UIC John Marshall Journal of Information Technology & Privacy Law

Volume 12
Issue 4 *Journal of Computer & Information Law - Spring 1994*

Article 1

Spring 1994

Electronic Data Interchange: Uses and Legal Aspects in the Commercial Arena, 12 J. Marshall J. Computer & Info. L. 511 (1994)

Robert W. McKeon Jr.

ELECTRONIC DATA INTERCHANGE: USES AND LEGAL ASPECTS IN THE COMMERCIAL ARENA

by ROBERT W. MCKEON, JR.*

Electronic Data Interchange ("EDI") is computer-to-computer communication. EDI is broadly defined as the exchange of coded electronic mail messages which originate in the sender's computer and travel to the recipient's computer.[1] EDI is revolutionizing communication be-

* Member of the New York State Bar; Licence spéciale, Université libre de Bruxelles (1992); J.D., Case Western Reserve University (1991); M.A., Middlebury College (1988); A.B., College of Holy Cross (1987).

Special thanks to Stuart N. Brotman, Esq., Chairman of the International Communications Committee, Section of International Law and Practice, American Bar Association.

1. Benjamin Wright, *Authenticating EDI: The Location of a Trusted Recordkeeper*, 4 SOFTWARE L. J. 173 (1991).

Computers think in terms of binary digits. A binary digit, or bit, is either a zero or a one. The computer recognizes a zero or one based on voltage or current streams, sequences or fluctuations. When the voltage or current is on, *i.e.* above a certain threshold limit, a one is registered. When the voltage or current is zero, or below this threshold, a zero is registered.

A group of eight bits (zeros and ones) is called a byte. The American Standard for Character Information Interchange ("ASCII") has developed a code permitting 255 various symbols (letters, punctuation marks and numerals). Each symbol, *e.g.* the letter lower-case "a", is derived from various eight bit combinations of zeros and ones. Therefore, the computer uses the ASCII code to translate a byte (eight bits) to one of 255 characters recognizable by humans.

Digital communication via telephone cable involves sending data to a modem. The modem converts the digital impulses, representing bits, to analogue (frequency). The information is then transmitted over a telephone cable to a recipient modem. This modem then deconverts from analogue back to digital for the recipient computer. When fiber optic cables are used, a modem transmits information by a stream, sequence or fluctuation in the levels of light intensity.

Computers have two levels of memory. The first is called Random Access Memory ("RAM"). RAM is the working memory of the computer, and data in RAM is lost once the computer is turned off. Data in RAM is reproduced for permanent storage on the hard disk drive of the computer, also known as secondary storage.

The ability to store a transmission, or modify it, is the distinguishing factor between computers and facsimile ("fax") machines. With a transmission between fax machines, the only processing which occurs is the compression and decompression of bits. The decompression results in a copy of the original, and the transmission cannot be stored (ex-

tween suppliers and purchasers. They will now be able to electronically exchange information within a matter of seconds. This more efficient communication is critical to keeping administrative costs down, and makes US industry more competitive.[2] Companies in Europe have already been using EDI to increase efficiency. As stated best by one European businessman, "we can't afford to be inefficient."[3] This article will analyze in three respective sections: EDI, evidentiary issues posed and commercial contracts.

I. ELECTRONIC DATA INTERCHANGE

EDI messages are transmitted via telecommunication systems, usually by telephone networks or satellites. These systems are faster and more efficient than mail, personal meetings or telephone communications.[4] Currently, between 80 and 85 percent of EDI trading partners communicate using a third party service provider.[5]

A. GREATER EFFICIENCY BY LOGGING ORDERS WITH EDI

EDI messages are structured and coded in alphanumeric characters according to a syntax already agreed upon by the sender and receiver.[6]

---

cept as duplicated on paper). However, a fax received by a computer can be stored and altered before printing. Chris Reed, *Authenticating Electronic Mail Messages - Some Evidential Problems*, 4 SOFTWARE L. J. 161, 163 (1991). The terms compression and decompression simply refer to the process whereby only the bits necessary to transmit the symbols on a page are sent over the cable (compression), and the receiving fax decompresses in order to duplicate the page which was sent (*i.e.* spacing and location of symbols on the page).

2. *See PCS Health Systems Inc. Activates New Interactive Computer Network for Health Care Transactions*, BUSINESS WIRE, Sept. 7, 1993. [*hereinafter PCS Health Systems Inc.*].

3. Bruce Fox, *To Tesco, EDI is Nothing New; U.S. Supermarkets Lag Behind U.K. Chain; Electronic Data Interchange*, CHAIN STORE AGE EXECUTIVE WITH SHOPPING CENTER AGE, July, 1993 at 40.

4. B. REAMS, L. KUTTEN & A. STREHLER, ELECTRONIC CONTRACTING LAW: EDI AND BUSINESS TRANSACTIONS § 2.03 at 29 (ed. 1993-94) [*hereinafter* REAMS]. Computers may be directly connected by wiring them together, using private telecommunications capabilities (*e.g.* microwave systems), using public common carrier telecommunications networks (*e.g.* the telephone system) and EDI third party carriers. *Id.*

5. M. BAUM & H. PERRITT, ELECTRONIC CONTRACTING, PUBLISHING AND EDI LAW § 3.1 at 108-09 (1991) [*hereinafter* BAUM & PERRITT].

6. An example of a part of an EDI invoice message is as follows:

N1*ST*The Corner Store$_{N/L}$
N3*601 First Street$_{N/L}$
N4*Big City*NJ*15455$_{N/L}$
N1*SE*Smith Corporation$_{N/L}$
N3*900 Easy Street$_{N/L}$
N4*Big City*NJ*15455$_{N/L}$
IT1*3*CA*12.75**VC*6900$_{N/L}$

Computer software programs are designed to interpret these structures and codes. Thus, information can be easily found, read and processed.[7] In a commercial context, once the recipient computer distinguishes that the received message is a purchase order, the computer then transfers the message into an inventory management program. Thus, without human intervention, the order is logged.

An order logged with EDI is more efficient because it is no longer necessary for the recipient to re-enter an order manually into its own computer, and invoice preparations are facilitated.[8] For example, the recipient can copy the sender's name from the purchase order for invoice message purposes, and also use the product number from the purchase order to immediately refer to electronically stored price lists.[9] This one-time data entry reduces errors,[10] and it is the primary reason why businesses are using EDI.[11]

Other considerations for using EDI to improve a company's market position vis-à-vis non-EDI competitors include on-line data storage, faster management reporting, automatic reconciliation, reduced clerical

---

Reprinted from Data Interchange Standards Association, Inc. (DISA), AN INTRODUCTION TO ELECTRONIC DATA INTERCHANGE 8-9 (1990), *reprinted in* BAUM & PERRITT, *supra* note 5, appendix C 782, 789-90 [*hereinafter* DISA].

In this message, * represents the data element separator and N/L is the segment terminator. A segment is an intermediate unit of information in a transaction set (invoice or purchase order).

ST means ship to, SE refers to remit to, IT1 is item number one, and 3*CA means three cases of 6900 (the supplier brand code) at a unit price of $12.75. *Id.*

EDI syntax is becoming publicly standardized by the American National Standards Institute, Accredited Standards Committee X12 ("ANSI X12") and the United Nations' EDI for Administration, Commerce and Transport ("EDIFACT"). The standard setting is slow and constantly being revised. Many EDI users modify public standards to suit their specific needs. B. WRIGHT, THE LAW OF ELECTRONIC COMMERCE: EDI, FAX AND E-MAIL: TECHNOLOGY, PROOF, AND LIABILITY § 1.1.4 at 10 (1991).

