EDI : Legal Issues in Japan

By Masami Muromachi

September 1994

Center for the Informatization of Industry (CII)

Japan Information Processing Development Center (JIPDEC)

Preamble

This booklet is intended to provide an introduction to the legal issues relating to Electronic Data Interchange (EDI) in Japan. As in many other countries, EDI is in its infancy in Japan but is developing very quickly. As a result, a body of legal principles is emerging to control the use of this important new medium and to protect the interests of those who use it. In some areas existing legal principles are proving adequate, while in others, such as in the field of authentication, Japanese law is only just beginning to deal with the main issues.

Central to the development of EDI in Japan is the international framework within which the law must develop. Data may be moved from country to country as easily as it may move within a single office. This suggests that a degree of international conformity is essential in the development of domestic law. This will be possible with a common understanding of the issues involved in EDI and cooperation at an international level.

In Japan, the Center for the Informatization of Industry (CII) has been appointed by the Ministry of International Trade and Industry to conduct research into the field of EDI. In 1989, CII established a committee for the consideration of EDI issues in Japan. The committee's members are academics, attorneys and business people, all of whom are active in the field of information technology.

The intention of this booklet is to introduce the main legal issues together with an explanation of the practical aspects of EDI in Japan. Part 1 deals with the basic concepts of EDI and the associated legal issues. Part 2 deals with data transmission and the formation of contracts. Part 3 discusses transaction security, as distinguished from system security (such as with the duplication of system data by a telecommunication line or a host computer). Part 4 deals with the use of EDI as evidence. Part 5

is the conclusion.

This booklet has been prepared by Masami Muromachi, of Miki, Yoshida & Muromachi, a Japanese attorney and member of the CII committee. The author wishes to thank CII for commissioning this booklet and their assistance in its writing.

The author has relied on numerous articles and sources of information published in Japan, the provenance of which has not been acknowledged in the text. The majority of these sources are only available in the Japanese language; a full bibliography is available from CII upon request.

Although this booklet has been prepared with the full cooperation of CII, the views set out herein represent those of the author and are not necessarily the views of CII.

