

# **Making Contract By Electronic Data Interchange Over Internet In**

Matej Cepl

LL.M. student, Spring semester '97

International Business Dispute Resolution



## **Introduction**

Purpose of this paper is to show main legal issues of emerging EDI over Internet (henceforth "MIME-EDI") and to differentiate them from traditional EDI over VAN legal issues.

There is much more talking about technology in this paper, than it is supposed to be in a legal paper. However, it is necessary to explain some technological concepts before discussing their legal implications.

## **EDI over VAN**

### **What is EDI and how it works?**

The majority of present companies have their accounting, inventory, etc. based on computers instead of old-fashioned paper folders. It is very convenient, it eliminates most of common errors produced by accountants and administrative personnel and last but not least it is much cheaper compared to salaries of employees.

So, except for of the real decision-making process only one task remains for these expensive and unreliable humans: to fill-in all data. Whenever a new invoice, purchase form, acknowledgment form, etc. comes to the company, it must be manually typed-in to the computer. Whenever any such form is to be sent to the other party it must be printed out and send via mail or (more often today) via fax. Addressee then types this data once again in his own computer. It is unnecessary to explain that such technique produces many mistakes in transmission and it is highly expensive, because there is a need for many workers who types an information, which already was in one computer, into another one.

While these employees are lower-skilled, they are still more expensive than a computer.

Moreover, modern business is based on just-in-time delivery. The need of retyping is so clearly impeding, that more than 20 years ago, in 1970's major manufacturers (particularly Big Three car manufacturers, gas industry & their retailers) began to use modern computer-to-computer mode of communication—Electronic Data Interchange (EDI). This method allowed computers to watch inventory and make orders in real time and so keep very small amount of inventory even in such huge companies.

Another industry that began using EDI in significant manner are major retailers like WallMart or Safeway. They persuaded all their suppliers and retailers to get EDI connection and communicate with them via EDI only. These big companies created in 80's group of cca 150,000 companies worldwide, who constitute whole EDI industry today.

It needs to be emphasized, that EDI is not the same as an e-mails. Contrary to e-mail, which is tool for people-to-people communication, EDI is oriented on computer-to-computer communication. It means that e-mail message is generally same text, as it would be send by fax or mail. It is not so with EDI message, which generally incomprehensible for humans.

Computers of all EDI parties are connected to one common network and through this network they communicate with one another. These networks, called Value Added Networks (VAN), are closed networks with limited number of securely identified customers of one provider.<sup>1</sup> The biggest VANs are: General Electric Information

---

<sup>1</sup> Actually, biggest VANs mentioned below are interconnected, but it is difficult to scale VANs to bigger network, than they are now, contrary to Internet, which is scaleable very easily.

Services,<sup>2</sup> EasyLink by AT&T;<sup>3</sup> IBM offers EDI as part of its Global Network.<sup>4</sup>

The biggest advantages of VANs over the current state of Internet are security, authenticity, secure record-keeping of messages and logistic help. It is a natural result of the fact, that every user is connected to VAN by its own phone connection, so he can be identified. Also every message is stored by VAN and can be used as evidence in a potential dispute resolution.

Promised cut in processing costs should go up to nine tenths of original cost.<sup>5</sup> These are some anecdotal examples of EDI advantages: Premenos technology, company that sells proprietary systems for sending EDI messages over Internet, claims that price of one paper purchase order costs company \$70, but processing similar EDI order costs only 99 cents.<sup>6</sup> Another example (this one is from a retailer company, which already uses EDI) is a British company Tudor Rosa, providing highly specialized services to the British food manufacturing industry, reported that its orders increased tenfold since computerizing its export documentation in 1992. They also benefited from improved efficiency and profitability.<sup>7</sup>

## **Legal issues arising from using EDI**

### **Offer and acceptance by computer**

Can computer make or accept an offer?