EDIFACT is intended for the international use of EDI, especially in the European Community. This standard is more concerned with customs and import/export regulations. *Id.*

Nevertheless, the ANSI X12 and EDIFACT standards are becoming harmonized, and eventually may become compatible. *Id.*

Another standard is the National Institute of Standards and Technology ("NIST"). This standard permits the use of EDI with and between U.S. federal agencies. This standard also allows for the use of ANSI X12 and EDIFACT standards. *Id.*

One additional standard is the Transportation Data Coordinating Committee ("TDCC"), which has in part been designed to aid the transportation industry. REAMS, *supra* note 4, § 2.07 at 61-65.

7. Jeffrey B. Ritter, *Symposium: Current Issues in Electronic Data Interchange: Defining International Electronic Commerce*, 13 NW. J. INT'L L.& BUS. 3, 22-23 (1992).

8. Barkan, *Preparing for EDI*, 5 HIGH TECH. L.J. 193 (1990).

9. Ritter, *supra* note 7, at 23.

10. *Id.* at 22-23.

11. B. WRIGHT, *supra* note 6, § 9.4.1 at 139.

workload and phone chatter and higher productivity without increasing staff. Moreover, timely communications are enhanced by the rapid exchange of business data, elimination of mail/courier charges, reduced inventory safety stocks and improved production cycle. EDI also provides for uniform communications with all trading partners, *i.e.* customers, suppliers, carriers, banks and financial institutions.[12]

B. CONTRACT FORMATION WITH EDI, PRESENT AND FUTURE SCENARIOS

Logging an order with EDI does not form a binding contract: an offer and acceptance are required. When the order is merely logged, an offer has been made by the sender, and it is subject to acceptance by the recipient. The acceptance may be conveyed back to the original sending computer in the form of an EDI acknowledgment message.[13]

The above scenario requires human intervention to place the order and also to accept it. Nevertheless, "interactive" EDI is coming of age. With interactive EDI, a sending computer, on its own initiative, will make an offer to a recipient computer for the purchase of goods based on the sender's inventory needs. The recipient computer will accept the offer if the recipient has the quantity of product in stock. This two-way conversation between computers will further culminate in negotiations. One computer will make an offer to buy 100 widgets, and the other will respond with a counteroffer of 50 widgets due to a shortage in stock. The computer that made the original offer will thereafter decide on its own whether to accept the 50 widgets or reject the counteroffer and search for another vendor.[14]

C. EDI RECORDKEEPING

EDI eliminates the need for paper, and as EDI is more widely used, businesses and offices will become "paperless."[15] This lack of paper does not impede recordkeeping. On the contrary, EDI messages are easily stored, by both the sender and receiver, for future reference. EDI messages stored on the hard disk drive of a computer provide reliable records due to security precautions such as a system access password or message encryption.[16] Nevertheless, EDI messages may, at either the

12. DISA, *supra* note 6, at 791.

13. B. WRIGHT, *supra* note 6, § 16.1 at 274.

14. *Id.* § 1.1.4 at 4 (supp. 1993).

15. Ritter, *supra* note 7, at 3; Reed, *supra* note 1, at 161.

16. REAMS, *supra* note 4, § 1.02 at 7. The reliability of EDI messages is incertain due to the necessity of a password to log onto to the EDI system before ordering or accepting. This password is only issued to someone with authority to place an order or accept an order. *See id.* The same holds true for encryption, where only the sending and receiving

sender's or recipient's end, be subject to security breaches and tampering.[17]

D. EDI USE TODAY AND FOR THE FUTURE

At present, 60 percent of EDI users are in the manufacturing business, 13.7 percent are in wholesale trade, 8.1 percent are in transport and utilities, 7.7 percent are retailers and all others comprise 10.4 percent.[18] EDI will be the required method of conducting business domestically and internationally in the near future. In addition, interactions between governments and citizens are expected to be reported and stored electronically.[19]

Plans to implement EDI in the US include a conception by the Pentagon to create a system which may aid the President to restructure health care. The Pentagon envisions electronic submission of health care claims to carriers, electronic patient records and data collection to monitor health care costs and quality. This health care information system will better manage defense health facilities,[20] and may be the precursor to part of Clinton's health plan which is expected to call for regional, integrated information networks.[21] Savings of $15 million in five years are estimated at the Veteran's Affairs Department if vendor EDI invoices are used instead of paper.[22]

Along these lines, BankAmerica has instituted its Health Information Service, and PCS Health Systems Inc. has created the Health Care

---

parties know how to encrypt or decrypt the message. *See infra* note 43 (discussing encryption).

17. *See infra* notes 43-45 and accompanying text; *see supra* note 1 discussing how EDI messages may be altered in the RAM memory of a computer, and then re-saved onto the hard disk.

18. REAMS, *supra* note 4, § 1.02 at 8.

19. Ritter, *supra* note 7, at 6.

20. *Network News: The Pentagon's Plan for Putting Defense Firms on the Health Care EDI Offensive*, AUTOMATED MEDICAL PAYMENTS NEWS, May 6, 1993. There are private groups, such as the Workgroup for Electronic Data Interchange which are tackling the business issues concerning the format and conditions under which the system would operate [such as the Work-group for Electronic Data Interchange]. *Id.* However, a network must be implemented. *Id.*

21. *Id.*

22. James M. Smith, *Keep Pressuring Major Suppliers to Use EDI, Consultants Advise VA; Electronic Data Interchange, Veterans Affairs Department; Report from PSI International Inc.*, GOVERNMENT COMPUTER NEWS, June 7, 1993 at 1. The VA is trying to get 220 suppliers to switch over to EDI invoices from the traditional paper ones. *Id.* By using EDI, the VA could process "purchase orders; invoices; eligibility, claims and payments for health care providers and insurers; enrollment certifications and financial information for educational institutions; and applications, defaults and foreclosures for mortgage lenders." *Id.*

Information Network.[23] By using EDI, the services automate claims processing, payments and remittances, and enrollment and eligibility services. Health care providers may then instantaneously update their accounts receivables and billing systems. This will result in savings of $3 billion to $10 billion, since 25 percent of US health care costs are administrative.[24] In addition, doctors and patients will no longer have to spend costly time filling out forms.[25]

Retailers could especially benefit from EDI use. For example, in supermarkets space is premium. Perishable products must be sold quickly and inventory creates high overhead by tying up money. To combat these problems, supermarkets in Europe have implemented EDI and Quick Response ("EDI/QR") programs with their vendors. With the EDI/QR programs, vendor and purchaser share front-end sales data so future demand can be forecasted. Now it is no longer necessary to hold weeks of inventory in stores and warehouses. Because of EDI/QR, only half a week of inventory is stocked in stores, thus freeing up capital.[26]

Other industries considering EDI use include oil and gas. Their goal is to improve business practices by pooling resources through EDI.[27]

II. EVIDENCE AND EDI

Evidence is anything which demonstrates, clarifies or shows the truth of a fact. The sole value of evidence is its ability to persuade the trier of fact, which is in most instances the jury. The admissibility of evidence is determined by the judge.[28] The judge will admit evidence if the evidence is relevant[29] and authenticated.[30]

---

23. *BankAmerica Has New EDI/EFT Service for Health Care*, EDI NEWS, Aug. 23, 1993. [*hereinafter BankAmerica*]; *PCS Health Systems Inc.*, *supra* note 2. The Health Care Information Network is active in nine states, and is the first step towards nationwide EDI for health care. *PCS Health Systems Inc.*, *supra* note 2. This system is being presently operated for a group of insurance carriers. *Id.*

24. *BankAmerica*, *supra* note 23.

25. *PCS Health Systems Inc.*, *supra* note 2.

26. Fox, *supra* note 3.

27. *European Diary*, EUROPE ENERGY, Sept. 3, 1993.

28. FED. R. EVID. 104(a).

29. Relevant evidence is defined as "evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable than it would be without the evidence." FED. R. EVID. 401. In short, evidence is relevant if it tends to prove a pertinent fact.

30. FED. R. EVID. 402, 901. In fact, the judge must admit evidence "if sufficient proof has been introduced so that a reasonable juror could find in favor of authenticity." United States v. Sliker, 751 F.2d 477, 499-500 (2d Cir. 1984), *quoting* 5 WEINSTEIN'S EVIDENCE § 901(a)[01] at 901-17.