Masami Muromachi
August, 1994

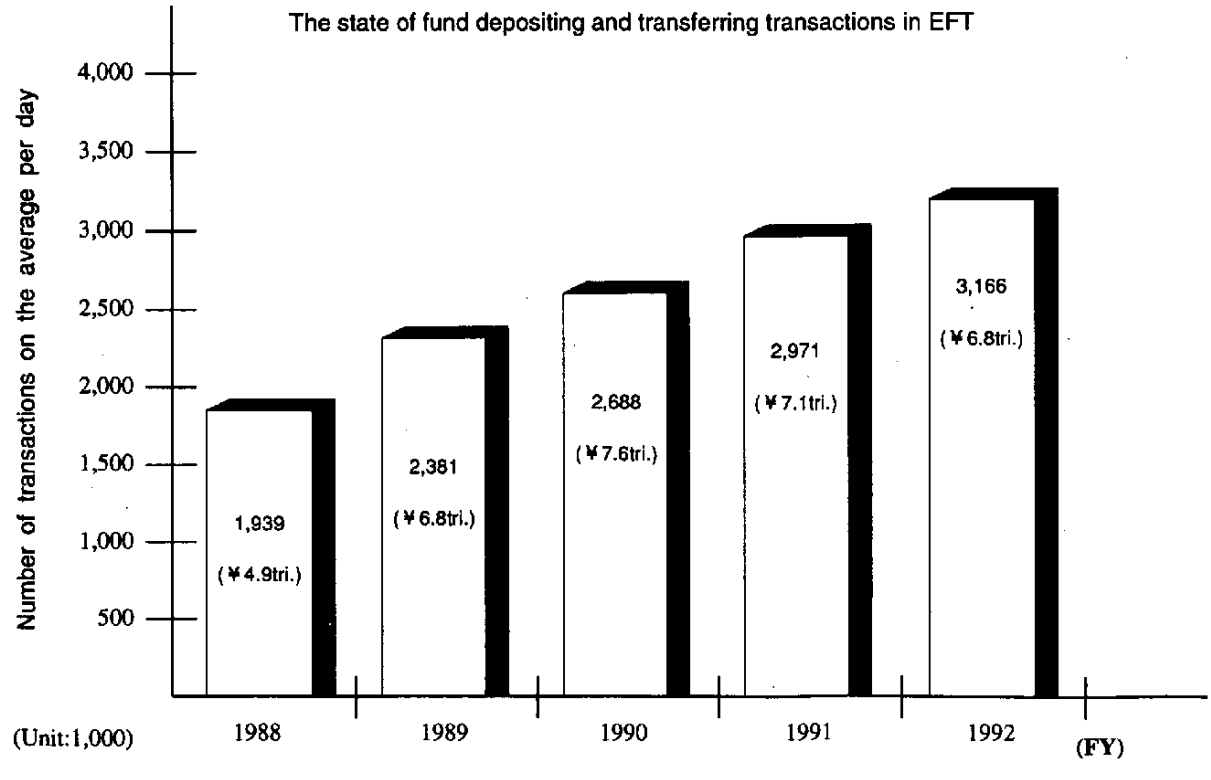
Table of Contents

1. Introduction

1.1 An Overview of EDI in Japan

In Japan as with many other countries, EDI is becoming an increasingly prevalent means of data interchange and is expected to become an integral part of Japanese commercial transactions in the very near future. Using electronic funds transfer as an example, according to the Financial Information System Center's White Paper of the Financial Information System published in 1994, in August 1993 the Bank of Japan Financial Network System (known as the Nichigin-Net System) carried an average of 30,100 transactions per day. The average total transaction value for this period was very large. The National Bankers Association acts as an inter-bank clearing house and uses an Electronic Fund Transfer (EFT) system called the "Zengin System". In the 1992 financial year this system carried transactions with a total value of 1,710 trillion yen ($17.1 trillion).

FET Surver (Source: The Federation of Bankers Association of Japan, 1993)



Another example of the increasing use of EDI is in the area of supermarket transactions. Many Japanese supermarkets have introduced "Empty Order Systems" and "Just in Time Systems". These systems store inventory information and allow automatic ordering of replacement products as sales are recorded at the point of sale. These systems have become increasingly popular in Japan and have accelerated the spread of electronic commerce into the manufacturing and wholesaling sectors.

1.2 Definitions of EDI

Throughout the world many definitions have been adopted for EDI. In Japan, CII has been studying the development of EDI since 1989. CII has adopted the following definition:

> "Exchange by different commercial entities of data that is necessary for commercial transactions between their computers (including terminals) via telecommunication lines according to a standardized protocol".

The United Nations Commission on International Trade Law (UNCITRAL) has prepared a draft set of uniform rules on the legal aspects of electronic data interchange and related means of data communication (UNCITRAL Draft). The UNCITRAL Draft adopts the same definition as the United Nations Rules for Electronic Data Interchange for Administration, Commerce and Transport. The UNCITRAL Draft definition of EDI states:

> "Electronic data interchange (EDI) means the computerized transmission of structured data between independent computer systems".

There are three main differences between the CII and UNCITRAL definitions of EDI. These may be summarized as follows:

(a) The Content of the Message Transmitted by EDI

Electronic communication technologies have made possible the

transmission of many kinds of data including data relating to everyday commercial transactions, medical data and administrative data. Recognising this, the UNCITRAL Draft definition includes all data transmissions. In contrast, the CII definition includes only data necessary for commercial transactions. However, different considerations apply to different types of data. For example, the transmission of medical data such as blood analysis requires not only a high degree of transaction security but also message integrity (in the sense of being completely accurate). Although this could be said to apply to other fields as well, there is clearly a need to impose strict controls over information that could potentially affect the lives of patients. Conversely, the transmission of commercial data which are transmitted in the form of a catalogue of advertisements will generally require a lower standard of message integrity. If it is assumed that the same security standard applies to both types of information, then it may be unlikely to produce a fair result.

It is clear from the above that different types of information have different requirements of message integrity and message security. As the range of information types has no effective limit, the only practical way to deal with disputes regarding the content of a transmission is to ensure that the parties to a transaction have a common understanding of the standards which are to apply if and when a dispute arises. This understanding needs to be completed at the time the contract is made. For the purposes of this booklet it has been assumed that the data referred to are of the type which are commonly encountered in everyday commercial transactions.

(b) The EDI Parties

If the range of EDI transactions is limited to commercial information, it is likely that the parties to the transaction will themselves be commercial entities. However, there are many cases in which parties to a transaction may be consumers or governments. In these cases, for example, it may be necessary to have additional forms of consumer protection for the benefit of

the everyday consumer or "home shopper". This appears to have been addressed in the UNCITRAL Draft whereas the CII definition expressly excludes consumer transactions.

Government EDI transactions in Japan are governed by Section 29-8 of the Accounting Code. This legislation requires that, in principle, the contract must be in written form, the parties' names must appear on the contract and it must be signed and sealed by the parties. This differs from the rules governing the formation of contracts between commercial (i.e non-government) entities. It is thought that the purpose of this provision is to establish and maintain financial and administrative certainty in government.

The CII definition is stated to apply to "different commercial entities" and may have been intended to exclude Government transactions. Although there has been little debate about this issue in Japan, a question arises as to whether the cause of financial and administrative certainty is promoted by EDI.

(c) The Requirement of a Standardized Protocol

The CII definition may have been intended to introduce a standardized protocol. However, because of the degree of interoperability between different computer systems a standardized protocol is likely to be of little use. As interoperability is further developed, the standardized protocol requirement may be replaced by the "structured" requirement in the UNCITRAL Draft definition.

1.3 The Model EDI Agreement in Japan.

In recognition of the growing importance of EDI in Japan, a number of model EDI agreements have been formulated. These include:

(a) The Basic Agreement for On-line Transactions

Using Standard Systems published by the Electronic Industries Association of Japan ("EIAJ") for the use of EIAJ members trading in electronic components. This agreement was drafted in 1990 and revised in 1992.

