LAW IN DIGITAL AGE

(A Study of Compatibility of ***Electronic Commerce*** with Existing Legal Regime with Special Reference to Contract, Banking and Intellectual Property Law)

A Dissertation Submitted in Partial Fulfilment of Requirement for the Degree of

MASTER OF LAWS

Submitted by

ANIRBAN MAZUMDER

National Law School of India University
Bangalore

1999

Dedicated

to

My Parents

DECLARATION

I hereby declare that this dissertation entitled "LAW IN DIGITAL AGE" is the outcome of research conducted by me under guidance of Dr. N.L. Mitra, Director, National Law School of India University, Bangalore

I also declare that this work is original except for such help taken from such authorities as has been referred to at the appropriate places.

I further declare that this work has not been submitted in part or in whole for any degree at any other university.

Anirban Mazumder

Date: 9.7.99. ANIRBAN MAZUMDER

ACKNOWLEDGEMENTS

I am extremely grateful and highly indebted to my guide Prof. N.L. Mitra for his valuable guidance, suggestions and encouragement which has been instrumental in the completion of this research study. I acknowledge profound influence of him on my academic career. I express limitless thanks to him for his constant moral support.

I am grateful to Prof. A.K. Rai and Prof. S. Dasgupta, for their useful comments and suggestions.

My greatest debt is to my family members without whose support, I would not have completed my course.

I am thankful to Joy, Anonnya and Vijjy for their encouragement.

I specially acknowledge Reshmi for her continuing moral support.

I am thankful to Srinivas for giving expression to my ideas.

TABLE OF CONTENTS

LIST OF CASES

24. Marks and Spencers Plc and Others v. One in a Million Ltd., Court of Appeal, July 23, 1998.
25. Minnesota. v. Granite Gate Resorts, 568 N.W. 2d 715.
26. Minnesota. v. Granite Gate Resorts, 568 N.W. 2d 715.
27. MTV Networks v. Adam Curry (867 F. Supp. 202, SDNY 1994).
28. Prince Plc v. Prince Sportswear Group Inc. CH-1997-PNo.2355 (July 18, 1997).
29. R v. Wood, (1982) 76 Cr. App. Rep. 23.
30. R. v. Daye (1908) 77 LJKB 659 at 661.
31. R. v. Spiby, (1990) 91 Cr. App. Rep. 186.
32. Raghubir Singh v. Thakwain Sukhraj Kaur, AIR 1936 Oudh 96.
33. Ralli Bros v. Compania Naviera Sota Y Anzar (1920) 2 K.B. 287.
34. Re a Debtor (No.2021 of 1995) (1996) 2 All E.R. 345.
35. Re Charge Card Services Ltd. (1988) 3 All E.R. 702.
36. Re Oriel Ltd., (1985) 3 All E.R. 216.
37. Schelde Delta Shipping B.V. v. Astrate Shipping Ltd., (1995) 2 Lloyd's Rep. 249.
38. Shetland Times Ltd. v. Dr. Jonathan Wills & Shetland News Ltd. (Scottish Court of Session, 24 October, 1996).
39. South India Shipping Co. Ltd. v. Export-Import Bank of Korea, (1985). All E.R. 219.
40. Spiliada Maritime Co. v. Consulex Ltd. (1987) A C 460 at 476.
41. St. Alban's City and District Council v. International Computers Ltd. (1998) 4 All E.R. 81.
42. State Farm Mutual Auto. Ins. Co. v. Brockhurst 453 F 2d. 53 (10th Cir. 1972).
43. Thornton v. Shoe Lane Parking Ltd. (1971) 1 All E.R. 686.
44. Ticket Master v. Microsoft (1997) U.S. Case No.97.
45. Vita Food Products Inc. v. Unus Shipping Co. Ltd (1939) A.C. 277 at 290.
46. Whitworth Street Estates (Manchester) Ltd v. James Miller and Partner Ltd. (1970), A.C. 583.

LIST OF FIGURES

LIST OF ANNEXURES

GLOSSARY AND ABBREVIATIONS

API	Application Programming Interface
ASCII	American Standard Code for Information Interchange
AUP	Acceptable Use Policy
Backbone	A special type of internetwork intended speicifically to connect other internetworkers to the Internet
Bandwidth	The amount of data that can be carried by communications link in a given time
Bit	The smallest unit of binary information, represented as either "1" or "0"
Browser	Usually refers to a World Wide Web client program
Byte	A basic unit of data, consisting of 8 bits
CGI	Common Gateway Interface
CIX	Commercial Internet Exchange
Client	A computer or system that makes requests for some kind of network service from another computer or system acting as a sever
Cryptanalysis	The study of cryptographic processes with the intent of finding weaknesses sufficient to defeat those processes
Cryptography	The study of mathematical processes useful for keeping data secret by encryption, guaranteeing its provenance, or guaranteeing that its content has been unchanged
Datagram	The basic unit of network transmissions under TCP/IP
Decryption	The process of reversing encryption; application of a mathematical process to encrypted data to restore it to its cleartext version
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
Digital Signature	The result of the application of a cryptographic process to the digital document being signed

DNS	Domain Name System
E-mail	Electronic mail
EBCDIC	Extended Binary Coded Decimal Interchange Code
EDI	Electronic Data Interchange
EFT	Electronic funds transfer
Encryption	A reversible process of modifying cleartextk for the purpose of keeping it secret from anyone other than its intended recipient
Ethernet	A basebad networking medium, initially developed in the 1970s by Robert Metcalfe
FDDI	Fiber Distributed Data Interface
Firewall Gateway	A special construct for the prevention of attacks on an organizational internetwork originating from the global Internet
FTP	File Transfer Protocol
Gateway	A special-purpose computer for internetwork connectivity
Gigabit	1 billion bits
Gigabyte	1 billion bytes
Hacker	A term applied to individuals interested in computers and computing. This term is often used popularly to refer to individuals involved in criminal pursuits such as breaking into computers without proper authorization.
Home page	The opening document of a World Wide Web site
Host	Any device connected to a network that can send or receive requests for network services
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IAB	Internet Architecture Board

IANA	Internet Assigned Number Authority
ICMP	Internet Control Message Protocol
IESG	Internet Engineering Steering Group
Internet	The network of networks connecting tens of millions of users around the world
InterNIC	The Internet Network Information Center
Intranet	Small network among professionals who makes regular transactions
IP	Internet Protocol
IP Address	A numerical address assigned toa computer connected to an internetwork that uniquely identifies it on that internetwork.
IPX	Internetwork Packet eXchange
ISDN	Integrated Services Digital Network
ISOC	The Internet Society
Key	A quantity of data used in cryptographic procedures to encrypt, decrypt, or authenticate other data
LAN	Local Area Network
MAC	Message Authentication Code
MIME	Multipurpose Internet Mail Extensions
Network	Any system of interconnected systems
NFS	Network File System
NIC	Network Information Center
NNTP	Network News Transfer Protocol
NOC	Network Operations Center
NOS	Network Operating System
NSF	National Science Foundation
PCT	Private Communication Technology

PEM	Privacy Enhanced Mail
PPP	Point to Point Protocol
Private key	Of the two keys used for public key cryptography, the one that must be kept secret , so the owner of the key can decrypt messages encrypted with the public key
Protocol	A set of rules defining the behaviours of interacting systems, particularly when applied to rules for exchanging of information between networked systems
Public key	Of the two keys used for public key cryptography, the one that can be made public, so that senders can encrypt messages
Public Key Cryptography	The cryptographic system in which encryption is done with one key and decryption is done with another
Router	A multihomed host (connected to at least two networks) that is able to forward network traffic from one connected network to another
S-HTTP	Secure Hypertext Transfer Protocol
Server	Any computer connected to a network that offers services to other connected systems on the network
SLIP	Serial Line Internet Protocol
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSL	Secure Sockets Layer
STT	Secure Transaction Technology
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
URL	Uniform Resource Locator
WWW	World Wide Web

INTRODUCTION

A. Prologue

B. Statement of the Problem

C. Conceptual Framework

D. Objective and Significance of the Study

E. Methodology

F. Chapterization

INTRODUCTION

A. PROLOGUE

Around the world electronic commerce is the subject of intense interest in many sectors like government, business, service sectors, etc.. Electronic commerce has expanded from the closed world of business to business transactions between known parties to encompass a complex web of different activities involving large numbers of individuals, many of whom will never meet each other. It has implications on many facets of economic and social life and its development is ushering in a new era of global communication and trade. It has the potential to fundamentally change the way commercial transactions, the business of government, the delivery of services and a host of other interactions are conducted. It has brought revolution in policies directed at the regulation of traditional practices and procedures. Of greatest impact is the shrinking of the distance between producers and consumers, in an environment where geographical and political boundaries are no longer as significant as in the paper-based world.

While many of these changes provide a significant challenge to existing regulatory structures, and sometimes may be regarded as having a negative impact upon accepted rules and practices, electronic commerce will, at the same time, provide a host of opportunities. It will reduce the cost of transactions, reduce barriers to entry into business and in some cases remove the necessity for a physical presence in any particular market, as well as providing improved access to information to consumers.

Clearly the setting for electronic commerce is different to that which exists for paper exchanges. This raises a number of legal issues, and challenges, of both domestic and international significance.

Cyberspace radically undermines the relationship between legally significant (on-line) phenomena and physical location. The rise of the global computer network is destroying the link between geographical location and (1) the power of the local government to assert control over on-line behaviour; (2) the effects of on-line behaviour on individuals or things; (3) the legitimacy of the efforts of a local sovereign to enforce rules

applicable to global phenomena; and (4) the ability of physical location to give notice of which sets of rules apply.[1]

Recent advances in three areas - computer technology, telecommunication technology and information technology are changing lives in such a way which was beyond imagination before few decades. This technological revolution touches every area of activity where the digital transmission of information serves a purpose, whether it is in the office, in business or in world of shopping.

At the doorstep of new millennium, factors like global market, world-wide communication and removal of trade barriers are forcing business organisations to adopt new ways of doing business in order to successfully survive in the changing environment.

Electronic commerce is the future of business. This revolutionary new way of doing business will bring more customers and make the business process far more efficient and cost effective.

---

1 Johnson and Post, *Electronic Signatures and Records: Legal, Policy and Technical Considerations*, September 1, 1997, Information Security Committee of the American Bar Association, p.2.
URL: http://www.abanet.org/scitech/ec/isc/stateds.html

Electronic commerce can be described in simple words as doing business electronically. In more precise terms, it is the conduct of business and the execution of business transactions using a combination of structured and unstructured message exchange across the entire range of networking technologies.

A number of tensions have emerged from the electronic commerce regulation debate. Daniel Greenwood, Deputy General Counsel for the Commonwealth of Massachusetts, sums up these tensions in this way:

A number of voices have sounded the alarm to be aware of the "wild west" of cyberspace. Some advocate enactment of an array of protective comprehensive statutes, tailored to meet the special host of issues presented by the new information technologies. It is doubtful that any particular suite of laws would be sufficient, or desirable as a legal response to the information age. It may be more accurate to say that nearly all fields of law will undergo a transition that reflects and shapes the underlying movement toward electronically based information and communication. When our civilisation had transition to the industrial age, our legal system did not adapt by the mere addition of a new area of "industrial law". Rather, nearly every area of law was transformed by, and helped to create, the new economic, social and political realities

associated with the industrial revolution and our subsequent industrial civilisation. Similarly the pervasive information revolution will relegate many currently familiar concepts to irrelevant historical curiosities.[2]

B. STATEMENT OF THE PROBLEM

Globalisation is a term that fits perfectly in the information and communication service industry, an industry that has grown by leaps and bounds during the past two decades. There was only some 4.5 million Internet users in 1991 and estimates suggest that there will be as many as 300 million or more by the turn of the century.[3] The value of electronic commerce has raised from virtually zero and it is expected to reach US $300 billion in next two years time.[4]

Internet has created virtual global market by providing largest possible market without maintaining private net work for sale, delivery and customer service. But Internet is inherently insecured and unreliable

---

2 *Electronic Signatures and Records: Legal, Policy and Technical Considerations*, 1 September 1997, Appendix G to the Statement by the Legislative and Policy Work Group of the Information Security Committee of the American Bar Association, p42.
URL: http://www.abanet.org/scitech/ec/isc/stateds.html

3 *Electronic Commerce and the Role of WTO*, A Special Study conducted by World Trade Organisation, 1998.

4 *The Organisation for Economic Cooperation and Development*,
URL: http://www.oecd.org.

and so there is a need of safe, simple and secure mechanism for commercial transaction to make it more popular. Electronic merchant needs confidence that he can safely market and deliver his product and gets paid for all products purchased. Electronic consumer needs confidence that they can safely select and take delivery of product and pay for that without exposing the payment information to fraud. So this confidence building is to be facilitated for the success of electronic commerce. Apart from this, merchant and customer creates a level of trust before conducting transaction of sale. The trust is regarding the fact that customer is a potential purchaser and can select and buy goods which are offered and merchant is offering desired goods and can deliver it if it is required. This kind of trust is not inherent in the network and this level of trust is not in existence yet.

In conventional commercial transaction, the identity of customer is known to the merchant but in electronic commerce there is no mechanism to judge the identity of consumer which is very important in case of transaction regarding certain drugs, alcoholic beverages, firearms, entertainment products.

In case of on-line transaction, consumer does not know how long a website will exist in the Internet and whether it is a genuine or false

website. Creating a counterfeit website is much easier than creating a counterfeit retail outlet. This creates uncertainty in the mind of consumers.

These are all technical and business related problems which are required to be addressed but in the present research emphasis has been given on the legal issues which are likely to come up in case of electronic commerce.

The law of contract creates binding obligation between those willing to do business with each other. The Internet build for and used as a means of communication and provides a new arena for agreements. Initially World Wide Web was used for marketing and advertisement. Possibility of selling products and service was not ventured. Now with the advent of electronic commerce, it is understood that Internet can offer transnational and cost effective opportunity for selling goods and services to consumers. It can act as shop window, as cashier and can send digital product also. The legal issues which are to be addressed are what are requirements of binding contract in Internet, when contract is formed, who has jurisdiction, which law will be applicable, etc.

The activity of merchants and consumers in the Internet has close relation with the role played by banks. Electronic cheques, digital money can be deposited, balances can be checked and bills can be paid. Payment instruction is sent to the bank where a customer's account is held. Receiving it, bank sends a packet of digital cash which consumer used for buying any item and merchant collects it and deposits in his bank which in turn asks the bank of consumer to transfer the fund. When a financial institution working in Internet can be called a bank, what is the nature of digital cash, when a payment is said to be final, what is the evidentiary value of computerised data base, what are the effects of digitalisation of negotiable instrument etc., are some of the legal issues which are required to be addressed.

Internet has created tremendous threat for intellectual property protection. Keeping aside copyright violation in Internet, Cybersqatting is the major issue which needs to be addressed for growth of electric commerce. Practice of acquiring popular trade mark as domain name and using it for extracting money from trade mark holders appears to be a danger so far as electronic commerce is concerned. Again the issue whether transaction of software through Internet is sale of goods or service is not clear and needs immediate attention.