The caselaw is very limited (as it is usual in most EDI issues). The case of *State Farm*

---

<sup>2</sup> <<http://www.geis.com>>

<sup>3</sup> <<http://www.att.com/easycommerce/easylink/edi.html>>

<sup>4</sup> <<http://www.ibm.com/globalnetwork/edibr.htm>>

<sup>5</sup> See 13 PCWeek 69 (10/96) Taking care of business the Net way

<sup>6</sup> See 9 Byte 5 (9/96, vol. 21) Internet + VANs = A Serious EDI Platform

<sup>7</sup> See Daily Telegraph from 6/9/1995

*Mutual Auto. Ins. Co. v. Bockhorst*<sup>8</sup> held, that a computer-generated insurance renewal was valid. The court wrote: “Holding a company responsible for the actions of its computer does not exhibit a distaste for modern business practices as State Farm asserts. A computer operates only in accordance with the information and directions supplied by its human programmers. If the computer does not think like a man, it is man's fault.”<sup>9</sup>

Yet another issue is acceptance. Can computer accept offer and so constitute enforceable contract? In *Corinthian Pharmaceutical Systems v. Lederele Labs*<sup>10</sup> court held, that a tracking number automatically issued by computer after order was placed by a touch-tone phone was merely “an automated, ministerial act”,<sup>11</sup> that cannot constitute acceptance. However, it could be argued on the basis of reasoning of the case, that it is possible to accept an offer by any “act that manifests the intention to accept the offer and make a contract” and “in any manner and by any medium reasonable in the circumstances”.<sup>12</sup> The court did not argue against acceptance done by computer itself, but held that purported acceptance did not manifest an assent to the terms of the contract.<sup>13</sup>

Automatic notification of receipt would then certainly not be sufficient as acceptance,<sup>14</sup> because it means just that a computer received message and it was able to read it (that is, the message was not garbled and it was in proper data format).

---

<sup>8</sup> 453 F.2d 533 (10th Cir. 1972)

<sup>9</sup> 453 F.2d at 536

<sup>10</sup> 724 F.Supp. 605 (S.D. Ind. 1989)

<sup>11</sup> 724 F.Supp. at 610

<sup>12</sup> *Id.*

<sup>13</sup> See Benjamin Wright, *The law of electronic commerce, EDI, E-mail & Internet, Technology, proof and liability* chapter XV. (Little, Brown & Co., 1996) (1994) [hereinafter Wright]

<sup>14</sup> Online law: the SPA's legal guide to doing business on the Internet 83 (Thomas J. Smedinghoff ed., Addison-Wesley Developers Press, 1996) [hereinafter Online Law]

## Statute of frauds

Statute of frauds is an issue only in the United States now (even the United Kingdom repealed Statute of frauds in 1954 except for “land contracts” and “suretyship”). Whether or not an electronic record would pass under the U.C.C. Statute of frauds (§ 2-201 and § 1-201(46)) is uncertain.<sup>15</sup> It is being fixed in a more certain way by EDI Trading Partner Agreements<sup>16</sup> now, but it is not certain whether these clauses would be upheld by court.<sup>17</sup> ABA EDI Trading Partner Agreement deals with Statute of frauds in section 3.3.2 by waiver of the Statute of Frauds as available defense by both parties.

The Statute of frauds is under the sharp criticism from many parties. It was repealed in the previous draft of U.C.C. §2-201<sup>18</sup>, but the last draft<sup>19</sup> introduced it again in changed reading, so that authenticated message satisfies it.

New section states that: “Except as otherwise provided in this section, a claim for breach of contract for sale in the amount of [\$5,000] or more is not enforceable by way of

---

<sup>15</sup> Closest to a precedent is probably case of *Hessenthaler v. Farzin*, 388 Pa. Super. 37, 564 A.2d 990 (1989), where a Union Express mailgram was accepted as sufficient “writing” to satisfy Statute of Frauds.

<sup>16</sup> EDI Trading Partner Agreement is old-fashioned paper-based agreement, which establishes parties’ rights and duties in using EDI and is signed before they begin their business via EDI.

ABA—Model Electronic Data Interchange Trading Partner Agreement, 45 Bus. Law. 1645, 1717 [hereinafter ABA Agreement].