(b) The Memorandum for Data Exchange Agreement Between Business Enterprises published by the Japan Petrochemical Industries Association for use by petrochemical companies in transactions involving chemical products. This memorandum was drafted in 1993.

(c) The Standard Agreement for EDI Using CI-Net, published by the Construction Industry Information Center in 1993.

(d) The Agreement for Standard On-line System Transactions Using HII-Net (Housing Industry Information System Network) published by the Housing Information Services in 1992.

These model agreements contain both procedural standards and clarification of the application of legal principles. For example, in the EIAJ's model agreement, provisions relating to the following are included:

- Presumptions as to the receipt of data
- The manner of the formation of each contract
- Modification of each contract
- Prohibitions on the alteration of data stored in the mail boxes of parties to EDI agreements

Each of the model EDI agreements referred to have been drafted for particular industry or business sectors and may not be appropriate codes for use in general EDI transactions relating to product purchase, EFT or other areas.

For this reason, in the event of a combined EDI system being introduced, a new model agreement will be required.

2. Types of Data Transmission Systems and the Formation of a Contract

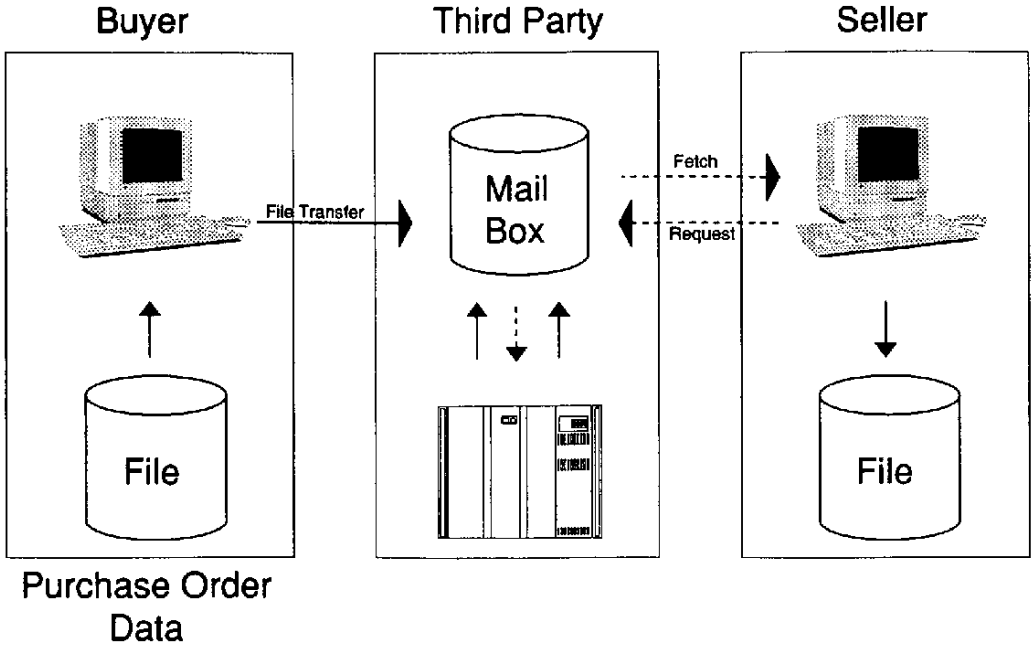
2.1 Types of Data Transmission Systems

(a) One Way Data Transmission Systems

A one way data transmission system is an EDI system used in commerce which does not require response or acceptance data from the receiving party. An example of this is a supermarket which deals directly with a wholesaler in circumstances in which the supermarket agrees to the bound by its orders without receipt of confirmation from the wholesaler. This type of arrangement is not uncommon where parties have a continuing business relationship which usually involves the regular ordering of quantities of goods.Where this type of ordering involves daily or weekly supplies, it is clear that the buyer intends to be bound by the orders. In the event of an ordering error a supermarket is often able to compensate for shortfalls or over ordering in the following period. As this example illustrates, there are many circumstances in which a one way data transmission system is preferable to the parties while being cost and time effective.

The use of one way data transmission systems in Japan can be shown as follows:

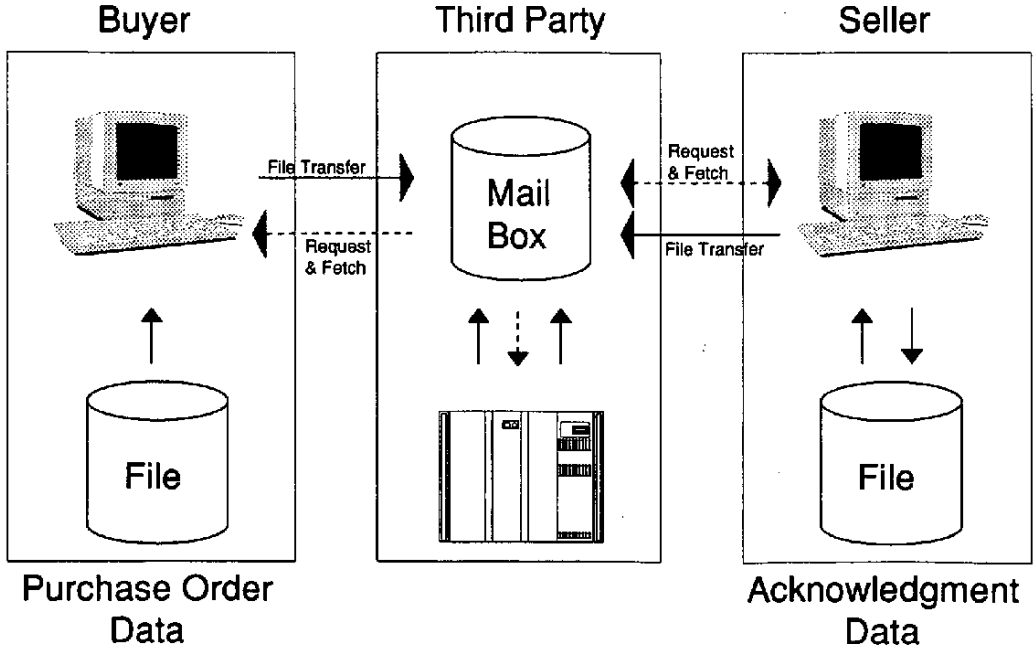
Pattern - 1 One Way Data Transmission Systems



(b) Two Way Data Transmission Systems

A two way data transmission system is a system in which a contract is concluded by the offering data being received and acceptance data being returned.

Pattern - 2 Two Way Data Transmission Systems



2.2 Legal Issues in the Formation of an EDI Contract

(a) General Issues

In the field of electronic commerce, substantial volumes of data are exchanged by means of EDI. In interpreting the legal effect of these arrangements, Japanese contract law applies the principle of freedom of contract unless there is some specific restriction imposed by statute. For example, under the Accounting Code contracts are required to be in writing but they are not required to be in any prescribed form. This factor together with the non-litigious nature of Japanese society, has led to there being very little discussion on the formation of EDI contracts between commercial entities. However, under Japanese legal theory, freedom to contract includes freedom in the formation of the contract and on this basis, it seems clear that an EDI contract can be binding. This argument is particularly forceful where the parties have agreed in advance as to the method of formation of the contract. In these circumstances it is submitted that EDI contracts will be valid unless a statute provides otherwise.

(b) One Way Data Transmission Systems

The formation of a contract using a one way data transmission system is supported by Article 509 of the Japanese Commercial Code. This provides that:

> "In cases where a trader has received an offer to enter into a contract which falls within any of the branches of the business carried on by him from a person with whom he is in regular business contact, he shall without delay, dispatch notice of acceptance or rejection. If he has neglected to dispatch such notice, he shall be deemed to have accepted the offer."

This illustrates that even where there is no express

consent, it is still possible for a contract to be formed without the receipt of acceptance data. Clearly, the test of "regular business relations" is a subjective one and must be determined on the facts of each case. The prevailing view of Japanese lawyers is that Article 509 is applicable to one way EDI systems and that these systems can create binding legal obligations.

In any EDI system, there is always a possibility that the message may not be received, either as a result of data loss or delivery error. To overcome this problem, it is possible to introduce a form of acknowledgment of receipt, even when the one way data transmission system is adopted. In cases where the offeror has superior bargaining power, it is possible to contract with the offeree so as to transfer all delivery risk to the offeree. An example of a clause purporting to do this is as follows:

> "The offering data shall be sent to the designated mail box as mutually agreed. The parties agree that when the offering data is sent to such mail box, such data shall be deemed to be received by the seller."

As an additional means of protection, it is also advisable to incorporate a system whereby the offer data cannot be received and acknowledged more than once. This problem may be overcome by a stipulation that once data in a designated mail box have been read they must be deleted.

However, an additional problem posed by one way data transmission systems is security. In the absence of security means, it is possible that unauthorized access to the offeror's data may result in the data being deleted prior to the data being read or actioned by the offeree. In these circumstances, it is difficult to agree that the receiving party should be deemed to have received the offer in accordance with the draft clause suggested above. Although there is no judicial authority on this point, it is submitted that the clause would not be effective in creating a binding contract in Japan due to the failure to adopt

security means. This issue is discussed further in Part 3.

(c) Two Way Data Tranmission Sytems

With two way data transmission systems contract formation is based on the usual offer and acceptance principles applied to written or oral contracts. In relation to the conclusion of written contracts, Article 526 of the Japanese Civil Code provides as follows:

> "A contract inter absentes comes into existence at the time when the notice of acceptance is dispatched".

The effect of this is that in the absence of any special agreement to the contrary, an EDI contract comes into existence at the time at which the acceptance data is transmitted. In practice, written contracts in Japan usually provide for the contract to come into existence at the time at which notice of acceptance is received by the offering party. If a practice develops in which this provision is adopted in EDI agreements, two way data transmission contracts would be concluded upon receipt of the acceptance data by the offeror. The effect of this would be to exclude the application of Article 526 of the Japanese Civil Code.

2.3 Cancellation and Modification of Data

In using EDI systems, there are many occasions on which transmitted data (i.e. messages) will need to be cancelled or altered due to errors in the description of the data or in their processing. The following provisions of the Japanese Civil Code are relevant to this issue:

(a) Subsection 1 of Article 521 provides:

> "An offer specifying a period for acceptance cannot be revoked".

