.

Other increasingly sophisticated methods to validate access to the single authorized user are available. The verification of the single user can be improved by the addition of various peripheral devices that measure some immutable physical characteristic. These devices include fingerprint scanners,84 voiceprint identifiers, and retina scanners. Each of these devices operate with a high level of confidence, and can be programmed to respond only to a single authorized user.85 Clearly, sophisticated hardware arrangements and software methods exist to secure access to computer files, i.e., the locked cabinet analogy. The decision becomes one of economics. The extent of security is proportional to the amount of investment.

Document authenticity further requires that the person to be charged apply a mark on the document indicating intent to authenticate the document, i.e., the equivalent of a signature.86 The actual "signing" or authenticating of the electronic document can be im-

---

79. Id.
80. Id.
81. Id. at CS40-760-112.
82. Id.
83. Id.
85. Id.
implemented in several ways. One method requires two password levels, where a separate "document authenticating password" must be entered. The first level password provides access to the document while the second level password confirms that access is gained by the actual contracting party with the "intent to authenticate." The existence of a dynamic "authenticating password" provides a strong measure of security and demonstrates the "intent to authenticate" by the appropriate contracting individual.

Another means of ensuring document authenticity as well as the "intent to authenticate" involves a software program which, in response to a unique command, immediately checks the identicalness of the document at the transmitting and receiving stations. After a high speed comparison process, the program locks the expression of the document in place so that no modification or alteration can occur. At that point, an authentication handshake from the two stations must occur before the document is processed. Such authentication is in real time, and the password and physical confirmation can be executed on both hardware and software. A "digital signature," subsequently discussed, may also serve to authenticate the electronic document.

In summary, various software safeguards exist which serve to provide evidence of document authenticity. The more sophisticated the system, the more assured the court will be that the integrity of the contract has not been compromised.

**Electronic Computer Media Storage Safeguards**

A further way to ensure document authenticity is through the use of a "digital signature". This computer software employs a complex mathematical formula to produce a series of 0 and 1 bits that are appended to the file to identify its contents. The identification is accomplished by the use of a "hashing" routine that uses each character in the file in a complicated mathematical computation to obtain, for example, a 128 character digital signature. Thus, the digital signature is dependent on the contents of the file. If a single character of the file is changed, then approximately 50 percent of the characters in the digital signature will change, and

---

88. *Id.*
89. Id.
90. *O'Brien, supra* note 74.
91. *Id.* at 58bb.
92. *Id.*
will not match the digital signature of the original document. Utilizing this procedure, the probability of two documents producing the same digital signature is less than one in 1,000 trillion. This adequately ensures that the contents of the original contract cannot be altered without the modification being detectable.

Transmissions Safeguards

Alterations of the contract during transmission between the involved parties is of particular concern with respect to both written and electronic contracts. The written document can easily pass through human hands that can expertly alter the contents of the paper expression. Detecting an alteration in the documents, such as signature forgery or a complete switch in documents, can be extremely difficult. Electronic document transmission is superior to paper document transfers in that sophisticated technology not only allows for secure transmissions, but also detects any tampering.

If rigid security precautions are unnecessary, the document can be transmitted via common carrier telecommunication facilities concurrently with many other transmissions. Anyone can access these transmissions, but locating a specific transmission and associating it with a particular sender is difficult, considering the number of communication channels supported by one common carrier facility. Physical “wiretapping” requires access to a user’s facilities, but is negated if adequate on-site security measures are employed. Therefore, even if security were an issue, the transmission methods and access to sending and receiving stations are already prohibitive.

If security is an issue, a party can encrypt the entire document to achieve a secured transmission. Encryption translates the document into coded form using a secret cypher key. This easily protects the Document from inspection or alteration by third parties. It does not however, protect the sender and receiver from fraud committed by each other, because both have knowledge of the cypher key. More complex encryption systems, involving a third party trustee, are available when the integrity of the contracting parties is in question, but can be costly to implement. The National Bureau of Standards has adopted an encryption algorithm

93. Id.
94. Id.
95. Rosner, supra note 73, at CS40-770-102.
96. Id.
97. Id. at CS40-770-102; Nye, supra note 75, at CS40-760-103.
98. Rosner, supra note 73, at CS40-770-104.
known as the Data Encryption Standard (DES). This encryption standard uses 64 bits, and therefore, does not require extensive processing time or consume much computer storage space. Additionally, the associated software is relatively inexpensive. The software employs complex station to station handshake verification processes, wherein data connections are permitted only between stations having specific handshake characteristics.