C. CONCEPTUAL FRAMEWORK

Electronic commerce - the outcome of advanced information technology has tremendous impact on existing legal system and the said situation can be extended to broader conceptual framework which provides for role of law in a society as well as interconnection between advancement of technology and progress of law. The basic purpose of law is to regulate human affairs with the ultimate objective of delivering justice. The existence of law presupposes an attempt to provide some sort of uniformity, certainty and consistency in the operation of social process. If technological advancement creates a situation where certain issues are not addressed by existing legal framework, then it gives an opportunity to the legal research to bridge the gap either by new legislation or by amendment of existing laws and thus to foster the progress of law, and if it is not done law will become slumbering sentinel.[5]

D. OBJECTIVE AND SIGNIFICANCE OF THE STUDY

Trade via Internet and other electronic networks is expected to reach $300 billion by 2000 and more than 300 million users will be

---

5 WEERAMANTRY C., SLUMBERING SENTINEL - LAW IN THE WAKE OF SCIENTIFIC AND TECHNOLOGICAL DEVELOPMENT, (Penguin Publication, London, 1983).

engaged in this transaction which is 60 times more than 5 million users in 1991. This very fact shows the rapid growth in popularity of electronic commerce and it is also true that electronic commerce is going to capture a substantial share of tomorrow's business. This expected growth of electronic commerce needs the support of a substantial legal regime, specifying the rights, duties and obligations of the players of the game like buyer, seller, service provider, bank etc., so that electronic commerce can flourish according to its potential. This study is to examine whether existing legal regime in India is sufficient enough to address various issues emerged due to electronic commerce and also if it is required, to suggest necessary legislation and amendments to make electronic commerce compatible with the existing legal regime.

E. METHODOLOGY

1. Hypothesis

Last few decades have witnessed a steady growth in scientific and technological development. Electronic commerce is the outcome of such development. These scientific and technological developments often give birth to certain issues which are not addressed by existing legal framework. In such a situation, laws are required to be remodelled so

that it can properly fit into newly created environment, and thus prevent law from becoming a slumbering sentinel. This idea perfectly suits in the circumstances prompted by electronic commerce in the present digital age.

2. Research Questions

1. What are the effects of electronic commerce on Indian Contract Act?
2. How Banking law is influenced by electronic commerce?
3. What is the implication of electronic commerce on Intellectual Property Laws?
4. What are the other laws which will have bearing upon electronic commerce?
5. How safe is electronic commerce?
6. How much control Government should have on the electronic commerce?
7. Why should people go for electronic commerce?

3. Operationalisation of Hypothesis

I. Contract

1. What are the requirements for a binding contract to be made over the Internet?

2. At what stage can it be said that a contract has been concluded over the Internet?
3. How can digital form of payment be used to bind agreement?
4. Which country's court will resolve the disputes arising out of n on-line contracts?
5. Which country's law will apply to an Internet contract?
6. What are the requirements for making a contract through Internet?

II. Banking

1. When do financial institutions operating over the Internet act as a bank?
2. What is the legal nature of digital cash?
3. When is a payment regarded as complete?
4. What are the ramifications of digitalisation of negotiable instruments?
5. What is the evidentiary value of computer based documents?

III. Intellectual Property

1. What is the implication of cybersquatting in the field of electronic commerce?
2. What changes do we need to stop cybersquatting?
3. What is the status of sale of software through Internet - sale of goods or supply of service?

4. Data Collection

To conduct this research secondary data, collected from various Study Reports as mentioned in the bibliography have been used to assess growth and impact of various Internet related activities. Primary sources like legislations of various countries on Electronic Commerce and Digital Signature as referred in the bibliography, UNCITRAL Model Law on Electronic Commerce, Information Technology Bill have been analysed to have understanding about the nature of law in digital age. Secondary data like books, articles and study reports, seminar papers as mentioned in bibliography have been used to do this research. Various Indian laws as mentioned in the bibliography have been examined to analyse how they are going to be affected by electronic commerce. Internet is the storehouse of information for such topic. Resources available from Internet, as referred in the bibliography have been used quite exhaustively. To get information regarding practical aspects of the subject, researcher has interviewed personnel of bank like ICICI who has pioneered on-line banking in India and software manufacturer who has provided electronic commerce solution for the first time in India like Satyam Infoway, IBM through unstructured questionnaire.

5. Mode of Citation

In the present work, citations have been used according to improvised version of Harvard Blue Book: A Uniform System of Citation.

F. CHAPTERIZATION

Present work starts with brief introduction of the subject and adopted methodology.

Chapter I - Conceptualisation	- This chapter contains discussion on concept of electronic commerce, instruments used for it and its working procedure
Chapter II - Electronic Data Interchange	- Concept of EDI as predecessor of net based electronic commerce and its merits and demerits have been discussed in this chapter.
Chapter III - Digital Cash	- This chapter contains discussion on the system of digital cash, its working procedure and its ramification on the

	society
Chapter IV - Encryption	- The necessity of encryption, different types of encryption and concept of digital signature have been highlighted here.
Chapter V - Legal Issues	- This chapter deals with discussion on implication of electronic commerce on Contract, Banking and Intellectual Property Law.
Chapter VI - Legislative Initiatives	- Initiatives taken by legislatures of various countries regarding electronic commerce have been analysed here.

Present work comes to an end with brief concluding remark containing suggested Policy, Principles, Recommendations and a note on tasks to be done in future.

CHAPTER I

ELECTRONIC COMMERCE: CONCEPTUALISATION

I.1. What is Electronic Commerce?

I.2. Instruments of Electronic Commerce

I.3. Why Electronic Commerce?

I.4. Scope of Electronic Commerce

I.5. Electronic Commerce in Practice

I.6. How Does the System Work?

CHAPTER I

ELECTRONIC COMMERCE: CONCEPTUALISATION

The rules of business are no longer governed by whims and fancies. Today, if one's claws are not sharp and eyes are not watchful, his or her company can take the quickest route to the endangered list. The only answer for staying away from the hungry jaws of change is to run faster than change itself. The change is also not unwarranted. It is an eternal process and in case of commercial transaction, the need for change is overdue for a considerable period.[6]

The growth of telecommunication and computing, known collective as "telematics"[7] has enabled business to establish new means of managing their business, internally and externally, nationally and

---

6 "This is already my ninth hour at work and I have not eaten or drunk, I have been seated all day without even going out and I won't get to eat until night but who will deliver me from this endless round of letters and invoices?" This quotation is not from someone in our recent past but from a Florentine Merchant in 1385 -
PETER GARDNER, ELECTRONIC TRADING - A PRACTICAL HANDBOOK 21 (Butterworth Heinemann, 1994).

7 "A French term coined to describe the combination of computers and telecommunication networks" -
DICTIONARY OF INFORMATION TECHNOLOGY (34th ed. 1989).

internationally.[8] Recent advances in computer[9] technology, telecommunication[10] technology and software[11] & information technology[12] have brought new means of exchanging information and transacting business. This technological revolution[13] has influenced

---

8 Access to telecommunication infrastructure in selected countries in 1996 (ANNEXURE-A).

9 A computer is a device that solves problem by applying prescribed operation on data entered into it. The computer can perform its data processing operations accurately at high speed without human intervention. There are two basic types of computers-analog and digital. The analog computer operates on data represented by variable physical quantities. By contrast, the digital computer works with numbers, words and symbols expressed as digits which it manipulates and counts discretely. A third general class of computers, the hybrid computer, combines the feature of the other two and utilises both analog and digital quality of data. The majority of computers in use today are of the digital variety. Extremely versatile, digital computers can carry out a multitude of varied tasks, from routine accounting and book keeping to the control of space craft and analysis of scientific data -
THE NEW ENCYCLOPAEDIA BRITANNICA 638 (Chicago University Press, 15th ed., 1991, Vol.16).

10 Telecommunication systems are devices and techniques used for the transmission of information over long distances via wire, radio or satellite. A wide variety of information is transferred by such systems, including sound, visual images, computer processed data, telegraph and teletypewriter signals -
THE NEW ENCYCLOPAEDIA BRITANNICA 464 (Chicago University Press, 15th ed., 1991, Vol.28).

11 Computer program is a detailed plan or procedure for solving a problem with a computer. More specifically, an unambiguous, ordered sequence of computational instruction is necessary to achieve such a solution. This program is also called software -
THE NEW ENCYCLOPAEDIA BRITANNICA 508 (Chicago University Press, 15th ed., 1991, Vol.3).

12 Information technology deals with communication, storage, processing, and use of information for a variety of valuable users. Information technology helps in optimizing the use of scarce capital, for example, by improving the utilization of aircraft, railway wagon, steel mills, by supporting intelligent decision making and coordination without wasteful delays. It promotes better utilization of scarce resources, such as electricity, water and raw materials. Information technology also makes it possible to improve quality of life by streamlining a whole variety of services such as travel reservation, hotel reservation, banking, commercial transaction, educational program -
P. SADANANDAN, R. CHANDRASEKAR, INFORMATION TECHNOLOGY FOR DEVELOPMENT vii (Tata McGraw-Hill Publishing Co. Ltd., New Delhi, 1987).

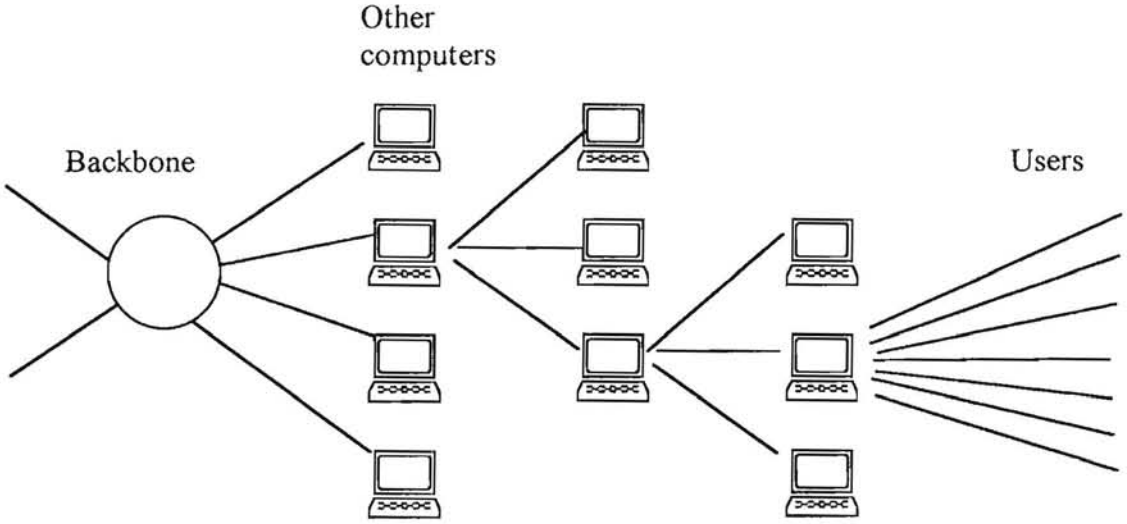
13 Technical innovations very likely between 1967-2000 (ANNEXURE B).

every area of activity where the digital[14] transmission of information serves a purpose whether it is in the office, in business or in world of shopping, leisure and entertainment. These modern technologies are being combined, specially through the Internet[15] to link millions of people

---

14 Telecommunication centres on the problems involved in transmitting large volumes of messages over long distances without damaging quality due to noise and interference. The basis of relatively noise free and interference free telecommunication is the so called binary signal. The binary signal consists of two stages, the dot-dash of Morse Code, an on-off signal in teletype, 0 or 1 in binary mathematics and a punch or no punch command of computer card. Practically all voice, picture, instrumentation and other data can be coded in binary form. Long distance telecommunication system capable of transmitting voice, teletypewriter, facsimile, data or television signal performs through digital transmission by using binary signal. If digital transmission is employed, signals are first processed in a code that completely transforms their character. The versatility of modern information system stems from their ability to represent information electronically on digital signals and to manipulate it at exceedingly high speed. Information is stored in binary devices which are basic component of digital technology. Information is represented in them either as absence or presence of energy or electric pulse - THE NEW ENCYCLOPAEDIA BRITANNICA 508 (Chicago University Press, 15th ed., 1991, Vol.3).

15 Internet is made up of hundreds of thousands of separate networks, each connected to some way to a back bone that moves data from one network to another.



The backbone is formed by the biggest networks in the systems, owned by major Internet Service Providers. Every back bone has at least one point where it

in every corner of the world. In the recent past, Internet has got a

---

exchanges data with another back bone. As a result of this, when a Local Area Network connects a back bone, people using it automatically gain access to the entire system. No one person, company, institution, government or organisation owns the Internet. The World Wide Web Consortium sets the standards for HTML and other specifics of the web. The Internet Engineering Task Force focuses on the evolution of the Internet with an eye on keeping the Internet running smoothly. The Internet Engineering Steering Group is an organisation responsible for managing IETF activities and the Internet standard process. The Internet Architecture Board is responsible for defining the over all architecture of the Internet and providing guidance and broad directions to the IETF. The protocol (set of rules that define procedure, convention and networks used to transmit data between two or more networked devices) presently used at the heart of Internet is TCP and IP (Transmission Control Protocol and Internet Protocol). It comprises of a coding system that enables different computers to electronically narrate data to each other over the network. Every computer that hooks on to the Internet, understand these two protocols and uses them to send and receive data from other computers on the network. A client-server network is a collection of computers (server) designated to store, process and distribute data, resources on the one hand and computers (clients) that access and use the data, resources managed by server on the other hand. Many commonly accepted methods exist for data exchange over the Internet, including electronic mail, news, file transfer, remote access to distant computers and the World Wide Web. The World Wide Web has become the ultimate information utility on the Internet responsible for carrying out most of the Net's applications. The types of fuctionalities and modes of delivery of information that have been promised for decades are now a reality. These include, among others, video conferencing, inexpensive global phone call, instant data access, live new feeds and real time interactivity. Applications that are rapid and reliable transmission of data over the Internet are now being used in the fields of business, education and entertainment. Another interesting and important factor that the medium possesses is "global reach". The Internet is essentially a community of people that has helped to establish the first truly global community spanning every continent, government, race, religion, sex and age. For a small tender, the Net can offer the best services by providing a direct client base and an international coverage at a nominal cost. Businessmen, traders and advertisers are not the only one who can take advantage of Internet. Institutions and public sector units can adopt it as a new mode of disseminating information, whereas for individuals, it can be a source to broaden this horizon. The pool of information available via Internet is freely accessible by its users. On-line, one can find vast chunk of information on almost every known subject, available 24 hours a day, seven days a week. Internet has already exhibited the potential of a future global village -