(b) Article 524 provides:

> "An offer which has been made inter absentes without limiting a time for acceptance cannot be revoked before the expiration of such time as reasonably necessary for the offeror to receive the notice of acceptance".

In the case of transactions between commercial parties, Article 508 of the Japanese Commercial Code provides:

> "When a receiver of an offer without limit on time for acceptance does not provide the notice of acceptance within reasonable time, the offer will be void from the failure of such notification".

It is submitted that these provisions will apply to EDI contracts in Japan. The effect of this is that any offer which provides for acceptance within a specified period, or any offer which is made without specifying a period for acceptance, cannot be cancelled or revoked unilaterally. However, in accordance with the principle of freedom of contract, it is possible for the parties to an EDI contract to agree to permit revocation of the contract prior to acceptance.

In relation to the alteration of data, Article 528 of the Japanese Civil Code provides:

> "If the acceptor has delivered the acceptance notice which adds a condition to or modifies the offer, he shall be deemed to have rejected the original offer and to have made a new offer himself".

This issue frequently arises in the context of EDI contracts. Again, in accordance with Japanese legal principles, it is possible for the parties to agree in advance as to the modification or alteration of offering data at the time of

acceptance. Although there are inherent dangers in adopting this practice, there are circumstances in which the offeror of a volume of goods may agree to the offeree accepting a lesser quantity of such goods.

Other than as described above, there are few specific provisions of Japanese law which deal with the issue of cancellation or alteration of an offer or an acceptance in the course of making a contract. Generally in Japan these issues are resolved pursuant to an agreement between the parties or business customs. In the EDI context, these issues are dealt with in the various industry agreements discussed above. Again, pursuant to the principles of freedom of contract, mutual agreements relating to the cancellation and alteration of message data are deemed to be valid. The only caveat to be added to this is that in circumstances in which a consent to alteration of data is deemed to be unfair, such consent could be void under the Japanese Anti-Monopoly Code or related legislation. For the moment, however, there are no precedents as to the application of the anti-monopoly legislation to EDI agreements.

3. Transaction Security

3.1 Risks Relating to EDI

There are a variety of risks with EDI that do not necessarily arise in commercial transactions where agreements are recorded in paper documents. These include (i) risks imposed by computer system failures and the interruption of communications, (ii) risks involved in network systemization such as where the insolvency of a member bank involved in a financial settlement system causes a chain reaction effect on other member banks (these risks are sometimes referred to as "system risk"), and (iii) risks involved in computerization, such as unauthorized data origination and unauthorized data transmission. These risks may influence the stability and certainty of commercial transactions.

In order to minimize these risks, it is necessary to understand the underlying legal issues which apply to each area. Although research into these issues is ongoing, it must be acknowledged that in Japan much more study will be necessary in order to make EDI transactions as secure and reliable as paper documented transactions.

In Japan, the Ministry of International Trade and Industry (MITI) and the Ministry of Posts and Telecommunications have established security standards to minimize the risks identified above. With respect to computer system failure, the security standards deal with the duplication of communication circuits, the installation of independent electric power plants as back up facilities for power failures and general counter measures for natural disasters such as earthquakes.

Although there have been no post-war bankruptcies of major financial institutions in Japan, the Japan Bankers Association has adopted measures to deal with problems arising from network systemization. These have been applied to the Clearing House System which is the banks' management system for dealing with the remittance of same day settlements.

In relation to computerization risks, problems of unauthorized data origination and data transmission create a considerable threat to the stability and certainty of EDI transactions. This has produced a field of research which focuses on "transaction security".

3.2 Functions of Transaction Security

There seems to be no international consensus as to whether EDI rules should be applied exclusively to the transmission of commercial data or whether they should also be applied to other forms of data transmission such as administrative data (for example, in the delivery of tax demands). As the overwhelming majority of EDI transactions are commercial in nature, this

section analyzes transaction security issues related to these transmissions.

(a) Unauthorized and fraudulent origination and transmission.

In EDI systems, information from both the offeror and offeree is processed in binary form. At some point during this processing, the identity of the originator of the information needs to be verified. The most popular means of achieving this verification is through the use of passwords and secret codes.

The most important legal issue is in determining what happens when a third party uses a password without the authorization of the owner, originates commercial data in the name of the owner and transmits it another party. Where the unauthorized use is by a representative of the owner, the answer to this question lies in the application of Article 110 of the Japanese Civil Code. This provides that:

> "If, where a representative has done an act in excess of his authority, the third person had just reason to believe that the representative had just authority to do such act, the provisions of the preceding Article [109] shall apply mutatis mutandis."

The effect of Article 109 is to make the person which appointed the representative responsible for the representative's acts.

Where the unauthorized use is by a person completely unrelated to the owner, the owner will not be responsible.

However, in the EDI field it is often difficult to prove the identity of the originator of the message. In addition, in systems requiring the verification of a password, it is questionable whether the good faith and absence of negligence requirements (implied by Japanese case law) are applicable.