A more secure and complex system that minimizes the possibility of fraud by the contracting parties is the RSA Public Key Cryptosystem. This system uses two encryption keys. A “private key”, known only to the document sender, is used to scramble the data, while a “public key”, obtained by the document recipient, is used to decode the received document. The private key is not easily decipherable by the operator of the public key because of the complexity of the cryptosystem. The registered public key will only unscramble data that was scrambled with the private key, thus allowing the parties to identify each other. Again, complex handshake verification operations are used to validate the appropriate transmitter and receiver stations. This system is analogous to handwritten signatures in that the electronic signature can be verified but not easily forged. Where the trustworthiness of the other party is in doubt, this system can be used in lieu of the DES system. In addition to encryption, the parties should maintain thorough records to provide a credible record of the document, its transmission, and reception by the other party.

**Electronic Contracting Competence Summary**

Using minimum and economic security measures, file access security can be implemented by limiting physical access to the computer terminals and employing a user access password scheme where the passwords are frequently changed to ensure file content security. The most cost effective means of implementing the document authenticity criterion is by the use of a separate “document authentication password” procedure where the signing party must prompt the computer with a second password to authenticate the document. The difficulty in locating a particular document

---

100. Krauss, *supra* note 76, at CS40-760-120.
102. *Id.*
103. *Id.*
105. *Id.*
transmission in the typical common carrier network, and the existing software which ensure identicalness of documents through the use of encryption validation keys and handshake verification provide document transmission security.

Obviously, no system is foolproof, and the systems described above are still susceptible to fraud and forgery, although this possibility can be decreased depending on the level of computer security employed. The analogy to paper contracting is achievable in electronic contracting: file access security, document authentication procedures, file content security, and document transmission security. For those wishing to employ computerized contracts, economic factors are of paramount concern. The most secure system would employ strict file access control (e.g., retina scanners), a long digital signature appended to the document, a secure encryption key transmission system, and any available security algorithms. Such a system, however, may be cost prohibitive. One must weigh the economic cost of each separate factor against the increased security provided, in light of long-term usage.

Any business entity adopting electronic document authentication standards must be aware that it may be held to a higher level of security. In The T.J. Hooper v. Northern Barge Corporation, Judge Learned Hand set forth a test applicable to the failure of implementing modern technology. This balancing test weighs the cost of a certain technology against the benefit received. The case involved two tug boats which lacked adequate radios, and consequently were unable to receive a weather forecast warning of an approaching storm. When the barges pulled by the tugs sank during the storm, Judge Hand held for the barge owners. He found the cost of the radios and their upkeep to be insignificant when balanced against the prevention of harm they would have achieved. Clearly, high technology has an investment price; but in the long run, the initial investment when contrasted with the damages realized for lack of diligence might weigh heavily in the direction of significant high technology investments.

106. Rosner, supra note 73.
107. 60 F.2d 737 (2d Cir. 1932).
108. Id.
109. Id.
110. Id.
111. Id.
VI. RECOMMENDATION

This article provides an overview of the legal possibility of electronic contracting, the state of the art available to ensure that legal requirements are satisfied and often times enhanced, an appraisal of the needs of the business community and the existing use of technology to conduct business. No question, the trend in business leans toward the electronic communications method of transacting business. The trepidation in pursuing a complete electronic networking method of doing business lies in part in the unclear nature of the law with regard to high technology. Although case law is slowly addressing the issues associated with electronic communications, such a piecemeal approach will not address the business communities' needs in a timely manner, nor provide consistency in the issues related to electronic contracting. The computer environment is technically complex, and judges, although learned in legal interpretation and application, are not technically skilled in the computer art. They cannot adequately address electronic contracting issues without an appreciation of the state of the art. Therefore, a legislative task force comprised of technical computer and legal experts should develop legislation to address electronic contracting. Such a group could achieve a uniform and informed approach to the use of advanced technology to consummate legal commitments and obligations between parties.

Electronic contracting: the state of the art and a legal possibility—the quest for the paperless office is achievable, provided industry is willing to accept electronic contracting as standard business conduct.