INFORMATION TECHNOLOGY, October 97, pp.50-58; Robert B. Palmer, Chief Executive Officer, Digital Equipment Corporation, Address at *Spring Internet World* (March 12, 1997); PETE LOSHIN, PAUL A. MURPHY, ELECTRONIC COMMERCE 15-23 (Jaico Publishing House, 2nd ed., 1998); Vic Sussman, Kenan Pollack, *Gold Rush in Cyberspace*, SPAN, April-May 1996, p.19; *Freedom or Censorship-II*, INFORMATION TECHNOLOGY, January 98, p.97; Sukesh A., *The Information Storehouse*, TECHNOWORLD, October 97, pp.43-47; *Freedom or Censorship-I*, INFORMATION TECHNOLOGY, November 97, pp.80-82; WTO Secretariat, *Special Studies 2, Electronic Commerce and the role of WTO*, 1998 at 10.

phenomenal growth (Fig. 1 & 2).[16]

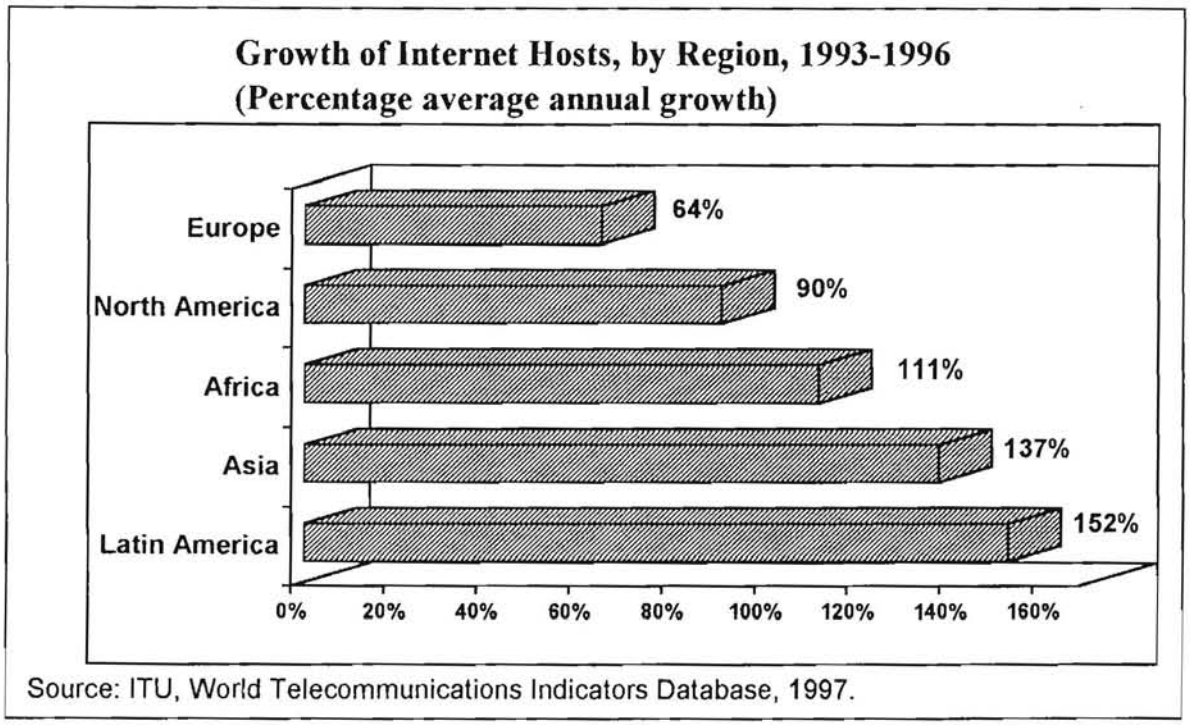


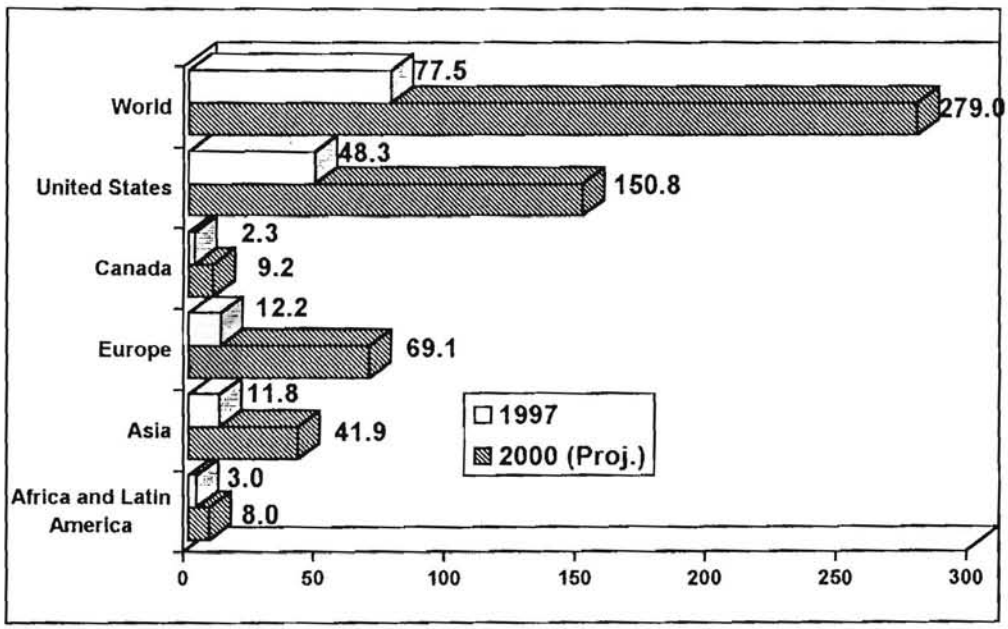
Fig-1

---

16 Internet use has tripled over the last two years, according to most Internet researchers. By the end of 1997, more than 1 out of every 4 Americans were using the Internet. Neilson's "Internet Demographies Survey" estimates that 58 million adults in North America were using the Internet at the end of 1997. Another Net census takers -IntelliQuest Information Group - estimates that 51 million adult American used the web in 1997, a 46% increase over the 35 million who used the web in 1996. World wide, an estimated 65 million people use the web, according to International Data Corporation. As many as 42 million of these are classified as regular or active Internet users, up from 8 million in 1995, according to Cyber Dialogue.
Web Commerce: A Tempting Target For Tax Collector?,
URL: http://www.house.gov/cox/Nettax/web-commerce.htm>

The previous graph illustrates that Africa, Asia and Latin America have reported the highest growth rates[17] and the graph below shows that all regions are expected to gain user market share by next year.

Internet User Population, by Region, 1997 and Projection for 2000 (Millions)



Source: ActivMedia, Incorporated, 1997; (http://www.activmedia.com).

Fig-2

17 *WTO Secretariat, Special Studies 2, Electronic Commerce and the role of WTO,* 1998 at 26.

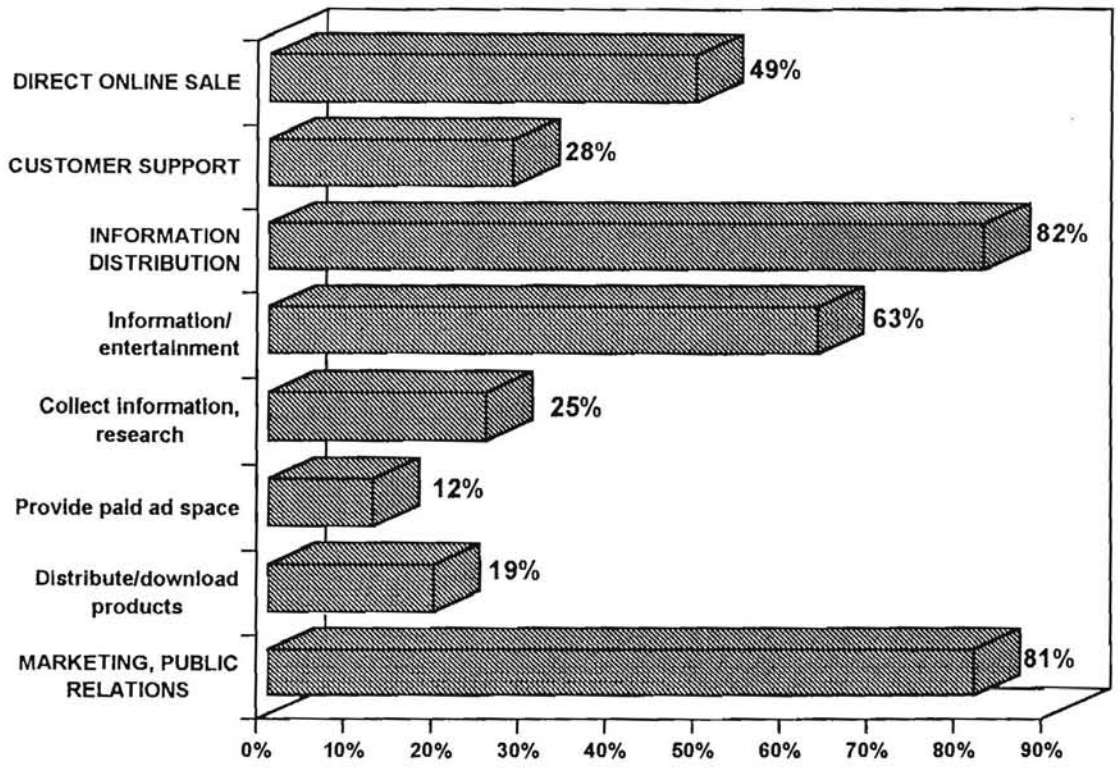
The Internet has been tremendously successful and it has a significant impact on our lives in almost every possible area.[18] The growing pervasiveness of the web has made business organisations sit up and take note of the tremendous potential of this medium (Fig.3).[19]

---

18 Using Internet, one can get (a) information about best schools, teachers and courses available to students without regard to geography, distance, resources or disability; (b) information about resources of art, literature and science; (c) on line health care service; (d) facility of using office in different places, residing in other place with the help of electronic highway; (e) orders from all over the world electronically, even though he or she is small manufacturer; (f) opportunity to see latest movies, plays, video games, to listen latest music, to have new software, to get air ticket through digital transmission; (g) opportunity to use bank, to do shopping sitting in home; (h) opportunity to obtain information from government or exchange information among government organs and business organisations -
Lawrence H. Summer, Deputy Secretary, Department of Treasury, United States (05/27/97 08:00:47) URL: <http://www.treas.gov/treasury/press/pr 052297 a.html); WTO Secretariat, *Special Studies 2, Electronic Commerce and the role of WTO*, 1998 at 15-21.

19 Mr. Peterson has predicted following changes due to this medium -
(a) Improved market information for sellers, (b) Improved market information for buyers, (c) Increased interactivity between buyer and seller, (d) Enhanced interconnectivity between buyer and seller, (e) Emergence of new market intermediaries, (f) More technology based channels of physical distribution, (g) Additional technology based consumer service, (h) More worldwide sourcing, (i) Increased emphasis on building customer loyalty, (j) Safeguards designed to provide information security and confidentiality. -
ROBERT A. PETERSON, ELECTRONIC MARKETING AND THE CONSUMER, 164-171 (Sage Publication, 1997).

Purpose for Maintaining a Website, 1993-1996
*(in per cent of all websites)**



Source: ActivMedia, Incoporated, 1997 (http://www.activmedia.com).
* Based on survey reports.

Fig-3

One of the revolutionary uses of the Internet is in the world of commerce.[20] Already, books and clothings can be bought, business

20 The number of people using the Internet for commercial purposes is growing faster than the number of new people getting on-line. 27% of regular Internet users brought products on-line this year, compared to 19% two years ago,

advices can be obtained, everything can be purchased from garden tool to high-tech communication equipment over Internet. But it is just the beginning. Days are not far away when almost all activities can be done through Internet (Fig.4).

Application of Internet

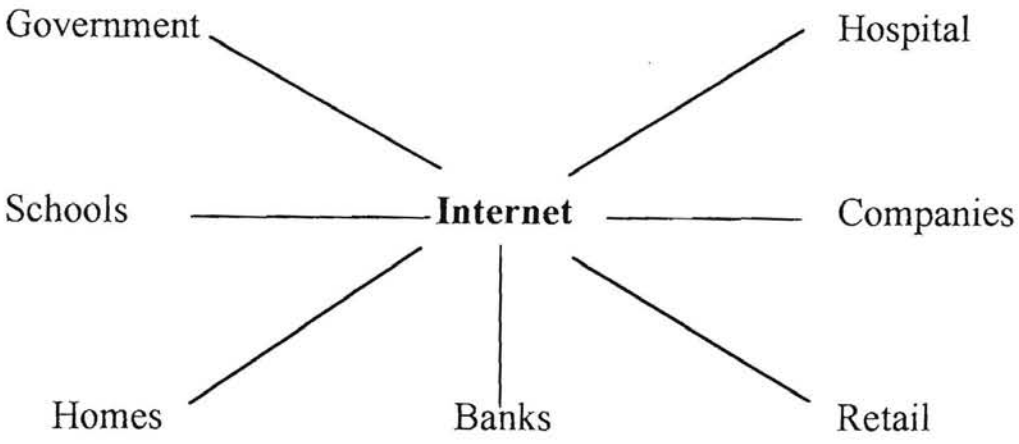


Fig-4

---

according to Media Dialogue, which projects that 39% of regular web users will be buying on-line by 2001. In all, 10 million Americans have made a purchase on-line, according to Neilseon - Commerce Net figures. More and more businesses are eyeing the Internet's growing market of consumers. According to one study, fully 25% of all small businesses have established an Internet presence. 40% of all U.S. companies are expected to be selling products on-line by the end of the century, according to IBM. On-line retail sales grew up by 150% in 1997. The sale of retail goods over the Net generated $2.6 billion in total receipt in 1997 - up from $1.1 billion in 1996 and $500 million in 1995, according to Forrester Research. Among the fastest growing areas of commercial development in 1997, travel, tourism, computer hardware, consumer electronics, gifts and books. On-line advertising revenue surged to $700 million in 1997, more than double of the $300 million spend in 1996, according to Media Control. Business to business commerce accounts for a significant amount of Internet related commerce. In 1997, businesses exchanged $8 billion worth of goods and services over the Internet, according to Forrester Research. Manufacturers, chiefly in electronics and airplane parts, totalled $3 billion, services and utilities totalled $3 billion and middlemen, computer related and office supplies totalled $2 billion.
Web Commerce: A Tempting Target For Tax Collector?,
URL: <http://www.house.gov/cox/Nettax/web commerce, htm>.

Trade on the Internet is doubling or tripling every single year. In just a few years, it will generate hundreds of millions of dollars in goods and services[21] as shown in Fig-5.