EDI messages pose four evidentiary problems:

1. Proving that an electronic communication actually came from the party that it purports to come from;
2. Proving the content of the transaction, namely, the communications that actually occurred between the parties during the contract formation process;
3. Reducing the possibility of deliberate alteration of the contents of the electronic record of the transactions; and,
4. Reducing the possibility of inadvertent alteration of the contents of the electronic record of the transactions.[31]

Generally, electronic transactions may be proven by three types of records when admitted into evidence: a record of the contents of an electronic message during some stage of its existence; a computer audit record which notes the time when the computer issued the message; and, a statistical or analytical report generated from a computer survey of a quantity of stored data.[32]

When relevant and authentic electronic messages are involved, the opposing party may still object to admission of the evidence based on the hearsay and best evidence rules.[33] This section will analyze authentication, the hearsay rule and the best evidence rule as they apply to the admissibility of relevant electronic messages.

A. EVIDENCE MUST BE AUTHENTIC

Authentication is a special aspect of relevancy.[34] Evidence, though necessary to prove a pertinent fact, is not relevant if it cannot be authenticated.[35] Therefore, evidence must pass judicial relevancy scrutiny.[36] Any judicial determination of relevancy, including authentication, is merely preliminary. It is the jury which makes the final determination.[37]

---

31. *Reprinted from* BAUM & PERRITT, *supra* note 5, § 6.23 at 344.

32. B. WRIGHT, *supra* note 6, § 7.1 at 97-98. EDI messages and electronic messages are terms which will be used interchangeably. EDI messages comprise a subset of electronic messages. An example of another type of electronic message is e-mail.

33. *Id.* § 7.1 at 99.

34. Jerome Michael and Mortimer J. Adler, *Real Proof*, 5 VAND. L. REV. 344, 362 (1952).

35. This statement is according to the Notes of the Advisory Committee on 1972 Proposed Rules, *reprinted in* FEDERAL CIVIL JUDICIAL PROCEDURE AND RULES 381-82 (West 1993).

36. If direct testimony is given concerning the authorship of a writing or oral statement, the judge will admit the evidence. J. STRONG, 2 MCCORMICK ON EVIDENCE § 227 at 53 (4th ed. 1992). However, when the authenticating evidence is circumstantial, the judge will admit it if reasonable men could find its authorship as claimed by the proponent. *Id.*

37. *See* United States v. Sliker, 751 F.2d 477, 499-500 (2d Cir. 1984), where Judge Friendly points out that the trial judge was correct in allowing into evidence a taped telephone conversation. The trial judge made a preliminary ruling as to the authenticity of a

1. *Authentication Requires a Sufficient Connection to Avoid Fraud*

In order for evidence to be authentic, a connection must be established between the evidence and the person, place or thing to which it relates. This connection must be sufficient to support a finding that the matter in question is what the proponent claims.[38] For example, a contract may be admitted into evidence when the signature has been authenticated, by having established a connection with a party to the litigation.[39] In *United States v. Sliker*, Judge Friendly identified two methods of authenticating evidence: comparison with other authenticated specimens[40] or distinctive characteristics (including contents)[41] in conjunction with where the evidence was found.[42]

2. *Signatures or Peculiar Knowledge Provide the Sufficient Connection*

The possibility of forged, handwritten signatures has historically been the source of much litigation. Unique, cryptographic digital signatures are possible, as are system passwords, but authenticity will similarly be an issue. Once someone learns the digital signature or password of another, that person will easily be able to duplicate them over and over again, until they are changed. Digital signatures are not likely to be widely implemented in the near future,[43] but passwords are

---

voice on a tape after having heard testimony by that person. *Id.* Judge Friendly stated that it was nevertheless up to the jury to make a final determination of authenticity. *Id.*

38. BAUM & PERRITT, *supra* note 5, § 6.24 at 345.

39. *See* 2 MCCORMICK ON EVIDENCE, *supra* note 36, § 221 at 41-43.

40. United States v. Sliker, 751 F.2d 477, 499-500 (2d Cir. 1984), *quoting Fed. R. Evid.* 901(b)(3). Comparisons may be performed by either the trier of fact (jury) or by expert witnesses. *Id.*

41. *Sliker*, 751 F.2d at 499-500; *quoting* FED. R. EVID. 901(b)(4). Distinctive characteristics include, but are not limited to, "appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances." FED. R. EVID. 901(b)(4).

42. *Sliker*, 751 F.2d at 499-500. Judge Friendly noted two cases where the contents of seized documents, and the location where they were found, provided a sufficient basis for authentication. *Id.*

43. B. Wright, *supra* note 1, at 174 n.2. Digital signatures are the best means for proving authentication. *See* Reed, *supra* note 1, at 170-72. RSA is the digital signature cryptosystem of preference since it is almost impossible to decode and the recipient cannot alter the message. *Id.* This system requires three numbers: N, E (for encryption), D (for decryption). *Id.* at 171. The sender has already given the N and E key to the recipient, but the sender's D key is kept secret. *Id.* The RSA cipher is named after its founders: R.L. Rivest, A. Shamir and L. Aldeman. *Id.* at 170, n.40.

The federal government prefers use of its proposed Digital Signature Standard ("DSS"). Tyrone Power, *Board Questions True Cost of DSS Standard; National Computer Systems Security and Privacy Advisory Board, Digital Signature Standard*, GOVERNMENT COMPUTER NEWS, Aug. 16, 1993 at 1. Vendors to the government will have to pay royalties for using DSS. *Id.* The royalty will be up to 2.5% of their sales revenues for hard-

commonly used.

Nevertheless, digital signatures and passwords should permit authentication of an EDI message, and users should diligently and periodically change them to maintain security.[44] These security precautions should safeguard judicial concerns to protect against forgery. In fact, EDI trading partners which use the ABA's Model Agreement acknowledge that any code or symbol which they designate as a signature will be sufficient for identification and verification that they signed the document.[45]

A statement of origin that accompanies a communication, as with a fax, is not sufficient to establish authentication by means of a signature.[46] However, a message may be shown to have come from a particular person by circumstantial evidence, such as if the message contains facts which were known peculiarly by that person. For example, a telex was authenticated as a communication by the defendant when it had been shown by content that the telex was a reply to a prior letter addressed to the defendant.[47]

3. *Trustworthiness of Evidence to be Authenticated*

When authentication is involved, the ultimate question is trustworthiness. According to the majority rule, an EDI message should be considered authentic if the computer and transmission methods are apparently reliable, when neither the source of information nor method or circumstances of preparation or transmission indicate a lack of trustworthiness.[48] In addition, the burden should be on the opponent of admissibility to demonstrate a lack of trustworthiness.[49]

Before beginning the next sub-parts, please note that some cases

---

ware implementations, and up to 5% for software. *Id.* The software royalty drops to 1% on any portion of the product exceeding $1,000. *Id.* The federal government has been under fire for failing to make DSS free to all users. *Id.* DSS user costs may cause economic fallout. *Id.*

44. Power, *supra* note 43; Michael Kabay, *Securing a Net Security Plan; Workable Guidelines for Devising Network Security Policies*, NETWORK WORLD, Apr. 12, 1993, at 44.

45. Electronic Messaging Services Task Force, *Model Electronic Data Interchange Trading Partner Agreement*, 45 BUS. LAW. 1717, 1731 (1990) [*hereinafter Model Agreement*]. The Model Agreement is a suggested, preliminary contract between trading partners which controls the subsequent contractual arrangements made through the use of EDI. *See infra* notes 136-40 and accompanying text concerning trading partner agreements.

46. Identification messages may be falsified, and, in any event, identification messages only identify the machine, not the sender. Reed, *supra* note 1, at 166.

47. United States v. Weinstein, 762 F.2d 1522 (11th Cir. 1985), *cert. denied*, 475 U.S. 1110 (1986); B. WRIGHT, *supra* note 6, § 8.3 at 112.