Perhaps the most reliable means of providing transaction security is through the use of encrypted messages which are then translated or decrypted by the receiver. Encryption enhances transaction security and so increases the reliance which may be placed on an EDI transaction should a dispute arise.

(b) The Legal Effect of Entry Error

If, for example, a purchaser of product A makes an ordering error and in fact requests product B, a seller who received the order for product B would, in a one way data transmission system, proceed to deliver product B to the purchaser. Upon receipt of product B, the purchaser may claim that there has been a mistake and could seek to return the goods. In this case, Article 95 of Japanese Civil Code provides that:

> "A declaration of intention shall be null and void if made under a mistake in regard to any essential elements of the legal act; however, if there has been gross negligence on the part of the declarant, its nullity cannot be asserted by the declarant himself."

However, it is not always clear what "gross negligence" or the requirement of good faith (as implied by Japanese case law) in an EDI context actually means, and how a standard for measuring degrees of negligence can be clearly defined.

To avoid these problems when entering data in Japan, the following procedures may be adopted:

(a) The purchaser should enter both the product code expressed in numerals and the product name expressed in kana (a Japanese alphabetical script) with each order, and

(b) Data should only be regarded as valid "ordering data" for a product when both the product code

and product name relate to the same product.

In circumstances in which this procedure has been agreed in advance by the purchaser and seller, a seller of goods in receipt of the data may then action the order with the confidence that it is correct. This is another instance of transaction security.

On the basis of the above, it can be seen that transaction security may be implemented by the parties to EDI transactions agreeing to a series of procedures which must be followed for each transaction. These procedures may be arrived at through a course of dealing between the parties although written agreements are preferable. This gives the parties to the transaction added confidence as to the correctness of data received and encourages greater use of the EDI system.

3.3 Phases of Transaction Security

The various aspects of transaction security that require further study in Japan may be identified at each phase of the EDI process. These may be summarized as follows:

(a) The phase of data origination. In this phase, it is necessary to determine that the data has been originated by an authorized person and that the contents of the message are correct. Confirmation of these two factors is essential to transaction security.

(b) The phase of data transmission. Any data originated through EDI must be received by electrical transmission by a person specified as the addressee in a way that ensures that the contents of the message are identical to the data originated and transmitted. Further, there is always a possibility that a message may be altered or distorted during the course of data transmission. Although these risks may be small, there are instances in which errors in processing or converting data can occur and erroneous data can be transmitted to a recipient. A related problem is the mis-delivery of data either

through errors in defining the recipient or through other transmission errors.

Each of these transaction security problems may be avoided or at least significantly reduced by means designed to confirm that the data have been transmitted without alteration and that they have been correctly addressed.

(c) The phase in which data are received. This phase is obviously related to but cannot be regarded as identical to the transfer phase. At this point, it is possible that other problems may occur such as where data are correctly transmitted to the addressee but are received and stored in a file within the addressee's system whereby they become unreadable due to some system error. If the data cannot be completely deciphered, the problem is defined as one of transaction security. This may be overcome by measures to confirm that the complete message has been received by the addressee.

3.4 Concepts Relating to Transaction Security.

In order to properly discuss and deal with the issues arising from transaction security it is necessary to have a clear understanding of the concepts involved. Three of those concepts are:

"Authentication": The act of verifying the claimed identity of an individual, station or originator.

"Identification": The process that enables recognition of a user described to an ADP [automatic data processing] system. This is generally by the use of unique machine-readable names.

"Non-repudiation of EDI notification": This provides the recipient of an EDIN [EDI notification] with proof of the origin of the EDIN which will protect against any attempt by the originator of the EDIN from falsely denying sending the EDIN.

These first two of these come from the Second Draft glossary of IT Security terminology drafted by the International Organization for Standardization and the International Electrotechnical Commission. The third comes from Recommendation F.435 of the International Telegraph and Telephone Consultative Committee.

In addition to technical means of transaction security, it is also possible to provide physical back up systems to acknowledge the receipt or dispatch of data. For example, by issuing a written notice of receipt by fax to acknowledge an order. This type of back up system is given additional weight where the parties to a transaction have agreed in advance that faxed confirmation letters shall be provided and that such shall constitute irrevocable evidence of receipt. In Japan, this type of device is not technically regarded as being part of transaction security as it is not dependent on the same electronic data network. It may also be viewed as defeating the real advantage of EDI, namely the facilitation of commercial transactions in a paperless environment.

As a variation on this idea, it is also possible to transact business pursuant to a contract that requires that when ordering data is received, an acknowledgment of receipt is provided which restates the original order. Again, this type of transaction does not require special computer or communication technologies as the confirmation may be sent by fax or by post as a precaution against data transmission failure. This method overcomes the unlikely scenario of only part of an order being received and being interpreted as being the whole order.

3.5. The Cash Card Case and Transaction Security.

There are few reported cases in Japan relating to transaction security issues, however, at least one important decision, known as the "Cash Card Case", does exist.