Internet is an extremely versatile means of commerce. In respect of some products, all elements of the production, distribution chain can be completed on line and across border. For example, after reading an advertisement in Internet, a customer in Switzerland can send a data request to the American owner of a data bank stored in Canada. The computer of American owner forwards the data request to the data bank for automatic retrieval. The retrieved data is then sent from Canada to

---

21 Total web related revenues are projected to reach $1 trillion by 2000, according to Active Media. Others, including the accounting firm of Arthur Anderson, have put this figure as high as $150-600 billion. In 1996, the U.S. Treasury Department projected more conservative on-line revenues of $70 billion by 2000. On line retail sales are expected to double almost every year. Forrester Research provides that on-line sales has grown from $2.6 billion in 1997 to $4.8 billion in 1998, $8 billion in 1999 (projected), $12 billion 2000 (projected), $18 billion in 2001 (projected). By 2001, on-line purchases of computer hardware could account for 10% of total hardware sales. On-line ticketing could reach $10 billion in 2001, with $8 billion through airline ticket sales and $2 billion through on-line sports or entertainment ticket sales. Internet access service are expected to generate $50 billion in annual revenues by 2000, up from $8.4 billion in revenues in 1997, according to Maloff Group International. At the end of 1997, Internet access revenues were growing by 25% a month, compared to 3.8% in March 1996. On-line advertising revenue is expected to double in each year of the next few years, growing to $2-5 billion in 2002, according to Cowles-Simba Information. On-line revenue was $700 million in 1997 and $980 million in 1998. Business to business commerce is expected to grow to $327 billion by 2000, up from $8 billion in 1997, according to Forrester Research.
Web Commerce: A Tempting Target For Tax Collector,
URL: <http://www.house.gov/cox/Nettax/web commerce, htm>.

America. The computer in America requests, receives and varieties the credit card payment or possibly the electronic money transfer from the Swiss client and sends the requested data to Switzerland.

Internet-Generated Revenues in the United States, by Sector, 1996 and projection for 2000

	1996		2000 (Proj.)	
	million $	percentage	million $	percentage
Internet access related equipment and services	4,010	27.0	29,510	15.0
Hardware	2,840		19,820	
Software	270		5,540	
Service	900		4,150	
Internet access	4,230	20.5	33,130	17.0
Consumer	3,460		17,350	
Business	770		15,780	
Business-to-business commerce	600	4.0	66,470	34.0
Consumer retail	530	3.6	7,170	3.5
Financial services	240	1.6	22,580	11.5
On-line securities/mutual fund fees	220		3,090	
On-line insurance purchases	0		18,630	
On-line consumer banking fees	20		860	
Content (various services)	5,240	35.3	37,280	19.0
Consumer	80		4,800	
Business	5,160		32,480	
Total U.S. Internet economy	14,850	100	196,140	100

Source: Forrester Research Inc., 1997.

Fig-5

In other words, advertising, production, purchase, payment, delivery of the service can be conducted electronically through just one instrument, that is Internet. This shows the enormous potential of the Internet for electronic commerce.[22]

I.1. WHAT IS ELECTRONIC COMMERCE?

Definition[23] of electronic commerce vary considerably but, generally, electronic commerce refers to all forms of commercial

---

22 Supra note 17 at 11.

23
- Electronic commerce defined simply is the commercial transaction of services in an electronic format.
  (Transatlantic Business Dialogue Electronic Commerce White Paper 1997).
- Electronic commerce refers generally to all forms of transactions relating to commercial activities, including both organisations and individuals, that are based upon the processing and transmission of digitized data, including text, sound and visual images.
  (OECD, 1997).
- Electronic commerce is about doing business electronically. It is based on electronic processing and transmission of data, including text, sound and video. It encompasses many diverse activities including electronic trading of goods and services, on line delivery of digital content, electronic fund transfer, electronic share trading, electronic bill of lading, commercial auction, collaborative design and engineering, on-line sourcing, public procurement, direct consumer marketing and after-sale service. It involves both products (consumer goods, specialised medical equipments) and services (information services, financial and legal services), traditional activities (health care, education) and new activities (virtual malls).
  (European Commission 1997).
- Electronic commerce is the carrying out of business activities that lead to an exchange of value across telecommunications networks.
  (European Information Technology Observatory, 1997).
- Electronic commerce that has been limited to a number of specified companies, is entering a new era when many unspecified persons

transactions involving organisations and individuals that are based upon the processing and transmission of digitized data. The term "electronic commerce" is poorly understood and frequently used to denote different meanings, very often depending on the individual's job function, professional orientation, background, local product or services and type of information technology deployed.[24] Electronic commerce denotes the seamless application of information and communication technology from its point of origin to its end point along the entire value chain of business processes conducted electronically and designed to enable the accomplishment of a business goal.[25] The goal of electronic commerce is the creation of a new kind of commercial environment in an electronic milieu, in which many of the separate steps that normally intervene between a buyer and a seller in a commercial transaction can be integrated and automated electronically, thus minimizing transaction costs.[26]

---

including general consumers are involved on the networks. In addition, its contents have come to not only simple transactions of data concerning placing orders or order acceptance but also to general commercial acts such as publicity, advertisements, negotiations, contracts and fund settlements. (Ministry of International law Trade and Industry, Japan, 1996). BUSINESS AMERICA at 44 (January 1998).

24 Rolf T. Wigand, *Electronic Commerce: Definition, Theory and Context*, THE INFORMATION SOCIETY at 5, Vol.13, No.1, Jan-Mar. 1997.

25 Id.

26 BUSINESS AMERICA 44 (January 1998).

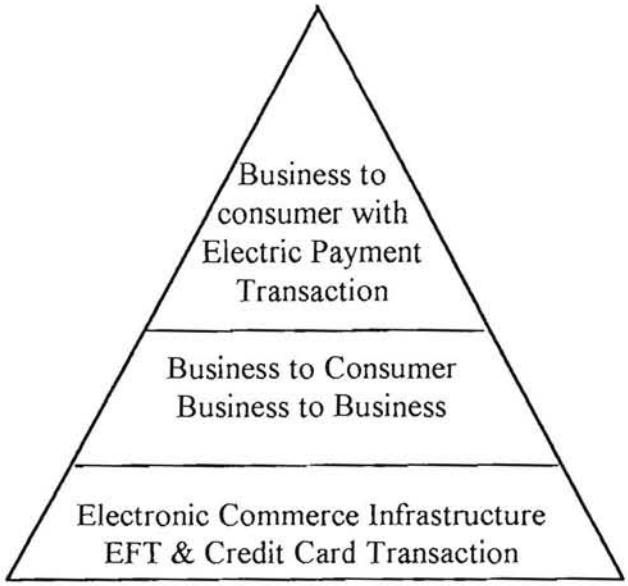


Fig-6

In classifying electronic commerce, broadest definition includes electronic fund transfer[27] and credit card[28] transaction along with

---

27 Electronic Fund Transfer is a mechanism to do paper based transfers with the help of electronic transmission. United States Code, Commerce and Trade, Sec.1693(6) defines electronic fund transfer as any transfer of fund, other than a transaction originated by check, draft or similar paper instrument which is initiated through an electronic terminal, telephonic instrument or computer or magnetic tape so as to order, instruct or authorise a financial institution to debit and credit an account. It includes but is not limited to point of sale transfer, automated teller machine transaction, direct deposit or withdrawal of fund and transfer initiated by phone. UNCITRAL Report of the Secretary General on Electronic Fund Transfer, Para 4-7, describes that the distinguishing element in electronic fund transfer is that the payment instruction transmitted to or between the banks is made in an electronic form rather than by physical transmission of a paper based payment instruction. This substitution of electronic impulses for paper is made in order to achieve an increase in speed of transmission of the payment instruction and to facilitate the handling of the volume of such messages, thereby reducing the cost.

28 Credit card is a plastic card with an embossed magnetic strip to record transactions and to activate the system. In case of Electronic Fund Transfer at the Point of Sale, it is used. This is a consumer payment system which allows a consumer to pay for goods and services by conveying details of the transaction

infrastructure required to support electronic commerce. The comparatively narrower definition includes business to consumer and business to business electronic transaction. The narrowest definition includes business to consumer electronic transaction with electronic payment system (Fig-6).[29]

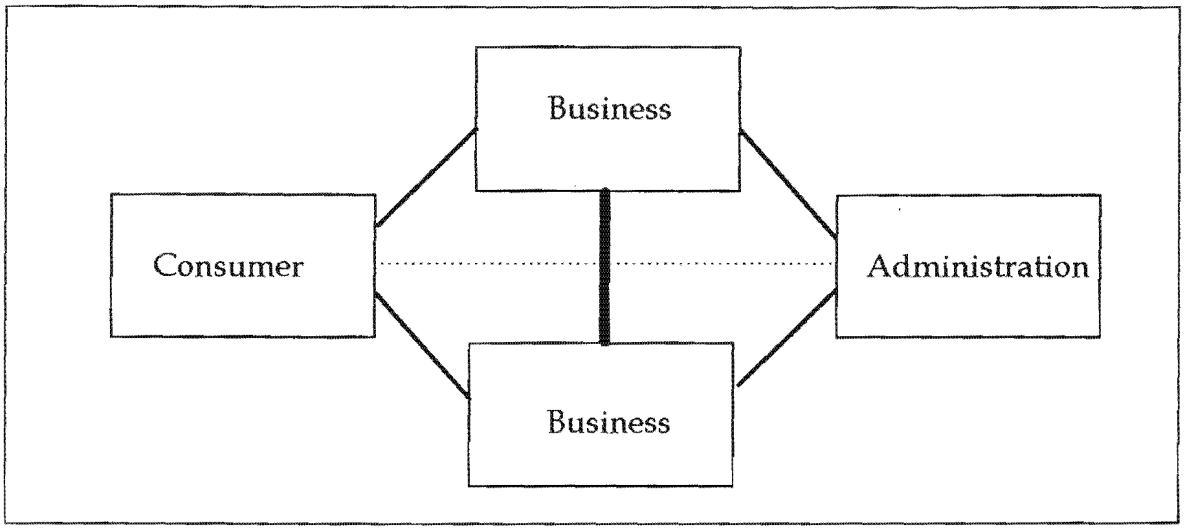


Fig-7

---

to the payer and payee bank, without using any paper vouchers. Credit transfer systems help a person to make payment through his bank either to other customer of the same bank or those of other bank. Thus if X has to pay Y, he may either write out a cheque or if he is using electronic fund transfer, he may instruct his bank to credit Y's account with the specified amount. In this, things which are required are a terminal in the super market, linkage between this terminal and the customer's bank and a plastic card. The manner of operation is that the customer purchases goods or services and then produces the plastic card at the counter. The plastic card activates the terminal and the consumer's account is debited and the seller's account is credited.

29 Supra note 26.

Electronic commerce can be sub divided into four categories business - business, business - consumer, business - administration, consumer - administration (Fig-7). In business - business category, company uses a network for ordering from its suppliers, receiving invoices and making payments by using Electronic Data Interchange[30] over private or Value Added Network.[31] The business - consumer category is like electronic retailing using Internet which offers all sorts of consumer goods from cakes to computer. The business - administration category covers all transactions between companies and government organisations. With the growth of electronic commerce, administration may offer option of electronic interchange for transactions like Value Added Tax return and payment of corporate taxes. The consumer - administration category has not yet emerged but in future government may extend electronic interaction to such areas as self assessed tax return.[32]

---

30 Electronic Data Interchange refers to the exchange of business information, including purchase orders and invoices between computers used by cooperating companies.
PETE LOSHIN, PAUL MURPHY, ELECTRONIC COMMERCE, 271 (Jaico Publishing House, 1998).
For further discussion see chapter II.

31 Value Added Network is a third party network service provider who offers Elecronic Data Interchange service which can be used by a company who has decided to communicate via Electronic Data Interchange.

32 *Electronic Commerce - An Introduction,* Esprit home page, pp.3-4, URL: <http://www.cordis.lu/esprit/srce/ecomint.ht>.

All trade - between retailer and consumer, supplier and manufacture - revolves around communication in its broadest sense, communicating messages about the goods themselves, their utility, unique selling points, communicating orders or request for information and communication in the sense of transporting those goods to the market. Where Internet can help in the communication of correspondence, it can also support this trade communication. The basic measure of marketing success is the sale of the advertised goods. The order from consumer to retailer or manufacturer to supplier informs the supplier of the requirement to be filled and results in the delivery of two things - the goods themselves and an invoice. The invoice results in payment which in turn results in a receipt. This is therefore the basic chain of the trading process, marketing, delivery, invoice, payment, receipt and customer service.[33] Some or all of this chain can be transferred to the domain of Internet. So if an environment is created in which electronic commerce can grow and flourish, then every computer will be a window open to every business, large and small, everywhere in the world.

---

33 NEIL BARRETT, THE STATE OF CYBERNATION 79.

I.2. INSTRUMENTS OF ELECTRONIC COMMERCE

There are six main instruments of electronic commerce which can be distinguished. These are telephone, fax, television, electronic payment and money transfer system, Electronic Data Interchange and the Internet.[34]

Growing Networks for Electronic Commerce

(Million units)

Category	1991	1996	2001 (Proj.)
Telephone main lines	545.0	741.0	1000
Cellular subscribes	16.3	135.0	400
Personal computers	123.0	245.0	450
Internet host computers	0.7	16.1	110
Personal computers with Internet access (Internet users)	4.5	60.0	300

Source: ITU, "Challenges to the Network", (1997a).

Fig-8

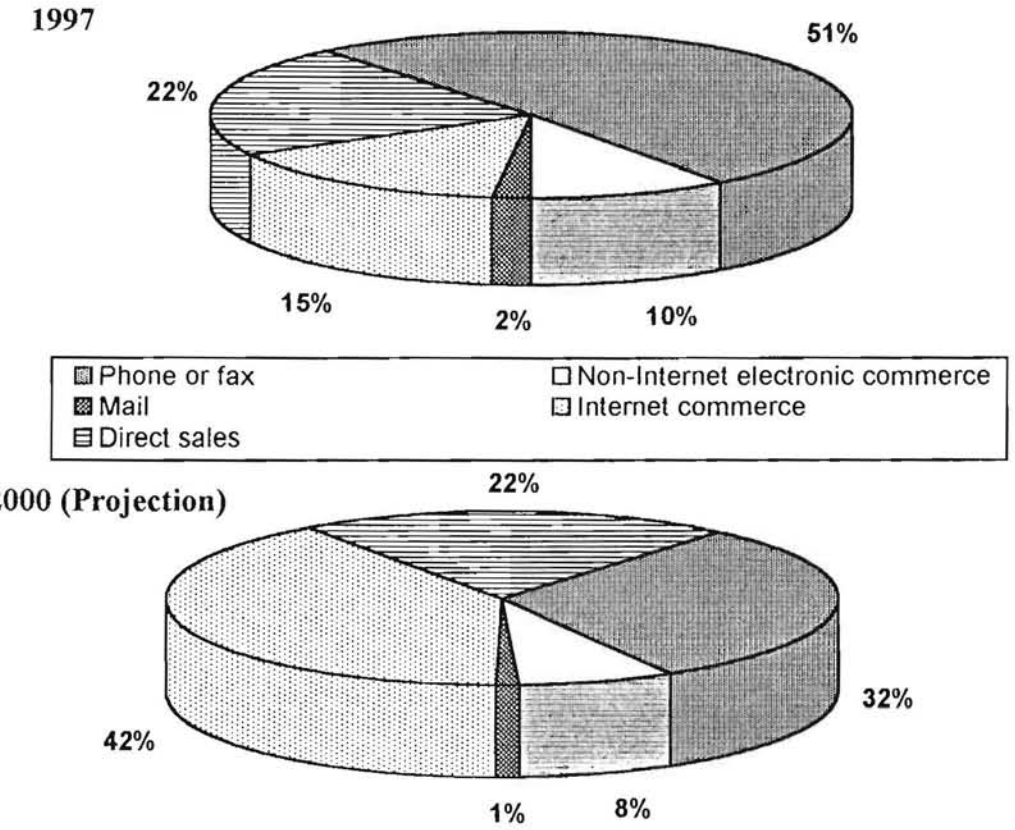
In most of the cases, electronic commerce refers only to the Internet and other network-based commerce. But instruments like telephone, fax and television are already used for commercial transactions. It is very much usual to get information about some product from television advertisement and to place order over phone and pay through credit card. So it can not be said that emergence of new instruments such as Internet has brought electronic commerce for the first time (Fig-8) but it is true that, Internet has opened up many new possibilities. With the help

---

34 Features of Main Instruments (ANNEXURE-C)
Electronic Connection between retailer and customer (ANNEXURE-D).

of this instrument, all elements of commercial transactions can be conducted on an interactive basis with less time and lower cost. Thus Internet is regarded as much more versatile than other instruments of electronic commerce.[35]

Percentage of Different Instruments Used in Electronic Commerce During 1997 and 2000 (Projection)



Note: Based on a survey of 63 companies by Forrester Research Inc.
Source: Forrester Research, Inc., 1997.