48. *See* United States v. Miller, 771 F.2d 1219, 1237 (9th Cir. 1985).

49. *See* United States v. Vela, 673 F.2d 86, 90-91 (5th Cir. 1982); BAUM & PERRITT, *supra* note 5, § 6.24 at 348.

analyzed involve hearsay's business records exception. Analogies are drawn between authentication and the business records exception since both have similar exigencies pertaining to trustworthiness.[50] Keep in mind that trustworthiness considerations should be even more accentuated when computer transmissions are involved, since there is a risk of lost data or malfunction.

4. *Laying the Foundation for Trustworthiness in Majority Jurisdictions*

In federal and most state courts, the witness is not required to have technical knowledge concerning the equipment's methods for data processing and storing. In *United States v. Vela*, computer records were automatically admissible under the hearsay rule if they were created in the ordinary course of business and if circumstantial evidence showed that the records were reliable. In *Vela*, the Court noted that the computer records of telephone bills were sufficiently trustworthy, since they were made by a disinterested company and relied upon by the company in its day to day business. According to the Court, failure on the part of the proponent to "certify the brand or proper operating condition of the machinery involved does not betray a circumstance of preparation indicating any lack of trustworthiness."[51] Moreover, an opponent's contention that the record is unreliable goes to the weight of the evidence, not its admissibility.[52]

The rationale in *Vela* was also applied in *United States v. Linn*, where a computer printout indicating the time and date of a telephone call was admissible and deemed trustworthy even though the "qualified witness" had no personal knowledge of computer programming or how the printout was generated. This knowledge was not necessary since the telephone record was generated automatically and retained in the ordinary course of business.[53] In fact, computer records have been admitted to prove that the defendant altered them, and the fact the records had been altered in no way showed that they were untrustworthy.[54]

---

50. Each have a similar interest in protecting against fraud.

51. *Vela*, 673 F.2d at 90. *But see* United States v. Scholle, 553 F.2d 1109, 1124-24 (8th Cir. 1977), where the original source of the computer program had to be delineated, and procedures for input control including testing for accuracy and reliability had to be presented. Nevertheless, the Court assented to the evidence's admission, stating that any shortcomings went to the evidence's weight, not admissibility. *Id.*

52. *Vela*, 673 F.2d at 90-91.

53. United States v. Linn, 880 F.2d 209, 216 (9th Cir. 1989).

54. United States v. Bonallo, 858 F.2d 1427, 1436 (9th Cir. 1988). In *Bonallo*, the defendant bank employee was convicted of fraud by altering bank transaction records. *Id.* These records amounted to computer data compilations made in the ordinary course of business. *Id.* The Court noted that if ordinary records were proven to have been altered,

Among these federal standards, one scholar has proposed five techniques to create an effective audit trail which will effectively furnish an EDI message recipient with the origins of a particular message. This information will enable the recipient to authenticate the message, if a dispute should later arise involving litigation. The techniques are as follows:[55]

1. the incorporation of a secret password into the message;
2. the return of an acknowledgement from the recipient to the purported sender;
3. if the message crosses a third party computer network, which demands a password from the user before granting access, the delivery by the network to the recipient of audit information showing the message's origin;[56]
4. the incorporation of a transaction serial number into the message to prevent message loss or duplication; and
5. the incorporation of circumstantial information into the body of the message, such as the code "HU567," which by private agreement might mean "apply extra glue to the bottom of the widget."[57]

5. *Laying the Foundation for Trustworthiness in Minority Jurisdictions*

In some state courts, it may be necessary to prove the following facts in order to authenticate:

1. the message came from computer X;
2. the message accurately represents what is in computer X now;
3. what is in computer X now is what was in computer X at the time of the transaction;
4. what was in computer X at the time of the transaction is what was received from the telecommunications channel; and
5. what was received by the telecommunications channel is what was sent by computer Y.[58]

Facts 1 through 4 are established by testimony as to how informa-

---

this fact would "tend to show that they were unreliable." *Id.* at 1435-36. However, in this case, the government introduced altered records to show that they were actually altered. *Id.* at 1436.

55. *Reprinted from* Wright, *supra* note 1, at 175.

56. This "third party network" could even be owned and controlled by the recipient, as long as the trustworthiness of the records is ensured. This arrangement would be classified as an internal recordkeeper. Trustworthiness could be maintained by assigning responsibility of the recordkeeping to trusted employees who are not involved in purchase orders. *See id.* at 176-78 discussing the pros and cons to having an internal recordkeeper as opposed to an external one.

57. This information is common in EDI relationships due to significant, advance testing to ensure reliable communication between trading partners. *Id.* at 175, n.5. Reliability must be confirmed due to potential problems in transmission and software compatibility.

58. *Reprinted from* BAUM & PERRITT, *supra* note 5, § 6.24 at 347.

tion is written[59] to and from telecommunications channel processors, primary storage[60] and secondary storage.[61] To establish fact 5, testimony must be offered concerning the accuracy of the telecommunications channel, along with characteristics of the message which associate it with computer Y. The latter element to establish fact 5 relates to signatures, since signatures associate the message with its source.[62]

These more technical means for laying a foundation for authentication stem from *King v. State ex rel. Murdock Acceptance Corp.* The third prong of the *King* standard requires that the party seeking to authenticate evidence demonstrate, in technical terms, the trustworthiness (reliability) of the sources of information and the methods of the equipment involved. When hearsay's business records exception is implicated, *King* also requires a technical explanation of the equipment involved, *i.e.* the equipment is "standard" and trustworthy. In addition, the records must have been made in the ordinary course of business at or near the time of the recorded event.[63]

In a recent case, the Illinois Supreme Court determined that an unsigned fax was sufficiently authenticated by using the third prong of the *King* test. Technical,[64] circumstantial evidence which proved that the defendant had sent the fax included testimony by the complainant that

---

59. *See* note 1 discussing digital communication and storage.

60. Primary storage refers to the Random Access Memory of the computer. BAUM & PERRITT, *supra* note 5, § 1.10 at 22. This memory is lost once the computer is turned off. *Id.*

61. Secondary storage refers to permanent storage on the hard disk drive of the computer. *Id.*

62. *Id.* § 6.24 at 347-48.

63. King v. State *ex rel.* Murdock Acceptance Corp., 222 So. 2d 393, 398 (Miss. 1969).

> Print-out sheets of business records stored on electronic computing equipment are admissible in evidence if [. . .] (3) the foundation testimony satisfies the court that the sources of information, method and time of preparation were such as to indicate its trustworthiness and justify its admission.

Id. With respect to authentication, only the third prong of the test is necessary. The test in its entirety is set forth in *infra* note 74.

64. According to the Court, this evidence is substantiated by testimony of a person who can explain the business' procedures for compiling information, and who can explain the methods for checking for mechanical and human error. *Id.* The person must be able to explain the operation of the machine and testify that the machine functioned properly. People v. Hagan, 583 N.E.2d 494, 504 (Ill. 1991), *citing* Tapper, *Evidence from Computers*, 8 GA. L. REV. 562, 595 n. 193 (1974). In addition, that person must testify as to the mechanical reliability of the machine. *Id.*

The Court applied the *King* standard to prove authentication, even though *King* concerned the business records exception to the hearsay rule (each one requires the same foundation of reliability, trustworthiness). In any event, it appears that the Court in *Hagan* did not require a strict, technical demonstration by the witness of the equipment's reliability, since the witness only testified as to how she transmitted the fax, not how the fax actually worked by digital communication or her knowledge thereof.

the defendant told him a fax would be sent, a store employee testified that she helped the defendant send the fax, the complainant received the anticipated fax containing the type of information he expected from the defendant, the defendant had used the fax 50 or 60 times prior with no problems, and the fax's cover sheet indicated that it came from the defendant and was sent at that particular store.[65]

An Illinois court similarly found that a bank's computer record was inadmissable since it was not shown that the computer was standard and accurate, or that the method of processing data inside the computer indicated trustworthiness. General testimony saying that other institutions used similar systems and computers was insufficient, especially when a system which performs calculations is involved as opposed to mere information retrieval.[66]

6. *Subsection Conclusion*

Thus, authentication of electronic messages requires the establishment of a connection between the evidence and the person, place or thing to which it relates. The evidence may be authenticated by, *inter alia*, signature or peculiar knowledge. Additional requirements for authentication of electronic messages will differ significantly from one jurisdiction to another. The majority rule is that a witness need not have technical knowledge of the computer's data processing methods or the source of information if the records are used and stored in the company's day-to-day business. The assumption is that a business will regularly use a processing method only if the processing method is trustworthy. However, a minority jurisdiction will require technical knowledge on the part of the witness in order to insure trustworthiness of the electronic messages. This minority rule will demand increased levels of technical knowledge according to the complexity of the processing and transmission methods.