<sup>17</sup> See *The Formation And Enforcement Of Electronic Contracts* at <<http://www.uchastings.edu/plri/fall94/whipple.html>>

<sup>18</sup> See draft of U.C.C. in § 1-201(5):

“‘Authenticate’ means to sign or to execute or adopt a symbol, including a digital signal or identifier, or to do an act that encrypts a record or an electronic message in whole or in part, with present intention to establish the authenticity of, or signify a party’s acceptance and adoption of, a record or term that contains the authentication or to which a record containing the authentication refers.”

See <<http://www.law.upenn.edu/library/ulc/ulc.htm>>, where is located a website of The National Conference of Commissioners on Uniform State Laws and where current drafts are regularly posted [hereinafter U.C.C. Art. 2 draft].

<sup>19</sup> <<http://www.law.upenn.edu/library/ulc/U.C.C.2/397art2.htm>>

action or defense against a person that establishes by credible evidence that no oral contract was made unless there is a record authenticated or sealed by the person against which the claim is asserted as the record of that person that is sufficient to indicate that a contract was made. A record is not insufficient merely because it omits or incorrectly states a term, including a quantity term. If the record contains a quantity term, the claim is not enforceable beyond that quantity.”<sup>20</sup>

It has no sense for contracts under CISG, because it specifically invalidates it.<sup>21</sup> However, there is no much need of concern for Statute of frauds in Europe either, because most European law systems have a requirement of writing only for some kinds of contracts not usually closed over EDI (for example, sale of land, employment and finance contracts). Most countries have often very generous definitions of writing also.

### **The choice of law in EDI transactions**

The discussion of choice of law in the United States in case of EDI transaction will probably not be different from the paper-based transaction. If there is no contractual dispute resolution clause in the EDI Trading Partners Agreement, the usual balancing of different factors will take place.<sup>22</sup> These factors are: place of negotiating and closing the contract, place of performance, location of the “subject matter” of contract and nationality of parties.

The only problem may arise in the issue of the place of closing a contract, when the negotiation happened over EDI. However, by the UK precedent deciding the jurisdiction of dispute arising from the contract created by telex can be used by analogy,<sup>23</sup> where court

---

<sup>20</sup> U.C.C. Art. 2 draft § 2-201

<sup>21</sup> Art. 11 of CISG

<sup>22</sup> See Restatement (Second) of Conflict of Laws, § 188

<sup>23</sup> *Brinkibon Ltd. v. Stahlwarenhandelgesellschaft mbH*, 2 AC 34, 1 All ER 293, 2



held that telex communication is “instantaneous communication” most similar to phone communication, so place of contract was at the place where acceptance was received.

However, not every communication would be held instantaneous, even when parties communicated by telex as in *Brinkibon* case. Court held, that the message may not be intended to reach the designated recipient immediately ... No universal rule can [rule] over all such cases; they must be resolved by reference to the intentions of the parties, by sound business practice and in some cases by a judgment where the risks should lie.”<sup>24</sup> So, when there is intention of parties to conclude agreement instantaneously by EDI (as in majority of cases), “the contract (if any) was made when and where the acceptance was received.”<sup>25</sup>

Many transactions involving the international sale of goods are automatically governed by the Convention on the International Sale of Goods. However, such decision on choice of law issue does not rule what a proper court is.

### **Battle of forms**

Famous issue of statute of forms is not likely to have a substantial impact on EDI contracts. The EDI messages are primarily tools of sending standard business forms, so that they have fields containing description of goods, quantity, price etc., but very limited tools for incorporating any additional terms of contract. Even though there is a “free text” field in EDI transaction sets defined, most EDI Trading Partners Agreements specifically prohibit using them for any changes in contract.<sup>26</sup>

---

WLR 264, 1 Lloyd’s Rep 217 (1982)

<sup>24</sup> *Id.*

<sup>25</sup> *Id.*

<sup>26</sup> Communication with EDI administrators on Internet list edi-1@U.C.C.vma.ucop.edu; for information send e-mail to listserv@U.C.C.vma.ucop.edu with sole word “help” in body of message.