Fig-9

35 Supra note 17 at 5.

One set of projection of electronic commerce suggests that by 1999, 13 per cent of all consumer shopping will be conducted electronically and this share will reach to 26 per cent by 2007.[36] Internet is expected to expand its market share from 2 per cent of all electronic sales to about 50 per cent in ten years time.[37] Another set of projection suggests that telephone is by far the most important instrument of electronic commerce but by 2002 Internet and other network based commerce will comprise one quarter of all electronic sales.[38] Forrester Research, through a survey has revealed the companies which already sell their products on Internet, still conduct half of their sales by telephone and fax. However the share of on-line sale is projected to grow to 42 per cent of all sales by the year 2000, as it is shown in the graph above (Fig-9).

I.3. WHY ELECTRONIC COMMERCE?

The growth of electronic commerce - the ability to perform transactions involving the exchange of goods or services between two or more parties using electronic tools and technique - is one of the most exciting aspects of Internet. Electronic commerce will play a significant role in our economy in the years to come. Electronic commerce will

---

36 FINANCIAL TIMES, September 3, 1997.
THE ECONOMIST, May 10, 1997.

37 Supra note 17 at 23.

38 Supra note 17 at 23.

provide an integrated collection of reliable service to handle tremendous volumes of business and technical transaction. Organisation will be able to improve efficiency, accuracy and reduce costs and will provide faster, more reliable and more convenient services (Fig-10). Smaller firms will be able to enter and participate at lower cost and with greater efficiency in new market and larger firms will be able to evaluate, select and more readily work with other companies.[39]

Supplier's opportunity	Customer's benefit
global presence	global choice
improved competitiveness	quality of service
mass customisation & "customerisation"	personalised products & services
shorten or eradicate supply chains	rapid response to needs
substantial cost savings	substantial price reductions
novel business opportunities	new products & services

Source: http://www.cordis.lu/esprit/src/ecomint.htm.

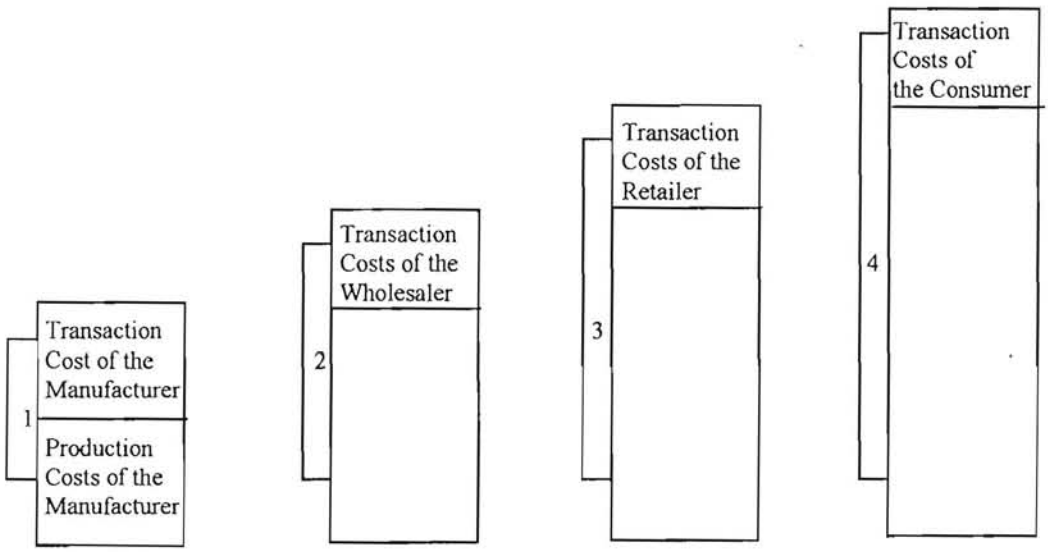
Fig-10

The boundaries of electronic commerce are not defined by geography or national borders but by the coverage of computer network. Electronic commerce enables even the smallest supplier to achieve a global presence and to conduct business world wide. It enables supplier to improve competitiveness by becoming closer to the customer. Many

---

39 Lawrence H. Summers, Deputy Secretary, Department of Treasury, United States (05/27/97 08:00:47) URL: <http://www.treas.gov/treasury/press/pr052297 a html>.

companies are using electronic commerce technology to offer improved levels of pre and post sale support, with increased level of product information, guidance on product use and rapid response to the customer queries. With electronic interaction, companies are able to gather detailed information on the needs of each individual customer and automatically tailor products and services to those individual needs. Electronic commerce allows traditional supply chains to be shortened dramatically (Fig-11). Goods can be shipped directly from manufacturer to the end consumer, by passing the traditional stoppages like wholesaler's warehouse, retailer's warehouse and retail outlet.

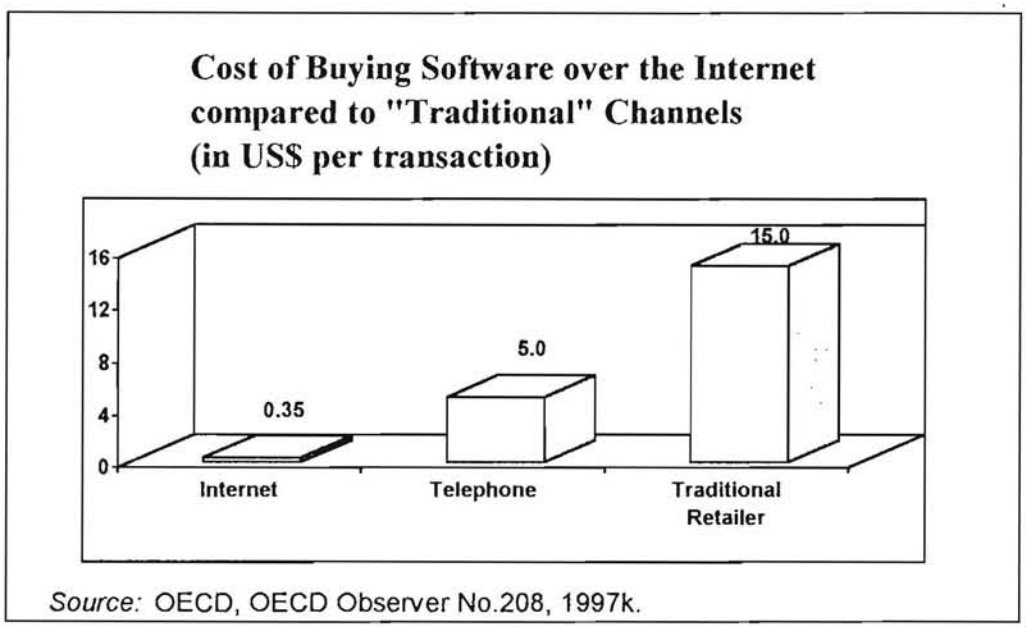


Market hierarchy and transaction costs in a stepwise fashion

- 1. Sales Price of the Manufacturer
- 2. Sales Price of the Wholesaler
- 3. Sales Price of the Retailer
- 4. Purchase Price for the Customer

Fig-11

In case of products and services that can be delivered electronically, the supply chain can be removed entirely. This has massive impact on things like film, video, music, magazines, newspaper. One of the major contribution of electronic commerce is a reduction in transaction cost (Fig-12).



Source: OECD, OECD Observer No.208, 1997k.

Fig-12

A.J. Campbell has observed that there are basic ten reasons why a company should be using E-Commerce to increase its competitive position in the global electronic market place.[40] On an individual level,

---

40 a - Getting started is easy - The starting point for most businesses is to develop a web page that contains basic information about the company, including a description about the nature of the business, the product list and how to reach the sales staff.

b - Faster and cheaper delivery of information - Printed materials of business such as brochures, sales pockets, price quotas, catalogues,

electronic commerce has created a host of opportunities for consumer to shop locally or globally. Merchants see it as a cost effective means of

---

product updates, technical specifications, new product information, cautionary information can be reached to the customers as soon as they are put on the Internet.

c - Quick feedback on new product - Getting information from customers about their likings and about their reaction against any product will help to adjust marketing strategy.

d - Improved customer service - The web pressure of a company acts as customer service centre which the customer can knock whenever they want.

e - Global audience - The World Wide Web is having now approximately 119 million users and it is expected to double in the next millennium. This massive audience is a positive reason for any business to go on line.

f - Levelling the field of competition - On the Internet, because of its unique feature, the impact of a large or small company can be similar. The difference lies on the fact that commitment, each organisation is going to make.

g - A Strategic Tool - Entering in to global Internet commerce world will bring new opportunities for the business which were not available earlier. Then to target potential buyer of a country becomes part of marketing plan.

h - It is cheaper than phone call - Sometimes trying to make phone call or sending mail can be difficult from some part of the world. In case of Internet, people can find the page, no matter where they are located. In some places, cost of making long distance call of extended duration can be very high. But due to highly competitive market of web access, cost of monthly charges is going down so much that the marginal cost of Internet based information comes less than international calling.

i - Enhanced business to business link - Using Electronic Data Interchange to link suppliers to producer to seller gives companies a fuller picture of supply and demand and saves time and money by shortening the ordering cycle.

j - Tough competition - With more and more businesses entering the web export market every day, your business has global competition. Along with good hold of actual market, a strong web presence is required to have advantage over the competitors.

A.J. Campbell, *Ten Reasons Why Your Business Should Use Electronic Commerce,* BUSINESS AMERICA at 12-14, May 1998.

increasing their customer base while consumers see Internet shopping as a fast, convenient way to shop or to pay bill electronically (Fig-13).[41] Electronic commerce is fast changing the way goods and services are brought and sold. Apart from shopping, electronic commerce is eliminating paper based transactions between organisations and streamlining the way corporations operate.[42] Modern communication and information technologies can enable change in organisation structures and business processes.

Business to Business Internet EC in Western Europe (in Millions of US dollars)	
1996	$ 214
1997	$ 681
1998	$1,795
1999	$4,343
2000	$8,809
(Source: International Data Corporation)	

Fig-13

Events within the market and market structure are experiencing changes due to increasing utilization of modern telecommunication media. The widespread use of personal computer coupled with telecommunication network and Internet has made paper-free trading reality.[43] In the traditional business office, records and documents have been recorded on visible media, predominantly microfilm. One of the

---

41 Chandra Agnihotri, *Cyber Shopping*, ASIAN AGE, June 14, 1998, p.5.

42 Id.

43 Supra note 24.

increasing their customer base while consumers see Internet shopping as a fast, convenient way to shop or to pay bill electronically (Fig-13).[41] Electronic commerce is fast changing the way goods and services are brought and sold. Apart from shopping, electronic commerce is eliminating paper based transactions between organisations and streamlining the way corporations operate.[42] Modern communication and information technologies can enable change in organisation structures and business processes.

Business to Business Internet EC in Western Europe (in Millions of US dollars)	
1996	$ 214
1997	$ 681
1998	$1,795
1999	$4,343
2000	$8,809

(Source: International Data Corporation)

Fig-13

Events within the market and market structure are experiencing changes due to increasing utilization of modern telecommunication media. The widespread use of personal computer coupled with telecommunication network and Internet has made paper-free trading reality.[43] In the traditional business office, records and documents have been recorded on visible media, predominantly microfilm. One of the

41 Chandra Agnihotri, *Cyber Shopping*, ASIAN AGE, June 14, 1998, p.5.

42 Id.

43 Supra note 24.

chief characteristics of these records is that they are physical objects, static entities, fixed and frozen in time and format. With electronic commerce, these organisations are in the midst of a historic change -a transition from visible to electronic media.[44] Because of electronic commerce, travel time and coat have been virtually eliminated for the buyer. Both buyer and vendor have merely perfect information about goods and services being marketed. Entering and exiting market place are relatively easy for both buyer and seller. Buyers will have substantial number of vendors to choose from (Fig-14) and vendor will have greatly expanded market that is not geographically based.[45]

World Wide Web Prices for Spyder™ Paintball Gun on October 19, 1996

Company	Price
Aretic Paintball	$240.00
Coast to Coast	139.95
Command Post	199.95
HORC	194.95
Olympic	175.99
On the Go	162.50
Paintball Headquarters	169.95
Paintball Mania	182.95
Paintball On-Line	176.53
Paintball Paradise	159.00
Planet Sports	159.99
Skan-line	164.85

Sypder™ is distributed by Kingman International Corp. (Walnut, California).

Fig-14

44 David O. Stephens, *Electronic Record Keeping Provisions in International Laws,* RECORD MANAGEMENT QUARTERLY at 72 (April 97).

45 ROBERT A. PATERSON, ELECTRONIC MARKETING AND THE CONSUMERS 12 (Sage Publication, 1997).

Through Internet, it is possible to get the lowest possible price offered for a particular good and competitive pressure will lead to average price levels that are lower than those that currently exist. This competition will not be limited to the Internet alone rather it will affect traditional retailing as well. For example, one can now get a price quote on the Internet for a particular product and then that price quote can be taken to a local dealer to negotiate the price and thus retail margin will shrink.[46] Among direct benefits of electronic trading are reduction in transaction cycle time, improved accuracy and lower cost per business transaction (Fig-15).

Speed and Costs of Different Ways of Document Transmission*

	Costs (US$)	Time
New York to Tokyo		
Air Mail	7.40	5 days
Courier	26.25	24 hours
Fax	28.83	31 minutes
Internet e-mail	0.10	2 minutes
New York to Los Angeles		
Air Mail/	3.00	2-3 days
Courier	15.50	24 hours
Fax	9.86	31 minutes
Internet e-mail	0.10	2 minutes

Example of sending a 42 page document.
Source: ITU, "Challenges to the Network", 1997a.