B. THE HEARSAY RULE APPLIED TO ELECTRONIC MESSAGES

Hearsay[67] is an out-of-court statement, offered as evidence in court by someone other than the person who made the statement, to prove that the matter asserted in the statement is true.[68] Hearsay is non-ad-

65. *Hagan*, 583 N.E.2d 494, 501-02 (Ill. 1991). *But see* B. WRIGHT, *supra* note 6, § 8.7.3 at 58 (supp. 1993), arguing that the Court in *Hagan* should have followed instead *Vela*, 673 F.2d at 90 (5th Cir. 1982).

66. People v. Bovio, 455 N.E.2d 829, 833 (Ill. App. Ct. 1983).

67. " 'Hearsay' is a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted." FED. R. EVID. 801.

68. B. WRIGHT, *supra* note 6, § 9.1 at 122.

missible evidence in a court of law.[69]

It is hearsay for X to say in court that Y told him that Y would accept his offer for 100 widgets. However, it is not hearsay for X to say that he directly heard Y accept his offer. This latter example is not hearsay since X is not trying to prove that Y was truthful or sincere. X is only trying to prove that Y spoke the words to accept an offer.[70]

Electronic contracting messages are not hearsay, since they are offered into evidence merely to prove the fact that a legally potent document was issued, (Y issued a message to X to form a contract), not to prove the truth of what is in the document.[71] Therefore, with respect to electronic contracting, the issue is not Y's state of mind, that is, whether he was sincere in accepting and really wanted to buy the widgets. The issue is whether Y sent to X an electronic message of acceptance, and if so, whether that message is admissible evidence to prove that fact.[72]

Nevertheless, in order for EDI messages to be admitted for the truth of their contents, the messages must qualify under one of the exceptions to the hearsay rule. The applicable exception to the rule is that which concerns records of regularly conducted activity: the so-called "business records exception."[73]

Admission under this exception is similar to authentication. The business records exception requires a party to successfully lay a founda-

---

69. FED. R. EVID. 802.

70. B. WRIGHT, *supra* note 6, § 9.1 at 122-23. Double hearsay is of course inadmissable. A double hearsay scenario would involve Z testifying in court that X said Y accepted X's offer. In this case, Z would be testifying as to the truth of X's statement (*i.e.* that Y spoke the words to form a contract). *Id.* § 9.1 at 123.

71. BAUM & PERRITT, *supra* note 5, § 6.27 at 354; Comments to the Federal Rules of Evidence for US Courts and Magistrates, Rule 801(c), *reprinted in* J. KAPLAN & J. WALTZ, CASES AND MATERIALS ON EVIDENCE appendix B at B-71 (6th ed. 1987) [*hereinafter* Fed. R. Evid. Comments], *quoting* Emich Motors Corp. v. General Motors Corp., 181 F.2d 70 (7th Cir. 1950), *rev'd on other grounds* 340 U.S. 558 (1951).

72. B. WRIGHT, *supra* note 6, § 9.1 at 122-23, *quoting* E. CLEARY, MCCORMICK ON EVIDENCE § 249, at 732-33 (3d ed. 1984).

73. This exception to the hearsay rule includes:

> [a] memorandum, report, record or data compilation, in any form, of acts, events, conditions, opinions, or diagnoses, made at or near the time by, or 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 memorandum, report, record or data compilation, all as shown by the testimony of the custodian or other qualified witness, unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness.

FED. R. EVID. 803(6).

Other exceptions to the hearsay rule applicable to electronic messages include "public records and reports" (803(8)), and the catch-all "residual exception" (803(24)). For an analysis of these two exceptions, *see* B. WRIGHT, *supra* note 6, §§ 9.2.2-9.2.3 at 126-28.

tion which shows that the records are trustworthy.[74] As with authentication, the courts disagree as to whether technical knowledge on the part of the witness is necessary, and as to whether the equipment used must be shown as "standard."[75]

Presently, there is no case law which involves the admission of EDI messages under the business records exception to the hearsay rule. Indeed, it is not even necessary for EDI messages to qualify under this exception. A litigant will not offer EDI messages into evidence for the truth of their contents (hearsay), but will instead seek to have the messages admitted to prove that the sender obligated himself to buy something, to show that the order existed (not hearsay).[76] Nevertheless, if EDI messages qualify under the exception, some scholars maintain that the messages should constitute *a fortiori* proof of verbal conduct, when truth of contents is not at issue.[77] According to *Vela*, EDI messages will qualify since "computer data compilations . . . should be treated as any other record of regularly conducted activity."[78]

C. THE BEST EVIDENCE RULE

According to the best evidence rule, in order to prove the content of a writing or recording,[79] the original is required.[80] An original is, *inter alia*, the printout or other output readable by sight which accurately

---

74. FED R. EVID. 803(6) allows for the admission of business records when they are "(1) made or based on information transmitted by a person with knowledge at or near the time of the transaction; (2) made in the ordinary course of business; and (3) trustworthy, with neither the source of information nor method or circumstances of preparation indicating a lack of trustworthiness." United States v. Miller, 771 F.2d 1219, 1237 (9th Cir. 1985).

Compare the federal standard with that used by some state courts:

> Print-out sheets of business records stored on electronic computing equipment are admissible in evidence if relevant and material, without the necessity of identifying, locating, and producing as witnesses the individuals who made the entries in the regular course of business if it is shown (1) that the electronic computing equipment is recognized as standard equipment, (2) the entries are made in the regular course of business at or reasonably near the time of the happening of the event recorded, and (3) the foundation testimony satisfies the court that the sources of information, method and time of preparation were such as to indicate its trustworthiness and justify its admission.

King v. State ex rel. Murdock Acceptance Corp., 222 So. 2d 393, 398 (Miss. 1969).

75. *See supra* notes 51-66 and accompanying text discussing the split between federal and some state courts.

76. B. WRIGHT, *supra* note 6, § 9.4.1 at 139-40.

77. BAUM & PERRITT, *supra* note 5, § 6.27 at 354.

78. *Vela*, 673 F.2d at 90, *citing* Rosenberg v. Collins, 624 F.2d 659, 665 (5th Cir. 1980).

79. " 'Writings' and 'recordings' consist of letters, words, or numbers, or their equivalent, set down by handwriting, typewriting, printing, photostating, photographing, magnetic impulse, mechanical or electronic recording, or other form of data compilation." FED. R. EVID. 1001(1).