Moreover, even if the EDI Trading Partner Agreement does not contain anything concerning “free-text” fields, it is probably not a good idea to use them as a tool of incorporating additional clauses. When EDI messages are “read” by computers, it is not certain what will happen to the “free-text”. Either it will be lost (if receiving program has no action associated with “free-text” field) or it will lay somewhere in the system waiting to be read by officer of addressee and our nice idea of computers talking together without human intervention is lost.

Moreover, there are certain studies remarking, that the “battle of forms” itself is less occurring, than it was in the time of preparing U.C.C..<sup>27</sup>

## **EDI over Internet and Electronic Commerce**

### **Technical issues of EDI over Internet**

The EDI market in early 90's got to its limits. Cost of installment and high prices of monopolized proprietary Value Added Networks was too high compared to relatively small advantages for small companies. Their savings from using EDI were much too small and therefore they stayed mostly with the old manual typing-in method.<sup>28</sup>

In the middle of 1990's Internet<sup>29</sup> began its explosion. It offers fast, very cheap and easily scaleable communication technology which is now available in very affordable prices for everybody. It became obvious, that Internet could offer much better medium for business communication including EDI than old VANs.

---

<sup>27</sup> See Thomas J. McCarthy, The commercial irrelevancy of the “battle of the forms”, 49 Bus. Law. 1019

<sup>28</sup> See 10 PCWeek E1 (3/11/96, vol. 13) Snug fit or mishmash...

<sup>29</sup> Excellent explanation of Internet can be found in case ACLU v. Janet Reno, 929 F. Supp. 824 (1996).

EDI over Internet (thereunder MIME-EDI) creates also wholly different environment of commerce from classical VAN based EDI and thus the created legal issues are also very different.

### **Goals of Internet Commerce**

EDI was not invented in the first place as the tool of online bargaining. The main purpose of its creating was fast exchange of purchase orders and invoices among established trading partners. So, EDI Trading Partners Agreements were enough to rule EDI relations.

However, it is not the same with EDI when it moves to Internet. The main idea of MIME-EDI is not only keeping established trading relationships, but also creating paper-free environment for creating contracts on equal terms ad hoc. It should be an open marketplace, where every aspect of acquisition process is handled seamlessly (participants never need revert to off-line paper communication), where buyers can browse multimedia catalogs, solicit bids, place orders to whomever they wish. There should be possible interactive bidding and bargaining over EDI in real time or posting Requests for Quotations to all possible vendors.<sup>30</sup>

But there are some very serious problems with such commercial use of Internet: Internet is notoriously known to be insecure, so even an average computer professional is able to intercept Internet messages; there is not any widely used method of proving authenticity on Internet, so that without a special and non-standard software nobody can

---

<sup>30</sup> There is one problem unrelated to this paper: Internet has nothing like “Yellow pages”, so there is no possibility of sending message to “all vendors of hazelnuts in Northern California” for example. But, there is being created a new standard, which should allow this, LSDAP; for more *see* <[http://cgi.netscape.com/comprod/at\\_work/white\\_paper/vision/print.html](http://cgi.netscape.com/comprod/at_work/white_paper/vision/print.html)>

use e-mail message as persuasive evidence in court; electronic messages are usually located openly in computers and there is not any standard method of secure record-keeping; and last but not least there has not been created one standard for exchanging EDI messages over Internet yet. Internet Engineering Task Force—group preparing Internet standards—works on special standard for MIME-EDI.<sup>31</sup> The first messages were already sent between two different EDI platforms during the week of January 20, 1997.<sup>32</sup>

### **Digital signatures and security**

Security is the main difference between a current rudimentary state of Electronic Commerce over Internet and proposed state. Main problem is of technological character: there is not an enough widespread security e-mail standard over the Internet yet.

The main idea that underlies all existing keys to resolving problems with insecurity of Internet is a public key encryption.<sup>33</sup> Try to imagine lock that has two keys, one for locking up and the other for unlocking. You would be able to spread out copies of the “locking up key” (let’s call it “public key”) and keep your “unlocking key” (called “private key”), so that everybody who wants to send you a message can lock it in the box and send it to you, knowing that only you can read it.