Fig-15

46 Supra note 45.

Among with indirect benefits of electronic trading are improved responsiveness, higher productivity, enhanced integrity of business information, eradication of issue like inter working between geographical areas, closer working relationship with trading parties, exploitation of new business opportunities.[47]

I.4. SCOPE OF ELECTRONIC COMMERCE

Business of all sizes to understand the role that telephone, computer network and technology can play in creating new possibilities. And if they can exploit this potential, they will be successful entrepreneurs and business persons who will bring new product to the market, increase consumer's choices, lower costs and improve national economics.[48] The Internet, intranet, extranet and other communication networks are lowering entry business to commerce, enabling both small and large firms as well as consumers to engage in and benefit from electronic commerce. Electronic commerce is already generating important sales and savings for businesses.[49]

---

47 PETER GARDNER, ELECTRONIC TRADING - A PRACTICAL HANDBOOK, 42 (Butterworth Heinemann, 1994).

48 The volume of electronic commerce is poised to top $2 billion this year, according to IBM's electronic payment and certification division. Transaction through plastic cards make up as much as 6 per cent of the world's economy, according to S. Ramani, Director, National Centre for Software Technology, Mumbai and President, Computer Society of India, SEEARCC '97 - *Electronic Commerce and Regional Development*, NEWS BYTES NEWS NETWORK (December 12, 1997).

49 Larry Irving, *The Risks and Rewards*, ELECTRONIC JOURNAL at 29-73 1 November, 1997.

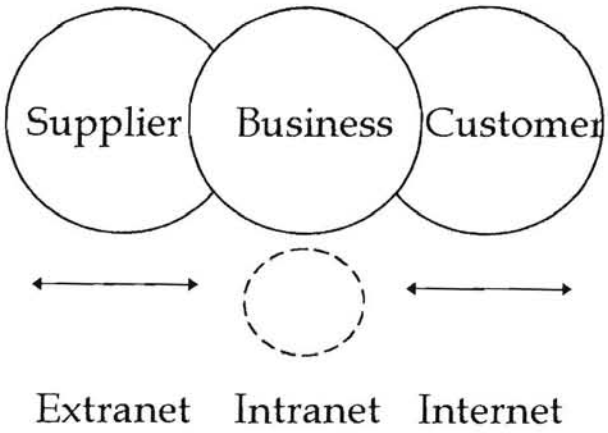
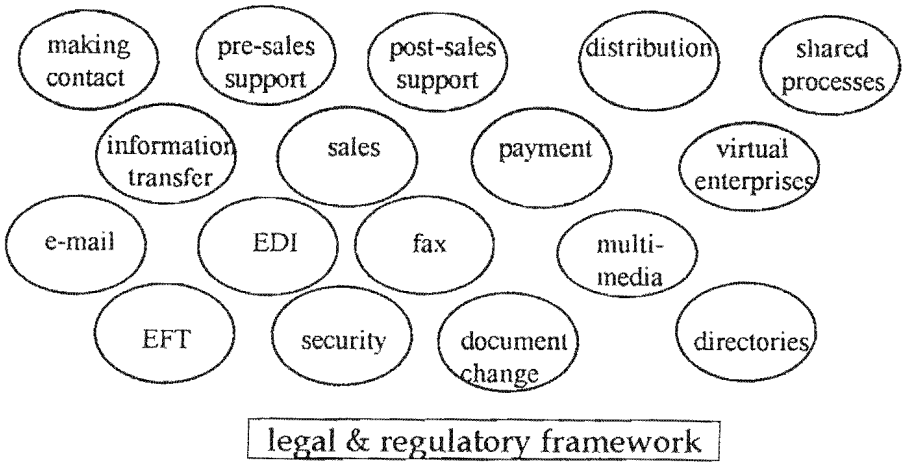


Fig-16

Electronic commerce - the new way of doing business, a composite of technologies and services that foster automated transaction of business and exchange of related information. This is done at three levels - within a business, between two business, one of whom could be a supplier, between a business and its customer. Since the back bone of electronic commerce is the global web of cyberspace, each of these interlocking circles of operation is enabled by a network. The interchange within a business is commonly known as an intranet. The transaction with another business as a supplier is called as extract and for coming together of buyer and seller, there is great electronic bazar-Internet (Fig-16).[50]

---

50 Anand Parthasarathy, *Cyber Business: A New Model for the Millennium,* THE HINDU, March 12, 1998, p.27.



Scope of Electronic Commerce

Fig-17

Electronic commerce is not a single uniform technology, rather it is characterised by diversity. It encompasses a wide range of business operations and transactions.[51] Also it encompasses a wide range of

---

51 a. establishment of initial contract, for example between potential customer and potential supplier.
b. exchange of information.
c. pre and post sales support, like, details of available products and services, technical guidance and product use, responses to customer questions.
d. sales.
e. electronic payment using electronic fund transfer, credit cards, electronic cheque and electronic cash (for further discussion, see Chapter III).
f. distribution - including both distribution management and tracking for physical products and actual distribution of products that can be delivered electronically.
g. Virtual enterprises - groups of independent companies that pool their competencies so that they can offer products and services that would be beyond the capabilities of any of the individual companies.
h. shared business process that are jointly owned and operated by a company and its trading partners.
Electronic Commerce - An Introduction, esprit home page,
URL:<http://www.cordis.lu/esprit/src/ecomint.ht>.

communication technologies including e-mail, fax, electronic data interchange and electronic fund transfer (Fig-17). Any of these technologies can be used to support electronic commerce, with the choice between them according to the context. There is also a need for a well defined legal and regulatory framework that is conducive to electronic commerce to facilitating electronic commerce by removing the barriers.[52] As the global interaction is one of the main pillars of electronic

---

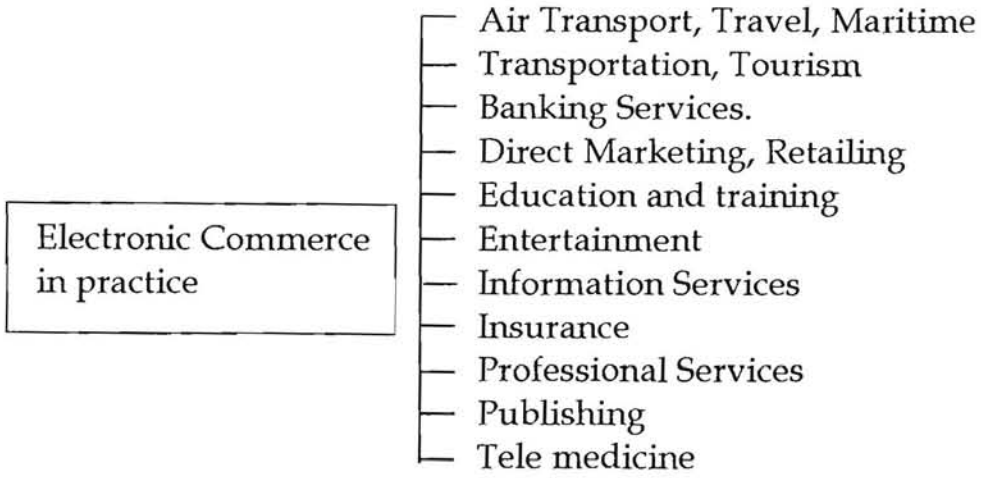
52 Apart from these, the secrets of selling on the web are as follows -

a. Choose the right niche - Niches as the Internet are based on what you sell, not where you are. So one should choose a niche small enough that you can dominate it.
b. Have high production values - High production values are critically important in catalogue, which have to convince consumers to buy based on a few sheets of paper.
c. Make your site easy - Visitors to a web site will leave at the slightest obstacle. So if people has to visit and order from the site, it is suggested not to put any obstacle in the way.
d. Be real - Visitors need to be reassured that they are ordering from a real company. So one should put in the web page, his name, phone number, address, image of catalogue, customer testimonial, brief history of company.
e. Emphasize service - Visitor is to be informed that there is guarantee that he will be satisfied with what he buys, otherwise, money will be refunded without any question.
f. Promote site - Most sites get most of the hits from search engines, so the web page is to be indexed with the search engines.
g. Lower the price - The emotional satisfaction of getting something at the cheapest price is almost like a drug. People will go to any length to get it.
h. Change site - Regular change in a web site is a form of high production value.
i. Think globally - It is to be shown that the vendor welcomes order from all over the world and shipping rate to each country is to be clearly informed.

Paul Graham, *Secrets to Selling on the Web*, WORLD EXECUTIVE DIGEST, 43-45 (August 1998).

commerce, thus legal and regulatory framework must have a global scope.[53]

I.5. ELECTRONIC COMMERCE IN PRACTICE



Over the last few years, more and more business houses, research organisations, educational institutions are putting up their sites on the Net. On-line service is available for airlines, freight carriers, travel agencies, booking services, tourism information resources. Web sites, e-mail, customized software provide Internet assess with an ever-expanding list of options to conduct business, plan vacations, take advantage of special travel opportunities.[54]

---

53 Supra note 33 at 5-6.

54 Eugene Alford, *Air Transport and Travel on the Internet: Flying and Shipping in the Computer Age*, BUSINESS AMERICA at 25 (January 1998).

Kenair Travels

- Web travel agency business
- Tours, specials on the web
- Customer interaction and transaction on the web
- Extensive backup infrastructure to keep the web information up-to-date and accurate

A business can contract for the pick up, shipment and tracking of its product and then book air travel, hotel and rental car for an executive to visit its customer through the Net.[55] The maritime industry has long been a user of electronic commerce. Information about a large number of transactions in the United States maritime trades between shippers and carriers, as well as between ocean carriers and other modes of transport in intermodal transport movements, is communicated electronically. The data contained in bills of lading, deck receipt, certificates of insurance, are generated and transmitted electronically. With the development of electronic commerce, shipping contracts will be signed and transmitted electronically.[56] Both shippers and carriers can incur substantial costs

---

55 The on-line air ticket sale can reach upto $4 billion by the year 2000 from an estimated $700 million in 1997.

56 C. William Johnson, *Maritime Transportation: Ocean Carriers Sail the Electronic Sea*, BUSINESS AMERICA, at 25 (January 1998).

when the paper trail becomes congested. The use of electronic signature for bill of lading and other documents can unclog the paper trail at every turn. Electronic negotiable bill of lading, in addition to speeding the data movement process, can solve the problem of paper work needed to release a cargo before ship reaches port as in maritime industry, negotiable bill of lading provides evidence of ownership. If the carrier releases the cargo to someone without original bill of lading, the carrier faces the risk of the claim of actual holder and liability for loss of cargo.[57]

Electronic Commerce Applications

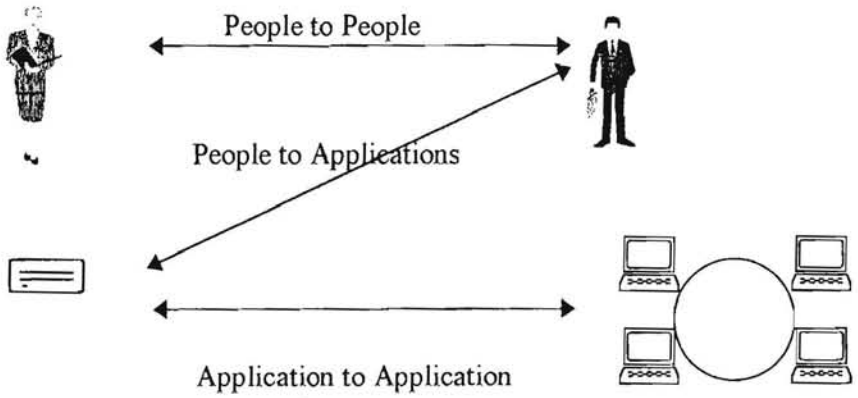


Fig-18

Electronic commerce presents the greatest challenge to and opportunity for commercial banking sector. Electronic commerce is specially attractive to banks and other organisations that deal with

---

57 Supra note 56.

mountain of paper. With the entry of home banking via personal computer, telephone based banking, automated kiosks, the conventional bank finds itself at an economic and cultural cross road. Electronic commerce, Internet banking and interactive banking allow customer to monitor checking, savings, credit and account activity and balances, transfer funds including paying third party bills, review their credit line status and send electronic mail to customer service (Fig-18).[58] Banks provide tools to customer to make informed investment decision by informing real time quotes, company news, research, stock, corporate bands, treasuries, options and mutual funds trading. Electronic commerce poses threat of fraud, loss, insolvency, piracy and unchecked issues of electronic money.[59] Barclays Bank (http://www.barclays.co.uk) has offered full banking services to the customers from their home computer. Electronic Share Information Ltd. (http://www.esi.co.uk) offers on line share information and trading facility. Customers can view London Stock Exchange prices and buy and sale shares on line.[60]

---

58 John R. Sieugmund, *Banking Services: Harness Technology And Come Up With a Winning Business Strategy Which Continues to Serve Public Interest,* BUSINESS AMERICA at 27 (January 1998).

59 Id.

60 Supra note 32 at 8.

Netscape - (ISN - Your Personal Computer Superstore)
File Edit View Go Bookmarks Options Discovery Window Help
http://www.Internet.net/ N

Internet Shopping Network

Your #1 source for computer products Free membership

Find it Here	What's New?	Today's Hot Deals
• Accessories • Desktop Computers • Drives • Memory & Processors • Modems • Monsters & Video • Multimedia Hardware • Networking • notebook Computers • Printers • Scanners • Software • Downloadable **Product Services** • Hot Deals Central • Rebates & Specials • Product Advice **Product Search**	CUPID'S QUEST Enter to win a video conferencing package to keep in touch with your valentine! JUST ARRIVED Hot low prices on new Microsoft Office '97 products Get MS Upgrades at $40 off our low prices PERSONAL PRODUCT NEWS	Block Financial Kiplinger Tax Cut 96 Acoleim Ent. NEA Jem Tourn. Ed. (DOS) Symantee Healthy PC 1.0 (Win98) Matrox Mystique PCI 2MB+SGRAM Labtec LCS-1012 Amplified Comp Spkrs Magnetically

Fig-19

Today direct marketers are some of the premier users of electronic commerce. Whether it is a catalog company directly marketing goods via Internet or a distribution center transferring information to its supplier of goods through Electronic Data Interchange, direct marketers are increasingly using electronic commerce to promote products and serve their customers (Fig-19). As postal and paper rates continue to rise, direct marketers may increasingly switch from using printed materials to utilize

the Internet.[61] The Internet allows the retailer to reach both customers and supplier and provides another medium for retailers to expand internationally at a relatively low cost.

Amazon.com (http://www.amazon.com) is an on line book store offering more than 2.5 million titles with sales increasing at a rate of 30 per cent each month.[62] Virtual Vineyards[63] (http://www.virtualvin.com) offers wines and gourmet foods, providing an outlet for a number of California wine producers. There is detailed on-line information on the various wines and foods and also an on-line query service through e-mail. Customers can order and pay through credit card and electronic cash.[64]

Education and training providers use progressively advanced methods to offer their services as new electronic technologies are developed. Fax, video tapes and distance teaching are giving way to on-

---

61 The Direct Marketing Association has reported that in 1996, the direct marketing has generated as estimated $640 billion in consumer sales and $500 billion in business to business sales and within five years it is projected to reach $1.8 trillion.
Bruce D. Harsh, *Direct Marketing's Future In Electronic Commerce,* BUSINESS AMERICA at 29 (January 1998).