80. FED. R. EVID. 1002.

reflects the stored data in a computer.[81] This subsection offers three interpretations of the possible application of the best evidence rule to electronic messages. Under all three, a record of the message will be admissible.[82]

First, Benjamin Wright correctly argues that by definition the best evidence rule is not applicable since proving the contents of an electronic message is not necessary to establish that a party issued a statement forming a contract.[83] However, Wright further asserts that electronic messages exist only for the fraction of time needed to transmit, and are merely saved on a computer's hard drive. He makes an analogy to a taped conversation, where words are spoken and merely recorded onto a cassette.[84] Any dispute over an electronic message will center on the contents of the message, not the contents of any recordings of the message.[85]

This author, however, disagrees with the contention that electronic messages exist only for the duration of transmission. As discussed below in the section concerning the Uniform Commercial Code, EDI messages must be treated as "writings," having a significant duration in time when stored on the tangible medium of a hard disk drive.[86] With EDI messages, there is no oral conversation which lasts for a fraction of time; the "original" messages are written (typed, input) onto the RAM memory of the computer, reproduced (stored, saved) onto the hard disk drive and then another reproduction is transmitted to the recipient computer. An immediate printout of the message in RAM would again be a reproduction. The original is lost once the computer is turned off or the message is deleted from RAM. Evidently this "reproductive" situation particular to computer documents, and photographic prints enlarged from negatives, must have been a factor in deeming an accurate printout of stored data an original.[87]

---

81. FED. R. EVID. 1001(3).

82. B. WRIGHT, *supra* note 6, § 10.5 at 158.

83. *Id.* § 10.5 at 156; Fed. R. Evid. Comments, *supra* note 71, Rule 1002 at B-126 - B-127.

Benjamin Wright is a member of the Texas Bar and scholar in the practice of electronic contracting.

84. B. WRIGHT, *supra* note 6, § 10.5 at 156.

85. *Id.* § 10.5 at 157. This analogy is based on United States v. Gonzales-Benitez, 537 F.2d 1051, 1053-54 (9th Cir. 1976), where the Court ruled that the best evidence rule does not apply when the content of a conversation is at issue. Tape recordings were admissible as evidence of the conversation, and were sufficient to establish what was said. *Id.* The Court maintained that the best evidence rule would have applied if the factual issue had been the content of the tapes (the sounds embodied on the tapes). *Id.*

86. *See infra* notes 108-17 and accompanying text discussing stored computer data or printouts as writings.

87. As with camera negatives, computer data can only be viewed after reproduction has been effectuated. One could argue that everything associated with computer data in-

Second, a less persuasive interpretation of the best evidence rule would be to consider the electronic message as the original writing.[88] If, after transmission, the message is lost, the saved message will serve as secondary evidence.[89]

A third interpretation of the best evidence rule would impose a hierarchy on the records of an electronic message. The rule would act to obtain the best obtainable evidence, preferring the most direct record of the message.[90] This approach is probably the most meritorious if a litigant desires to prove the contents of a message, since the more a message is transmitted, the more likely it may become distorted. Pursuant to the Federal Rules of Evidence, and even under *King*, printout sheets *accurately* reflecting data are originals for purposes of the best evidence rule.[91] In the case of electronic messages, the best obtainable original should satisfy the best evidence rule, and the accuracy of the data would presumably be best preserved on the originating computer's hard disk drive.

D. EVIDENCE SECTION CONCLUSION

Thus, the underlying theme to all three evidentiary issues (authentication, hearsay and best evidence) concerning electronic messages revolves around trustworthiness and accuracy. Evidence is properly authenticated once a sufficient connection has been established, and one means of so doing involves reliable signatures by encryption, password or code. Also, evidence to be authenticated must be derived from trustworthy processing methods and information sources. EDI messages will qualify under the business records exception to the hearsay rule, even though this is not necessary to show that a contract was formed. The trustworthiness of computer-stored business records is conditioned on the reliability of the processing methods and information sources, and the use of standard equipment. Different jurisdictions will place the burden of demonstrating trustworthiness, or a lack thereof, on either the proponent or opponent. In addition, when a party desires to prove the contents of an electronic message, the best evidence rule will not hinder admissibility since the printouts of stored data are considered

---

volves reproductions and translations from an original, where the original existed only in RAM and was destroyed once the computer was turned off. Digital data is converted by ASCII codes to a format readable by laymen. Transmission involves a serial reproduction sent to the modem, where the data is then converted from digital to analogue. A parallel reproduction is also sent to the printer. *See supra* note 1.

88. B. WRIGHT, *supra* note 6, § 10.5 at 157.

89. *Id. See* FED. R. EVID. 1004.

90. B. WRIGHT, *supra* note 6, § 10.5 at 157.

91. *See* King v. State ex rel. Murdock Acceptance Corp., 222 So. 2d 393, 398 (Miss. 1969), read in conjunction with FED. R. EVID. 1001(3).

originals. Moreover, the rule should call for the best obtainable original.

III. CONTRACT LAW APPLIED TO EDI

Contract law pertaining to the sale of goods will be analyzed since the current use of EDI in the United States heavily involves this area of law. Almost all states, and the District of Columbia, have enacted some version of the Uniform Commercial Code ("UCC"), a codified and updated version of the common law.[92]

Article Two of the UCC governs the sale of goods[93] in the enacting states. The UCC is based on three principles: liberal construction,[94] freedom of contract,[95] and good faith.[96] Article Two of the UCC has ex-

---

92. The one exception is Louisiana, which has not enacted some of the UCC's eleven articles (including Article Two pertaining to the sale of goods).

The states have enacted one of three official versions of the UCC, written in 1962, 1972 and 1978. However, the 1978 text is the most important, since 32 states have adopted it. The disparity in versions of the UCC is even more exemplified by the fact that most states have made amendments to the Code. J. WHITE & R. SUMMERS, 1 UNIFORM COMMERCIAL CODE § 1 at 1-2 (3d ed. 1988).

93. Article Two of the UCC applies only to the sale of goods, and is not applicable to security interests. In addition, Article Two does not affect "any statute regulating sales to consumers, farmers or other specified classes of buyers." UCC § 2-201.

Goods are defined as:

> (1) [. . .] all things (including specially manufactured goods) which are movable at the time of identification to the contract for sale other than the money in which the price is to be paid, investment securities (Article 8) and things in action. "Goods" also includes the unborn young of animals and growing crops and identified things attached to realty (§ 2-107).
>
> (2) Goods must be both existing and identified before any interest in them can pass. Goods which are not both existing and identified are "future" goods. A purported sale of future goods or of any interest therein operates as a contract to sell.

UCC § 2-105(1)(2).

94. UCC § 1-102 provides in part:

> (1) This Act shall be liberally construed and applied to promote its underlying purposes and policies.
>
> (2) Underlying purposes of this Act are
>
> (a) to simplify, clarify and modernize the law governing commercial transactions;
>
> (b) to permit the continued expression of commercial practices through custom, usage and agreement of the parties;
>
> (c) to make uniform the law among the various jurisdictions.

95. The provisions of the UCC may be varied by agreement unless expressly prohibited. UCC § 1-102(3). Nevertheless, obligations of good faith, diligence, reasonableness and care carry throughout the Act. By agreement, the parties to a contract may determine the standards of the above mentioned obligations, but these standards may not be "manifestly unreasonable." *Id.*; WHITE & SUMMERS, *supra* note 92, § 3-10 at 184.

96. Good faith is required in every contract under the UCC, and certainly where the sale of goods are involved. WHITE & SUMMERS, *supra* note 87, § 3-10 at 186. *See also* § 2-103(1) where merchants involved in the sale of goods are held to a rigid standard of good

panded the notion of a contract. Pursuant to Article Two, parties may form a contract[97] by any means sufficient to show agreement,[98] including conduct.[99]

Hence, a purchase order (offer) may be accepted by simply promising to ship or actually shipping the goods.[100] An acceptance does not have to agree to the exact terms of the offer, but may state terms which are in addition to those in the offer, or even incorporate different terms.[101]

EDI commercial transactions for the sale of goods necessarily implicate Article Two of the UCC. Such transactions carried out pursuant to Article Two raise issues concerning the statute of frauds, the parol evidence rule and the battle of the forms. Each of these three sections to Article Two will be analyzed below.

---

faith, requiring "honesty in fact and the observance of reasonable commercial standards of fair dealing in the trade."

97. Article One of the UCC defines a contract as "the total legal obligation which results from the parties' agreement as affected by this Act and any other applicable rules of law." UCC § 1-201(11).