However, this is only half the way. The lock is so designed, that it works even *the other* way. It means, that whenever *you* lock your message with your private key, only *your* public key can unlock it.

These two methods are the basics of public key encryption. Contrary to classic

---

<sup>31</sup> For more information see <<http://www.ietf.org/html.charters/ediint-charter.html>>

<sup>32</sup> See <[http://www.commerce.net/news/cnet\\_edi.html](http://www.commerce.net/news/cnet_edi.html)>

<sup>33</sup> See <<http://www.pgp.com/privacy/encrypt.cgi>> or William Stallings, Protect your privacy: the PGP user's guide, (Prentice Hall, 1995), and <<http://www.rsa.com/-rsa/S-MIME/smimeqa.htm>>

encryption, when message is encrypted with one key and can be decrypted only with the same one, there are two keys involved, public and private. Public key is spread over the Internet and the private one is kept secretly. Whenever sender creates new message, he will sign it with *his private key* and encrypt it with *the public key of addressee*. When a new message arrives to addressee's mail systems, he decrypts a message with *his private key* (he is the only one, who can read the message) and check with *public key of sender*, that he is the real author of the message.

Even digital signatures and public key encryption is not enough. The problem is that addressee must be sure, that the purported key is really the sender's one. However he cannot prove it without a trusted third party (called Certification authority—CA). This person collects public keys on its key server (public Internet server where everybody can find a public key by its owner's e-mail address). However, CA includes public key to its server only when it proves, that the e-mail owner is the authentic owner of the public key.<sup>34</sup>

There are two main standards of public key encryption: PGP and S/MIME. PGP is older and wider used standard, but it is not enough well supported by the biggest software industry. S/MIME is a standard proposed by Netscape, Microsoft, Verisign and Lotus,<sup>35</sup> which lies basically on network of CA as described above. The biggest current CA is Verisign,<sup>36</sup> which supports S/MIME only.

Digital signatures also allow resolving of a problem of unauthorized agents, because

---

<sup>34</sup> See generally The Essential Role of Third Parties in Electronic Commerce, 75 Oregon Law Review 49 (1996) or <<http://www.law.miami.edu/~froom-kin/art.s/trusted1.html>>

<sup>35</sup> See generally <[http://www.rsa.com/rsa/developers/SMIMEPPT/smime\\_ie/index.htm](http://www.rsa.com/rsa/developers/SMIMEPPT/smime_ie/index.htm)>

<sup>36</sup> see <<http://www.verisign.com/>>

each company can have more digital signatures each one assigned to different tasks with different authorization assigned to it.<sup>37</sup> In such a way an agent can prove not only, that he is who he says he is, but that he has a certain level of authorization also.

Unfortunately the whole security area, especially in the international perspective is frozen by US government irrational policy on strong cryptography encryption.<sup>38</sup>

### **Nonrepudiation of message**

Requirement of nonrepudiation of message is concerned with holding the sender to his communication. Sender should not be able to deny that he already sent the message, or say that the content of the message was different.

Nonrepudiation of message is established in VAN-EDI by the sole fact that every sender of a message is connected to VAN by its own link (either by phone or special link), so he can be identified with his electronic address. Also every message is stored on the system of VAN-provider, so there is no question of integrity of messages.

Unfortunately, neither of the methods is useful over Internet. Internet is just interconnected system of different networks with different architectures and with different access policies. Because there is not one network, every message hops between different networks to find its way to addressee and it is possible for administrator of every one of these networks on the way to create fake message that cannot be distinguished from the original one.

To have a secure Internet nonrepudiation of message has to be established in quite a

---

<sup>37</sup> Online Law 92

<sup>38</sup> See more in A. Michael Froomkin, It Came From Planet Clipper: The Battle Over Cryptographic Key "Escrow", 1996 U. Chi. L. Forum 15; draft is at <[http://www.law.miami.edu/~froomkin/art.s/planet\\_clipper.htm](http://www.law.miami.edu/~froomkin/art.s/planet_clipper.htm)>.

different way. By using encryption software and trusted third parties,<sup>39</sup> it is possible to prove authenticity and integrity of messages. Also, messages (or their condensed form) could be stored by a trusted third party.