62 Aaron Schavey, *Retailing On-line: Today's Promise and Tomorrow's Opportunity,* BUSINESS AMERICA at 40 (January 1998).

63 The full text of the web page (ANNEXURE - E).

64 Supra note 33 at 7.

line instruction and electronic commerce.[65] A person in Korea with a credit card can, by accessing the Internet services, register and work for a master's degree from University of Maryland, without ever coming to United States. The training materials can be transformed to multimedia documents, capable of integrating video, audio broadcast, three-dimensional graphics and animation with Internet technologies to make learning more interactive for the participants.[66]

Electronic commerce offers entertainment industries both opportunity for profit and risk of loss. Opportunity for profit arises when electronic commerce offers new delivery system for filmed entertainment and recorded music and risk of loss results from piracy over Internet of copyrighted movies and musics.[67]

Information services consists of data processing, network services, professional computer service and electronic information services. Many

---

65 Achamma C. Chandersekaran, *Education and Training Transformed By Internet - Enabled Electronic Commerce*, BUSINESS AMERICA at 31 (January 1998).

66 Id.

67 According to International Intellectual Property Alliance due to inadequate copyright protection over Internet, copyright based industry has suffered a loss of $10.7 billion, of which motion picture and music company's loss is $1.8 and 1.2 billion respectively. Computer program and books account for rest of the loss.
John E. Siegmund, *Entertainment and Electronic Commerce*, BUSINESS AMERICA at 33 (January 1998).

information service companies are providers of electronic commerce applications and services.[68] Network service firms are increasingly looking to the Internet for new business opportunities and are providing more sophisticated forms of electronic commerce, including services which facilitate sales and customized research over the Internet.[69]

The back office operations of insurance companies are almost all computerised and operate on an electronic commerce basis. Accounting, financing, investment, management, fund transfer, underwriting, product development and claim support are done electronically.[70] In addition, the vast majority of transaction between insurer, other insurer, agents and brokers, reinsurer, bank and other financial institutions are carried out by electronic means.[71]

Professional service providers, such as architects, engineers, accountants, lawyers and management consultants have potential to

---

68 Jennifer Tollarico, *Information Services and Electronic Commerce*, BUSINESS AMERICA at 34 (January 1998).

69 Id.

70 Bruce McAdam, *Insurance: In Electronic Commerce a Risk?*, BUSINESS AMERICA at 36 (January 1998).

71 Statistics show that in 1997, premium sales of personal, auto, home owner and life insurance on the Internet was about $200 million and it is projected that it will reach $6.3 billion by 2006.

increase their opportunities remarkably through electronic commerce. Architects and engineers can transmit technical drawing to colleagues or clients and accountants, lawyers and consultants can provide advice and counsel electronically.[72]

GE Trading Process Network (TPN)

- US$ 1 Billion purchases per year Electronically
- 1400 suppliers
- Request for bids include drawings, designs, etc.
- Bid submission also electronic
- Average bidding process time reduced by 50%
- Ability to procure internationally, more suppliers
- Cost reduction 5% to 20%!!
- Plans to include suppliers' suppliers as well.

Professionals and their firms can bid and win contracts without handling ream of paper, sending over night mail, having telephone messages, spending hours travelling to meet with clients and waiting indefinitely for answers. Electronic commerce also improve internal integration of the firm.[73] Mr. Joroen de Kreck, (http://www.dds.nl/de creek), a lawyer from Amsterdam provides a legal question answering service that is available 24 hours a day. He responds to the question

---

72 J. Mare Chittum, *Professional Services: Knowledge Transfer Redefined Through Electronic Commerce*, BUSINESS AMERICA at 38 (January 1998).

73 Id.

within two hours. The response to the first question is free but subsequent questions incur charges.[74]

On-line publishing offers potential benefits to publishers by dramatically reducing publishing cost, such as cost of printing and binding manuscript, distribution cost, inventory cost. On-line publishing has potential to reach much wider audience, including international market at a relatively low cost. It is estimated that publishers can cut their cost by 75 per cent by using electronic commerce.[75] Since retail book stores cannot afford to stock copies of all books, on-line publishers can offer to make such books directly available to readers through Internet. Electronic publishers have exploded a new way by offering on line version of newspaper.[76] The Times (http://www.the-times.co.uk) is now published on-line. The complete content of the newspaper is available and access is free.[77]

Telemedicine represents the most important application of electronic commerce that has emerged in the health care service sector in

---

74 Supra note 32 at 10.

75 Supra note 62.

76 Supra note 62.

77 Supra note 33 at 10.

recent years. It is a means for providing health care and communicating health care information over vast distances with the help of telecommunication technology.[78] This method can include transmission of basic patient data, images of X-Ray, ultrasound, magnetic resonance through computer network. Consultation with medical specialist and patient interviews offer another application of this form of treatment. The objective of telemedicine is to upgrade the quality and minimize the cost of medical care through easing communication of critical information between health care specialists.[79] One of its chief benefit is the elimination of the necessity for physician and patient to be in the same geographical region. U.S. medicinal service firms have already acted to reap the domestic benefits of this advanced technology form of health care delivery.[80]

I.6. HOW DOES THE SYSTEM WORK?

Internet can support the complete trade process or substantial part of it. Internet provides rapid access to information sources provided by marketing-service organisations. These services can be accessed by means of Internet-supported connection. Internet facilitated marketing

---

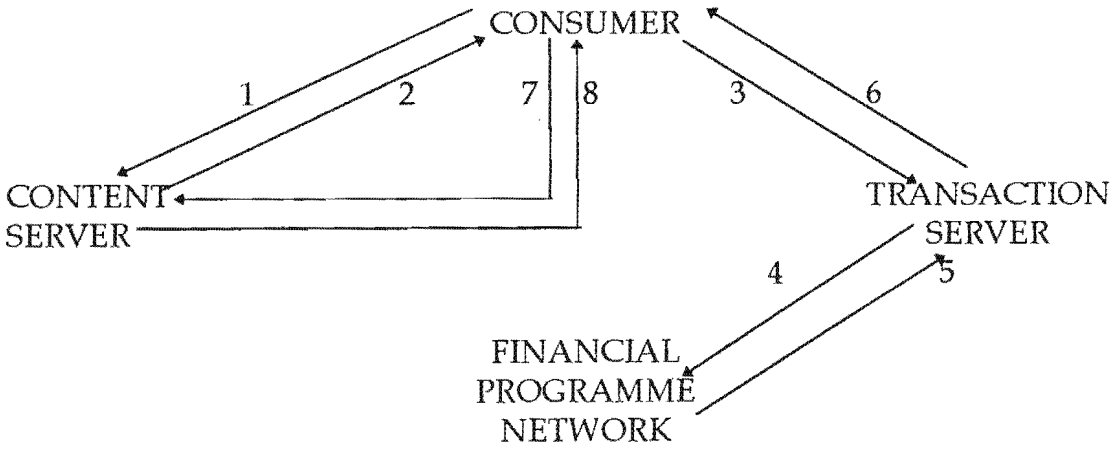
78 Ernest D. Plock, *Telemedicine is Emerging as a Cost-Effective Healthcare Alternative*, BUSINESS AMERICA at 42 (January 1998).

79 Id.

80 Supra note 78.

device is web page. Web page is the digital equivalent of a market stall.[81] The establishment of web page ensure the identity of the company within the Internet and it can be located by the prospective customer. It carries a host of relevant information. A customer can browse through that web page and comes to know in detail about the required goods - its description, price range, video clip of model, etc. To find a particular item or locate a particular web page, it is necessary to know the address of the page, in which case it can be accessed immediately, otherwise, a research has to be performed.[82]

Open Market's: Transaction Model



Source: Robert A. Paterson, Electronic Marketing and the Consumer, Sage Publication, 1997.

Fig-20

81 Supra note 33 at 79-91.

82 Supra note 33 at 92.

1) Consumer requests price and purchase information to Content Server.
2) Content Server sends price and purchase information to consumer.
3) Consumer begins transaction with specified Transaction Server.
4) Transaction Server sends consumer transaction information to Financial Processing Network for authorisation.
5) Financial Processing Network responds to Transaction Server with authorisation (allowed or denied).
6) Transaction Server sends sales confirmation on confirmed transaction to consumer.
7) Consumer request Content Server for product with confirmation from Transaction Server.
8) Content Server deliver products to consumer.

The individual or organisation selling product or service through Internet is called the vendor and the individual or organisation buying the goods or service through Internet is called purchaser. But the purchaser is ordinarily presumed to be a private individual shopping from home using personal computer connected to the Internet and the vendor is a shop having Internet presence.

The Buying Cycle (Business to Business) - Customer initiated

Step 1

Customer aware of you already
Aware of a need and looking for suppliers
Ensure effective information on your websites to ensure you show up in searches
Belong to relevant electronic catalogs

Step 2

Customer interact with your site
Looks for product, pricing, availability, service information
Wants answers to questions
Asks for quote, proposal

Step 3
Customer wants to place the order
Expects immediate order acknowledgement
Specific date/time of delivery
Commitment on quantity
Expects order status to be available for query on-line
Expects commitments to be met.
Delivery lead time expectations getting shorter.
Step 4
Invoicing, payments, etc.

The Buying Cycle (Business to Business) - Supplier Initiated

Step 1
You are aware of customers' web base sourcing site
Customer places Raps, RFQs on the Web.
Step 2
You interact with customer site
Look for product, delivery, support requirements
Seek clarifications
Check delivery capability (ex stock, change production schedule, etc.)
Submit quote, proposal
Step 3
Customer places the order
Expects order status to be available for query on-line
Expects commitments to be met.
Customer may initiate order changes.
Delivery lead time expectations getting shorter.
Step 4
Invoicing, payments, etc.

Source: Sanjiv Aiyar, Net Commerce Seminar, Confederation of Indian Industries, Bangalore, 1998.

At the basic level, to order particular goods, few steps are to be completed.[83] Along with these, to complete the purchasing, there has to

83 a. the general category of goods must be determined.
b. a vendor must be located and chosen.
c. the specific goods required must be identified.
d. the vendor must be informed of the goods and quantity required.
NEIL BARRETT, THE STATE OF CYBERNATION 92.

be a contract between the vendor and purchaser where vendor agrees to deliver the desired goods and the purchaser agrees to pay for those goods.

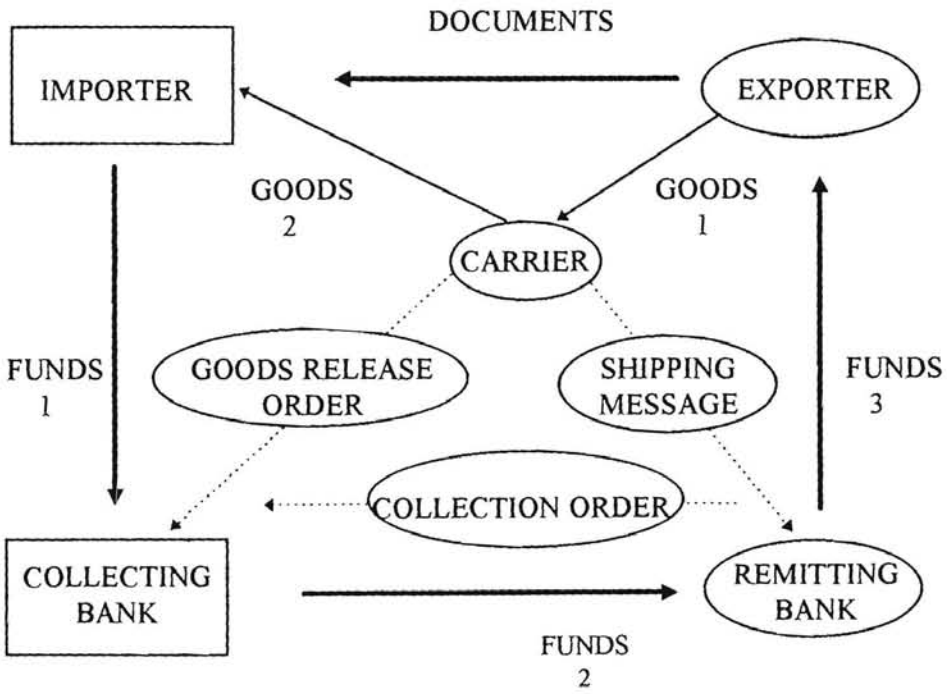


Fig-21

This agreement takes place through filing up forms. These forms are stored as part of the web page and they are ordinary files which have to be filled up.[84] The purchaser completes these forms by typing name, address, order details, into the appropriate parts of form. When the filling up of the form is completed, purchaser clicks on the "send" button

---

84 Andy Reinhardt, *Long on, link up, save big,* THE ECONOMIC TIMES, Bangalore, June 26.

and thus information is transmitted to the vendor. Here the criteria of placing order is fulfilled. When vendor receives order form, it becomes his responsibility to supply the ordered goods (Fig-21).[85]

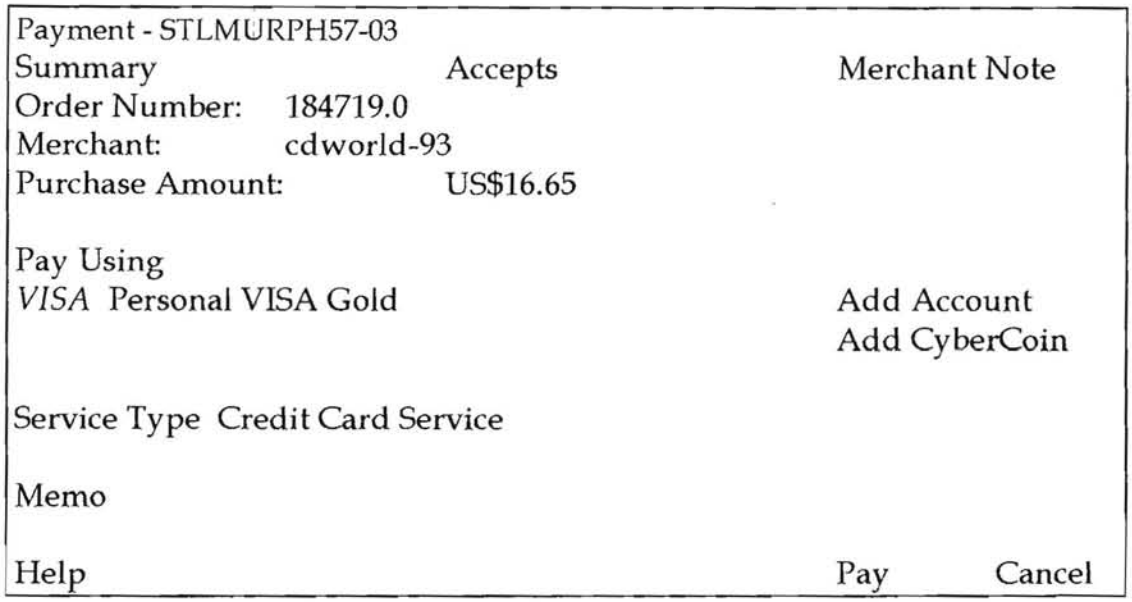


Fig-22

For the purpose of payment, vendor expects purchaser to simply provide payment detail, that is credit card detail over the Internet (Fig-22). But it is very risky to transmit credit card number in this way as there is every possibility to copy the number and use it elsewhere by others. So it is safe to transmit payment instruction through encryption.[86]

---

85 Supra note 47.

86 Encryption is a reversible process of modifying clear text for the purpose of keeping it secret from any one other than its intended recipient. (For further discussion see Chapter IV).