This case was decided by the Tokyo District Court and was

the first occasion on which the use of a password to verify the identity of a party was considered by a court in Japan. The decision of the court was affirmed by the Tokyo Appellate Court and the Supreme Court. However, the findings of fact and the reasoning of the higher courts differed in some respects from that of the Tokyo District Court.

The case involved the use of a cash card to make a withdrawal from an automatic teller machine by a person other than the person to whom the cash card had been issued. The person making the withdrawal used the four-digit numerical password registered when the card was issued. The person to whom the card had been issued sued the bank which had issued the card, alleging that the bank was liable to make good the loss suffered. Both at first instance and on appeal the bank was found by the court to have no liability. The reason for this finding was that the cash card system had a built in security system, namely the retention of the card by the person to whom it was issued and a password system of sufficient complexity to make its deciphering or the forgery of the card difficult without expert knowledge. In short, the security system established by the bank was sufficient in the circumstances.

This was a case involving a consumer and relating to a bank transaction, which would normally require a high degree of security. Therefore, it is unclear how far the reasoning can be applied to a case involving EDI in, for example, a merchandise trading transaction. What is clear is that in an open EDI system, in which it is likely that the parties to a transaction would never have met or dealt with each other before, the method of identification will be very important. It may be necessary to revisit the "commercial reasonableness" aspects of the Cash Card Case in the future in order to resolve this question.

3.6. Further Legal Issues in Transaction Security

Transaction security is vital to the maintenance, stability and certainty of commercial transactions using EDI. This need has

been widely recognized. In the United States, Article 4A of the Uniform Commercial Code introduced a system of EFT security procedures in 1989. Similarly, a system of authentication is included in the UNCITRAL Model Law on International Credit Transfers (1992).

Although transaction security has improved since the introduction of EDI, there are a number of key areas that will need to be studied in the future. These include the following:

(a) The appropriate level of transaction security.

In the financial settlement system, a high degree of transaction security is essential to avoid serious financial losses. In this system, sophisticated encryption methods are justified in view of the substantial risks. An example of this is the Nichigin-Net System operated by the Bank of Japan which has introduced Data Encryption Standards together with a high level of security measures. These include changing the key to the encryption system daily.

At the other end of the commercial scale, there are numerous uses of EDI which cannot justify the extra expense incurred in the maintenance of high levels of transaction security.

(b) Should standards of commercial reasonableness be introduced?

This issue is related to the necessity for transaction security discussed above. "Commercial reasonableness" is a requirement in contractual relationships under a number of codes, such as the UNCITRAL Model Law on International Credit Transfer (1992) and the Uniform Commercial Code (1989) of the United States. Under these codes, the transaction security measures that parties to a contract agree upon will not be enforceable unless they are "commercially reasonable". Although there are signs that a requirement of commercial reasonableness may one day become part of Japanese contract law (see, for example, the Cash

Card Case discussed above), such a development, if it happens at all, will take a long time. One reason for this is that, since different considerations apply to different types of data, it may be difficult to establish a test of commercial reasonableness which can be applied generally to EDI transactions.

For the future of EDI in Japan it will be important to determine the level of commercial reasonableness that should be implied into EDI agreements and the extent to which any of these protections may be varied by agreement.

If a standard of commercial reasonableness is to be adopted, it will need to be drafted so as to take account of the many types of EDI transactions, perhaps even taking account of technological developments which are yet to be introduced. Even at the consumer level in Japan, transaction security has produced greater efficiency. For example, the number of cash card forgeries has decreased in Japan since the introduction of personal identification systems (such as the Zero Password System and the Host Computer Check System) in which the password is not magnetically printed on the card.

4. The Use of EDI Data as Evidence

4.1 The use of electromagnetic data in civil suits.

(a) Admissibility. The Japanese Code of Civil Procedure does not provide any special limitations on the admissibility of evidence in civil suits except in special circumstances such as where evidence has been obtained illegally. To date, there has been no dispute as to the admissibility of electromagnetic data as evidence. There have been several cases in which such evidence has been used in civil suits in Japan.

(b) The Procedure Used to Examine Electromagnetic Data. The most topical issue regarding the use of electromagnetic data is in how the evidence is to be classified and examined. Although academic opinion is divided, the position may be

summarized as follows:

(i) The "documentary evidence theory" or "quasi documentary evidence theory". This is illustrated by machine readable forms of electromagnetic data. In this case, the data themselves may be regarded as documentary evidence or quasi documentary evidence and if so, the same procedure is adopted as with the examination of documents.

(ii) The "new documentary evidence theory". This theory supports the proposition that a hard copy representing a readable form of electromagnetic data is itself the original and that documentary evidence and the electromagnetic tapes or floppy disc storing records are the source of the hard copy.

(iii) The "verification theory". According to this theory, electromagnetic tapes and floppy discs should be subjected to verification before being accepted as documentary evidence because they cannot be read without mechanical assistance.

The Lower Courts in Japan have ruled that electromagnetic tapes are "quasi documents". An example of this ruling is a decision in the Osaka High Court on March 16, 1978 (Koto Saibansho Hanreishu Vol. 31, No. 1, page 38). However, it should be noted that the Japanese Code of Civil Procedure is currently under review and the issue of how to deal with electromagnetic data as evidence is being addressed as part of that review.