98. Article One defines "agreement" as the "bargain of the parties in fact as found in their language or by implication from other circumstances including course of dealing or usage of trade or course of performance as provided in this Act . . . . Whether an agreement has legal consequences is determined by the provisions of this Act, if applicable; otherwise by the law of contracts . . . ." UCC § 1-201(3).

99. "A contract for the sale of goods may be made in any manner sufficient to show agreement, including conduct by both parties which recognizes the existence of such a contract." UCC § 2-204(1).

100. UCC § 2-206(1)(b).

101. UCC § 2-207 states:

> (1) A definite and seasonable expression of acceptance or a written confirmation which is sent within a reasonable time operates as an acceptance even though it states terms additional to or different from those offered or agreed upon, unless acceptance is expressly made conditional on assent to the additional or different terms.
>
> (2) The additional terms are to be construed as proposals for addition to the contract. Between merchants such terms become part of the contract unless:
>
> (a) the offer expressly limits acceptance to the terms of the offer;
>
> (b) they materially alter it; or
>
> (c) notification of objection to them has already been given or is given within a reasonable time after notice of them is received.
>
> (3) Conduct by both parties which recognizes the existence of a contract is sufficient to establish a contract for sale although the writings of the parties do not otherwise establish a contract. In such case the terms of the particular contract consist of those terms on which the writings of the parties agree, together with any supplementary terms incorporated under any other provisions of this Act.

A. THE STATUTE OF FRAUDS

According to the statute of frauds, a contract for sale[102] for $500 or more is not enforceable unless there is a sufficient writing indicating such a contract. The writing must be signed by the party against whom enforcement is sought. A writing is sufficient even if it incorrectly states a term, but the contract is enforceable only to the quantity of goods stated in the writing.[103] Between merchants,[104] however, a mere confirming writing of an oral contract will satisfy the statute of frauds,[105] if the confirming writing is enforceable against the sender.[106] In addition, there are instances when a writing is not even necessary.[107]

1. *Writing Defined*

The writing does not have to state all the material terms of the contract. The writing serves the purpose of showing that a contract was formed, oral evidence may provide the rest.[108] There are only three requirements for a writing:

(1) it must evidence a contract for the sale of goods,
(2) it must be signed (any authentication which identifies the party to be charged), and
(3) it must specify a quantity.[109]

According to the UCC, " 'Written' or 'writing' includes printing,

---

102. When the sale of personal property is involved, a writing is required if the sale is for $5,000 or more. UCC § 1-206.

103. UCC § 2-201(1).

104. UCC § 2-104(1) defines merchant as:

> [. . .] a person who deals in goods of the kind or otherwise by his occupation holds himself out as having knowledge or skill peculiar to the practices or goods involved in the transaction or to whom such knowledge or skill may be attributed by his employment of an [. . .] intermediary [. . .].

105. The effect of a confirming memorandum is to remove the bar of the statute of frauds, not to render the terms of the memorandum binding. Different terms are not binding, and UCC § 2-207(2) restricts certain additional terms. WHITE & SUMMERS, *supra* note 92, § 2-3 at 76-77.

106. The recipient must have reason to know the contents of the writing. Objection to any contents of the writing must be made within ten days after receipt. UCC § 2-201(2).

107. A writing is not necessary when the seller significantly relies on an oral contract to manufacture special goods for the buyer (UCC § 2-201(3)(a)), the defendant admits that a contract for sale was made (UCC § 2-201(3)(b)), or payment has been made and accepted or the goods have been received and accepted (UCC § 2-201(3)(c)).

See also UCC § 1-103, the "estoppel exception." Some states require unconscionable injury or unjust enrichment in order for the estoppel exception to act as a bar to the statute of frauds, others require a defendant's deceitful promise and still others refuse to apply it all together. WHITE & SUMMERS, *supra* note 92, § 2-7 at 95-97.

108. UCC § 2-201, Official Comment 1 (1990); WHITE & SUMMERS, *supra* note 92, § 2-4 at 83.

109. UCC § 2-201, Official Comment 1 (1990).

typewriting, or any other intentional reduction to tangible form."[110] Evidently the word "includes" allows for other means of producing a tangible document. A tangible medium, for purposes of the Copyright Act of 1976, includes any means of expression from which copyright material can be perceived, reproduced or otherwise communicated, either directly or with the aid of a machine or device.[111] The tangible medium must be able to contain a "fixed" work for longer than just a transitory period.[112] Therefore, an EDI message stored (or "fixed") on the hard disk drive of a computer (or other means) should be a sufficient "tangible form" to qualify as a writing under the UCC, especially when the UCC's principle of liberal construction is applied.

The ABA has issued a report which states that a stored EDI message "constitutes objective, corroborating evidence, apart from oral testimony of the parties, which demonstrates the possible existence of a contract."[113] The report claims that the EDI message satisfies the writing requirement. Nevertheless, the report further argues that the printout of an EDI record should be sufficient to indicate contract formation if the production onto paper of a stored EDI message is necessary to satisfy the UCC's tangibility requirement for a writing.[114]

A significant case involving non-traditional writings is *People v. Avila*.[115] In *Avila*, the court found a lawyer, who falsified the driving records of his clients, guilty of forgery. The driving records were recorded on computer disks, and culpability under the statute required the falsification of a written instrument (defined as "any paper, document or other instrument containing written or printed matter or the equivalent thereof . . . .").[116] The court held that computer disks satisfy the definition of a written instrument, and the lawyer's conviction was affirmed.[117]

2. *Necessity of a Signature*

The UCC defines "signed" as including "any symbol executed or adopted by a party with present intention to authenticate a writing."[118]

---

110. UCC § 1-201(46).

111. 17 U.S.C. § 102(a) (1988).

112. 17 U.S.C. § 101 (1988).

113. Electronic Messaging Services Task Force, *The Commercial Use of Electronic Data Interchange — A Report and Model Trading Partner Agreement*, 45 BUS. LAW. 1647, 1686 (1990).

114. *Id.* at 1688, n.177.

115. 770 P.2d 1330 (Colo.App. 1988). *See also* Opinion of Justices, 114 N.H. 711, 327 A.2d 713 (1974)(registering a vote in a voting machine was considered a written ballot).

116. *Avila*, 770 P.2d at 1332.

117. *Id.* at 1332, 1335.

118. UCC § 1-201(39).

A complete signature is not required; authentication may be printed, stamped or written; and a signature may also include initials, a thumbprint, a billhead or a letterhead.[119] The issue regarding signatures is whether the party executed or adopted the symbol to authenticate the writing.[120]

The subsection of this article concerning authentication of evidence provides examples on how to effectively trace "signatures" back to their makers, such as system passwords and audit trails. One recent case specifically addresses the signature requirement of the statute of frauds with respect to facsimile transmissions. In *Parma Tile v. Estate of Short*,[121] a contractor guaranteed payment of goods to be delivered to its subcontractor. The guarantee was faxed to the seller, but it was not signed and merely contained the contractor's letterhead. The seller relied on this guarantee and delivered the goods. Both the contractor and subcontractor refused to pay, claiming that the statue of frauds requires a written signature at the end of the writing.

The Court acknowledged that a signature is required since it proves "assent to the terms of the guarantee, is associated with seriousness and deliberation, and confirm's the guarantee's existence and the intent of the guarantor to be bound."[122] However, the Court went further to say that any symbol or signature located anywhere on the document will suffice "so long as the intent to be bound is demonstrated."[123]

The Court held that the defendant-contractor's letterhead on the facsimile transmission satisfied the statute of fraud's signature requirement and was an enforceable guarantee. In addition, the Court stated that the defendant-contractor "should not be permitted to evade its obligation because of the current and extensive use of electronic transmissions in modern business transactions."[124]

3. *Subsection Conclusion*

Therefore, a stored EDI message should satisfy the writing requirement of the UCC's statute of frauds since the message has been reduced on a tangible medium on the hard disk drive. Liberal construction of the UCC's tangible form requirement should include EDI stored messages since the law must keep pace with developing technologies and advancing business practices. In any event, a printout will qualify as a writing since it has reduced data to a traditional, tangible form.