The other procedure is automatic acknowledgment of receipt. Whenever new message arrives addressee's computer system can automatically send back message confirming receipt of message and its readability (that is, message was not garbled and it was in a correct form). This does not mean acceptance of the offer in terms of a contract. However, such a message would be sufficient to give to both parties evidence about this communication, reliable enough to be used in a court, if necessary.

## **Legal issues**

### **About EDI Trading Partners Agreements**

Standard regulation of relationships created by EDI is in the EDI Trading Partner Agreements.<sup>40</sup> This method is sufficient in the current regime of EDI commerce. However, it certainly is not sufficient in proposed world of Electronic commerce.<sup>41</sup>

### **Evidence of contract**

Message must satisfy some legal requirements to be useful as evidence in court. These are: authenticity of author, integrity of message, nonrepudiation, and confidentiality. The last one is usually not necessary for enforceability of online contracts (contrary to some other areas of law, where message must be protected from any disclosure<sup>42</sup>), but it is highly desirable anyway.

---

<sup>39</sup> See *supra* note 34.

<sup>40</sup> See *supra* note 16.

<sup>41</sup> *supra* p. 9.

<sup>42</sup> See Online law, 31

The other requirements can be met by the system security (measures of protecting computer system from misuse), and moreover with the information security (protecting message when it leaves computer system of sender). An encryption with digital signatures, time stamping and trusted third parties may be helpful in securing information outside on Internet.

### **Mistake in transmission and liability third parties**

One danger that arises in using EDI over Internet instead of utilizing VANs is, that liability for correct transmission is unclear. There are usually many intermediary parties between sender's and addressee's computer. Who is responsible, when message comes garbled? It is not clear and usually all Internet Provides limits their liability for errors in transmission.

The best way, how to avoid problems with garbled messages, is probably to agree with all parties on the exchange of receipt acknowledgments as described on page 13. In such a case, messages would be binding only when sender is notified by acknowledgment receipt. This is roughly a rule proposed by UNCITRAL in its model law.<sup>43</sup>

### **Conclusion**

EDI is moving from the stage of proprietary game of big companies to a wide-spread tool for anybody, making the business to move even faster than it already does now.

There is a big need for some legal background for this shift. EDI Trading Partner Agreements are not useful for Electronic Commerce because they slow down Internet communication, where partners do not have any previous contacts with one another.

---

<sup>43</sup> See UNCITRAL Model Law on Electronic Commerce art. 14 at 36 I.L.M. 197 or <<http://www.un.or.at/uncitral/texts/electcom/ml-ec.htm>> [hereinafter UNCITRAL Model law]



Any legal tool underlying MIME-EDI transactions must be highly international in character as one of the results of MIME-EDI may be even bigger internationalization of commerce (communication will be probably much easier and international boundaries become less persuasive as a reason for not making a contract).

UNCITRAL Model Law on Electronic Commerce seems to be the best tool present for satisfying these issues without Trading Partner Agreements. However, it has some serious limitations also. It is oriented mainly on overcoming basic problems with electronic messages (for example, requirement of writing and signature or liability for garbled messages). Model law does not, however, rule in issues like late acceptance of message (remember, one of the most important usage of EDI is just-in-time delivery system), choice of law and choice of forum, other problems with digital signatures and unauthorized agents, etc.

When we concluded, that we have an international transaction issue (supposedly for sale of goods only, which creates another issue—what about sale of securities, for example), the first answer seems to be, why not to use CISG, which is created to deal with issues of international sale of goods. Unfortunately, a large number of issues are not covered by CISG. It is oriented on substance of contracts and does not care too much for their form. There is still something missing—some legal standard between UNCITRAL Model law, dealing with sole fact, that contract is not on the paper, and CISG, which does not recognize issues resulting from the form of contract at all.