Other issues relating to electromagnetic data as evidence in civil procedure are:

(i) Whether electromagnetic data are admissible as evidence of the existence of a claim under the Japanese Bankruptcy Code.

(ii) Whether electromagnetic data are admissible as evidence of the existence of an equitable lien under the Japanese Civil Enforcement Code.

Although these issues are yet to be finally resolved, hard copies which represent machine-readable forms of electromagnetic data have been admitted as evidence in bankruptcy proceedings. However, there is no record of the same having occurred in relation to the execution of equitable liens.

(c) Resolving Conflicts in Electromagnetic Data.

Although this issue is yet to be tested in the Japanese courts, it is inevitable that conflicts of this kind will arise. For example, where a seller's data relating to a quantity of goods purported to be sold through an EDI transaction differs from the buyer's data relating to the same transaction. All that can be stated in relation to such conflicts of evidence is that Japanese civil law gives the court the power to evaluate the competing evidence and exercise its discretion in favor of the more credible argument. In resolving these issues in the future, it is likely that the courts will look very closely at the transaction security procedures adopted by the various parties and would be likely to resolve any conflict in favor of a party which is able to prove that it has the more effective procedures.

4.2 Agreement for Evidence

Under Japanese law, there is a concept of "agreement for evidence" in which certain things shall be used as evidence of certain agreed facts in advance of making the contract. An example of this in the EDI context is where the parties agree in advance that data held by the seller shall be proof of conclusion of the contract. However, for the moment, it is still not clear whether and to what degree such EDI contracts will be recognized by the courts. For example, it is not clear whether such contracts will be recognized unconditionally by the courts, or whether the courts will inquire as to the accuracy of the seller's data sought to be relied upon.

4.3 The use of Electromagnetic Data for Tax Purposes.

Japanese corporate tax law does not contain any explicit rule as to whether or not electromagnetic data are admissible in lieu of documentation (including contracts) for tax purposes. This is likely to become an important issue in the future.

For the moment, there is no definitive understanding as to whether or not a tax filing can be made using data created on an EDI system without first creating paper documents. In this respect, it may be relevant that the Corporate Tax Law does not explicitly mandate the creation of documents for any individual transaction, but only requires the retention of such documents as have been created. On this basis, it is arguable that there is no obligation to produce documentation of transactions executed through EDI. Although this argument is attractive, for the moment, there is no clear authority in Japan that suggests that EDI records will be accepted for tax purposes. Accordingly, there must be a risk in filing returns with the tax authorities based solely on electromagnetic data. Again, this is an area which is in need of review by the Japanese government.

4.4 Issues in Signing and Sealing Documents

When parties conclude a written agreement in Japan, the document is executed by affixing a seal. Both individuals and corporations have seals which are registered with the authorities. A personal seal is registered with a municipality, whether it be a city, town or village whereas with a corporation, the representative director can register his seal at the Bureau of Legal Affairs (Homukyoku). The Bureau of Legal Affairs deals with commercial and real estate registration. Both personal and commercial seals may be searched at the respective offices and a certification of the seal may be obtained. Although in some circumstances it may be possible to execute agreements through the use of a hand written signature, in Japan, it is still the custom to execute documents with a seal rather than a signature. Documents which bear a seal are given special status by Article 323 of the Japanese Code of Civil Procedure. This provides that:

"A private document shall be deemed to be authentic if it bears the signature or seal of the principal or his representative."

In this context, it would appear that the word "authentic" differs in meaning from that commonly understood in the EDI context. However, there is still a possibility that Article 323 may be interpreted as applying to EDI contracts.

For the moment, there has been little academic discussion on the point and no judicial precedent on the status of electronic seals, signatures or stamps. However, if the term "signature or seal" includes such an electronic identification system, it is possible that Article 323 will apply. It is also possible that an official certification system for electronic identification may be introduced. If so, this would greatly enhance transaction security and increase consumer confidence in EDI systems.

5. Conclusion

The Japanese legal system appears to have the flexibility to accept EDI transactions in the formation of contracts and in the use of the resulting electromagnetic evidence. However, much of the current law has been drafted to take account of documentary transactions and is now being applied to technologies that were not considered at the time when this legislation was drafted. As the technology becomes increasingly sophisticated, it is inevitable that Japanese law will need to evolve so as to deal expressly with the challenges provided by EDI transactions. Similarly, the global nature of EDI makes it inevitable that legal reforms in Japan will need to display a degree of consistency with international legal regulation so as to provide certainty in commerce. This will require recognition of different legal systems and business customs and the identification of common elements which can be imported into domestic law.

For the moment, Japanese law has been able to provide a sufficient framework to allow the evolution of EDI systems at least in their early years. In the future, it is likely that laws will be adopted to more specifically deal with the challenges provided by this new and exciting technology.

****

Published by:

Japan Information Processing Development Center / Center for the Informatization of Industry (JIPDEC/CII).
Kikai Shinko Kaikan
3-5-8, Shibakoen, Minato-ku, Tokyo 105, Japan
Tel: +81-3-3432-9386 Fax: +81-3-3432-9389