---

119. Official Comment 39, UCC § 1-201.

120. *Id.*; WHITE & SUMMERS, *supra* note 92, § 2-4 at 80-81.

121. 590 N.Y.S.2d 1019 (Supp. 1992).

122. *Id.* at 1020.

123. *Id.*

124. *Id.* at 1021.

Moreover, an EDI message will be properly signed with any symbol, including a password, encryption, code or initials.

B. THE PAROL EVIDENCE RULE

According to the parol evidence rule of the UCC,[125] if the court determines that a writing is the *complete* and *exclusive* statement of the terms of the parties' agreement, the writing *alone* is the contract.[126] However, if the writing does not contain all the terms agreed upon, other evidence may be offered to prove the additional terms; but the writing's terms themselves may not be contradicted with other evidence, nor may they be explained or supplemented with anything contradictory.[127] In addition, a judge may exclude evidence of terms extrinsic to the writing if he believes the proffered evidence is not credible.[128]

The first obstacle with the UCC's parol evidence rule is that it only applies when there is a writing. As discussed in the writings part of the statute of frauds subsection above, documents stored on a computer's hard disk drive should constitute a writing. These are tangible mediums for purposes of the Copyright Act and should be tangible forms for the UCC's writing definition.

Assuming the parol evidence rule applies to EDI messages, it becomes apparent that there will be much extrinsic evidence proffered during litigation. EDI messages are usually very concise, and evidently do not cover every possible term which ought to be included in a contract. An EDI purchase order may simply identify the buyer and state a quantity of goods. If the seller sends a confirming acknowledgement, there is a contract with many terms left out.

Under such circumstances, the parol evidence rule will be indispensable. Trading partner agreements, which are reduced to writing[129] at

---

125. UCC § 2-202 defines the parole evidence rule.

> Terms with respect to which the confirmatory memoranda of the parties agree or which are otherwise set forth in a writing intended by the parties as a final expression of their agreement with respect to such terms as are included therein may not be contradicted by evidence of any prior agreement or of a contemporaneous oral agreement but may be explained or supplemented
>
> (a) by course of dealing or usage of trade (Section 1-205) or by course of performance (Section 2-208); and
>
> (b) by evidence of consistent additional terms unless the court finds the writing to have been intended also as a complete and exclusive statement of the terms of the agreement.

Id.

126. WHITE & SUMMERS, *supra* note 92, § 2-9 at 103.

127. *Id.* at 104.

128. *Id.* at 105.

129. This is a common term for the printout of a document stored in a computer hard drive or on a disk.

the outset by the EDI parties, may contain terms which are to be part of every subsequent electronic contract between the parties. The parol evidence rule will admit these terms along with any credible oral evidence proving additional terms. Moreover, the parol evidence rule will permit course of dealing, usage of trade and course of performance to explain or supplement EDI contracts.

C. THE BATTLE OF THE FORMS

At common law, a contract could be formed only if the offer and acceptance were mirror images of each other. An acceptance with different terms amounted to a counteroffer, and payment by the initial offeror would create the contract based on the counteroffer's terms. Therefore the last form usually succeeded as being the contract.[130]

As stated above, the UCC has expanded the notion of contract. UCC § 2-207[131] has for the most part discarded the mirror image rule, and makes many common law counteroffers into acceptances. Section 2-207 allows for contract formation even though there are additional terms in the acceptance.[132] Nevertheless, there is a limit as to how far a diverging acceptance may go and still form a contract. Scholars believe that there must be a mirror image concerning material terms such as price, quality, quantity and delivery. Diverging terms in an acceptance relating to warranty, arbitration and the like, usually found on the back of standard forms, will not hinder contract formation between the parties.[133]

The extent of the application of section 2-207 to EDI transactions is questionable. EDI messages are very concise, coded messages which normally indicate the price, quantity and shipping date. Trade terms and conditions ("TTCs"), indicating warranties, arbitration, etc., are not usually transmitted by EDI software since they are free-text and not coded. In any event, it is not economically feasible to transmit TTCs due to EDI user fees.[134]

Thus, even under the UCC, diverging terms in an acceptance regarding the price, quantity, quality or date of shipment will not likely form a contract, but merely a counteroffer. Therefore the acceptance must mirror the offer with respect to these terms. A lack of agreement concerning TTCs may initiate application of the UCC's contract, gap-fil-

130. B. WRIGHT, *supra* note 6, § 17.2 at 312-13; WHITE & SUMMERS, *supra* note 92, § 1-3 at 30.

131. The text is reprinted in note 101, *supra*.

132. Between merchants, a contract will still be formed, but materially altering terms will not be considered part of the contract. Terms that do not materially alter the contract will become part of it. *See* UCC § 2-207(2)(b).

133. WHITE & SUMMERS, *supra* note 92, § 1-3 at 30, 33.

134. B. WRIGHT, *supra* note 6, § 17.4 at 320-21.

ler provisions, by default.[135]

1. *Trading Partner Agreements*

To avoid default application of the UCC's gap-fillers, some EDI trading partners have created master purchase agreements, which address the TTCs and cover all purchases between the parties.[136] The ABA has written a Model EDI Trading Partner Agreement,[137] which suggests that mutually agreed upon TTCs or each commercial party's TTCs, as specified in their own form documents, be listed in the Agreement's appendix.[138] Benjamin Wright offers an Electronic Trading Letter which allows for the incorporation by reference into the contract of TTCs either transmitted in an EDI message as free text or as mutually agreed upon codes.[139] In addition, the EDI Association has adopted its own form contract which takes into account the EDI rules of conduct of the International Chamber of Commerce.[140]

D. UCC CONCLUSION

An EDI message will satisfy the statute of frauds since it is a signed writing, stored on a hard disk drive and contains some symbol identifying the sender. The parol evidence rule will be indispensable since an EDI message cannot possibly contain all the terms agreed upon. The parol evidence rule will permit the admissibility of a trading partner agreement to prove additional contract terms. The diminished role of the mirror image rule and the battle of the forms under the UCC will not significantly affect EDI contracting. Due to the brevity of EDI messages, transmitted contractual terms will most likely require a mirror acceptance, and TTCs will have already been addressed in a trading partner agreement.

CONCLUSION

The facility of commercial transactions through the use of EDI will enhance the efficiency of U.S. industry. The reductions in administrative costs and unnecessary inventory will ultimately benefit the consumer. Greater efficiency is a must if U.S. industry is going to

135. *See generally* WHITE & SUMMERS, *supra* note 92, §§ 3-4 - 3-9.

136. B. WRIGHT, *supra* note 6, § 17.4 at 321.

137. *Model Agreement*, *supra* note 45, at 1717.

138. *Id.* § 3.1 at 1738. Benjamin Wright points out that the attachment of form documents specifying each party's TTCs will lead to uncertainty should a dispute arise. Nevertheless, the optimal initial agreement between the parties on common TTCs is not likely since this would require extensive, time consuming and costly negotiation. B. WRIGHT, *supra* note 6, §§ 17.4.1 - 17.4.2 at 321-323.

139. *See* B. WRIGHT, *supra* note 6, § 17.4.4 at 324-25, appendix C at 401.

140. BAUM & PERRITT, *supra* note 5, appendix B at 774.

effectively compete worldwide. Europe is becoming more automated and efficient through the use of EDI, and other competitors will certainly follow. U.S. law regarding EDI commercial contracts will not pose an obstacle to further advancement. Security precautions taken to insure proper authentication and record storage, and technological progress guaranteeing trustworthiness, will satisfy evidentiary issues. In addition, the UCC will permit EDI contracts to qualify as writings, and the broad definition of a signature will permit any symbol or code for authentication purposes.