ELECTRONIC TRADE PAYMENT THROUGH SWIFT

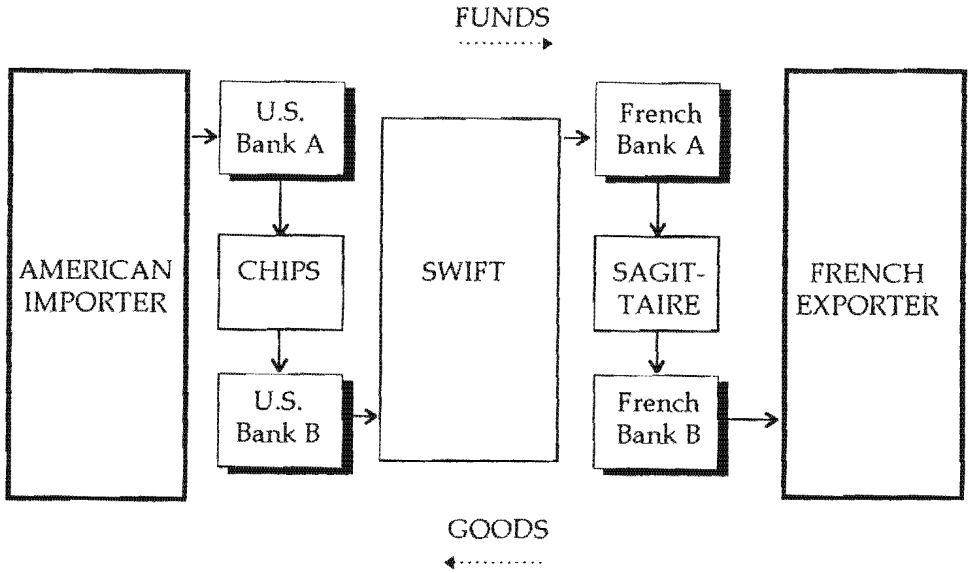


Fig-23

As in case of electronic order, there are number of risk factors,[87] it is better to encrypt either the whole order form or only the credit card details so that the information can only be read by the intended party (Fig-23).

---

87 a. form may not be genuine - it may not have been issued by the individual from whom it purports to come.
b. it may have been intercepted and read by some third party.
c. it may have been intercepted and altered by third party.
d. it must represent legally acceptable authority.
Ernest D. Plock, *Telemedicine is Emerging as a Cost-Effective health Care Alternative*, BUSINESS AMERICA at 42 (January 1998).

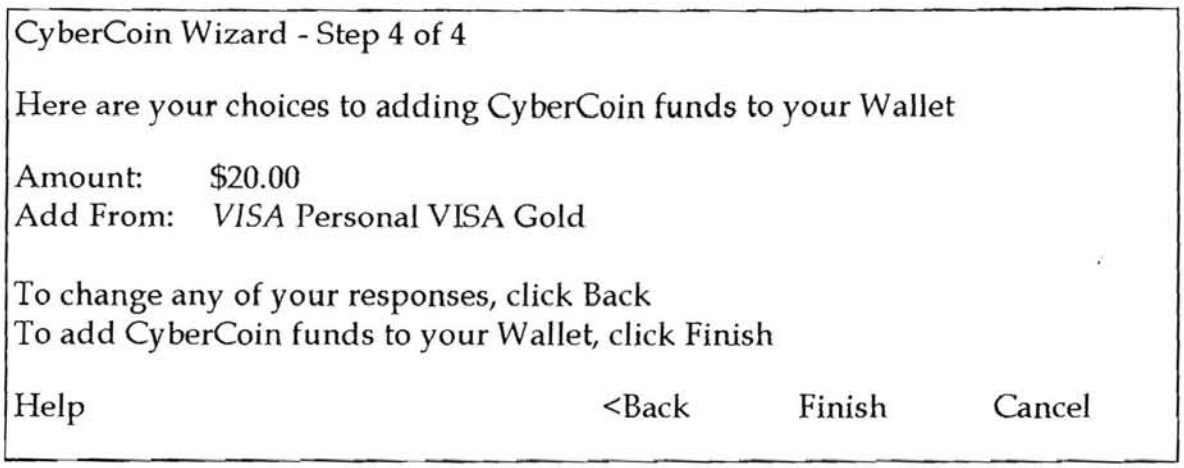


Fig-24

Payment can also be made through digital cash from digital wallet which is both mobile and untraceable and which allows individual to purchase goods from shop, equipped with this device to read and transfer digital coins from one wallet to another (Fig-24).[88]

Depending on the nature of the goods, for the purpose of distribution, goods have been classified into three categories.[89] For the first category goods, advertising, ordering, payment for the goods can be

---

88 Supra note 84.

89 a. goods that can be distributed through some 'real world' medium to the purchaser.
b. goods that can be distributed wholly over the Internet.
c. goods that can be distributed partially via Internet and partially through some 'real world' mechanism.
PETER GARDNER, ELECTRONIC TRADING - A PRACTICAL HANDBOOK 103 (Butterworth Heinemann, 1994).

effected through Internet but distribution of goods are carried out by some other means like, courier, parcel post, distribution from local shop, collection from some local point, etc. Clothes, equipments are few examples of first category of goods which can not be digitised to transmit through Internet.[90] The second category of goods like videos, software, music, books can be digitised and transmitted through Internet. But because of the risk of unwanted interception, these goods are transmitted in encrypted version.[91] In case of third category of goods, both Internet and other distribution mechanism are used. For example, in case of a computer game, a simplified versions of the game is made available, free of cost on the Internet and interested parties can download it and those who are interested in getting other episodes of the game have to place order through Internet and a CD-ROM will be delivered through standard postal service.[92]

---

90 Supra note 47.

91 Digital goods can be copied at any stage of transmission. When a file containing digitised goods are transmitted by the vendor to the purchaser over Internet, an intermediate host can take copy of that file. In that case, he gets a copy of goods without paying anything for that and as it is a master copy, he can create other copies from this. To avoid this problem, these type of goods are transmitted in encrypted form.
PETER GARDNER, ELECTRONIC TRADING - A PRACTICAL HANDBOOK 102 (Butterworth Heinemann, 1994).

92 Supra note 32.

Chapter II:

Electronic Data Interchange : the Precursor of Net Based Electronic Commerce

II.1. What is Electronic Data Interchange?

II.2. Benefits of Electronic Data Interchange

II.3. How Does Electronic Data Interchange Work?

II.4. Market Application of Electronic Data Interchange

II.5. Electronic Data Interchange Contract

II.6. Disadvantages of Conventional EDI

II.7. Internet and Electronic Data Interchange

CHAPTER II

ELECTRONIC DATA INTERCHANGE : THE PRECURSOR OF NET BASED ELECTRONIC COMMERCE

The growth of information technology has enabled businesses to establish new means of managing information flow both in intra and inter organisation level. The wave of modern technology and changes in business practice has brought the traditional paper-based method of communication in the verge of extinction. The paper-based communication stood as stumbling block for business expansion.[93] The electronic alternative to paper-based communication has reduced the cost of administration and also accelerated the whole transaction chain. Electronic Date Interchange[94] is one of the information technology tools for modern business.

---

93 Context for Electronic Data Interchange Use (ANNEXURE - F).

94 • In its simplest form, Electronic Data Interchange is the computer to computer exchange between two companies of standard business documents in electronic format.
Mohan Padmanabhan, *Benefits of Speedy Implementation in Ports and Customs*, BUSINESS LINE, April 13, 1998 at 4.
• The computer to computer transmission of business data in a standard format.
The United Nations Trade Data Interchange Directory (UNTDID), TRADE/WP.4/R.721.
• Electronic Data Interchange consists in using standardised electronic format to exchange business information.

II.1. WHAT IS ELECTRONIC DATA INTERCHANGE?

Electronic Data Interchange enables companies to conduct paperless, computer to computer exchange of business documents, in a structural format, over private or public data network, with little or no human intervention.[95] Electronic Data Interchange is a new mode of business communication, replacing standard paper documentation, such as invoices and purchase orders, with structured electronic messages.[96] Many businesses choose Electronic Data Interchange as a fact, inexpensive and safe method of sending purchase orders, invoices, shipping notices and other frequently used business documents.

II.2. BENEFITS OF ELECTRONIC DATA INTERCHANGE

The adoption of Electronic Data Interchange provides the opportunity to gain certain efficiencies and cost related benefits that improve information processing tasks and improve the business or manufacturing processes supported by information exchange between

---

Richard Hill, *Electronic Commerce, The World Wide Web, Minitel and EDI*, THE INFORMATION SOCIETY at 34 (Vol.13, No.1, Jan-Mar. 1997).

- The definition of Electronic Data Interchange is transmission of data structured according to agreed message standards, between information systems, by electronic means.

Art.1, 2nd definition, TEDIS Agreement.

95 LEN KEELER, CYBER MARKETING 51 (American Management Association, 1995).

96 Electronic Data Interchange can significantly reduce administrative cost, increase clerical productivity, increase speed of information flow, introduce just-in-time delivery, reduce inventories, ELECTRONIC TRANSACTIONS, § 5.2.

firms.[97] As Electronic Data Interchange eliminates paper work, it reduces significantly the number of times documents are processed by human beings.[98] Electronic Data Interchange has already reduced the cost of doing business among buyers, vendors, suppliers, manufacturers by ensuring the rapid flow of product, parts and materials and faster payment of bills and invoices. It can cut the time it takes to move product from the warehouse to showroom floor. Electronic Data Interchange, not only reduces paper works in conducting business transactions but also strengthens relationship with trading partners by creating tighter electronic relationship among Electronic Data Interchange trading partners (Fig-25).[99]

Frequency of Access by Type of Services

Banking services	25.5%
Travel (information, reservations)	11.5%
Catalog sales	7.5%
Professional database	6.2%
Training/development	4.4%
Classified advertising	4.2%
Generic database	4.0%

Note: Based on a survey of users. Not all types of service are shown - only those with potential relevance to electronic commerce.

Source: Richard Hill, Electronic Commerce, The World Wide Web, Minitel and EDI, THE INFORMATION SOCIETY at 35 (Vol.13, No.1, Jan-Mar. 1997).

Fig-25

---

97 Paul J. Harts, Carol S. Saunders, Emerging Electronic Partnership: Antecedents and Dimensions of EDI Use from the Supplier's Perspective, JOURNAL OF MANAGEMENT INFORMATION SYSTEMS, at 88 (Spring 1998, Vol.14, No.4).

98 The data is entered only once which eliminates rekeying, reduces errors and cuts clerical overhead. ELECTRONIC TRANSACTIONS, § 5.2.

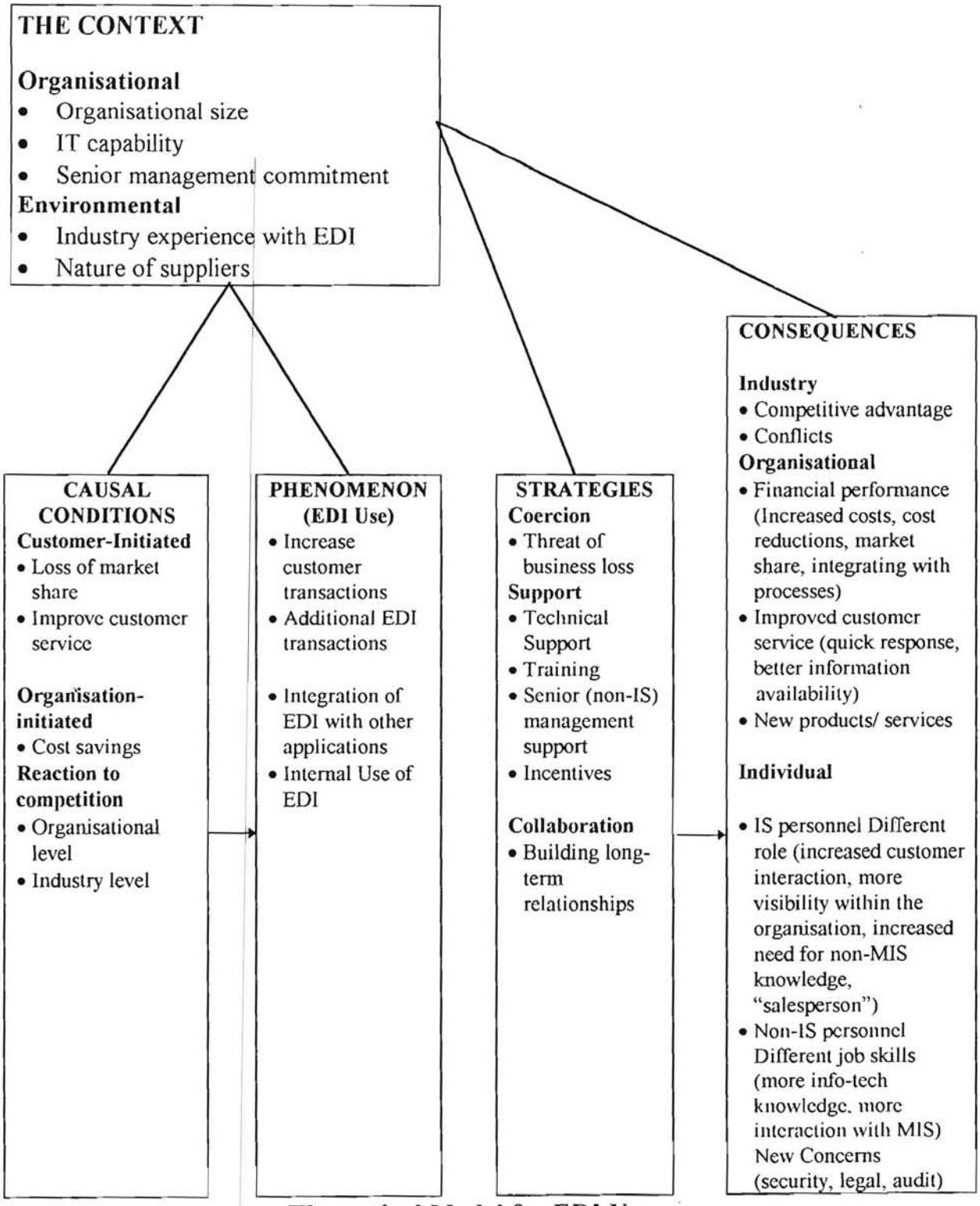
99 Supra note 95 at 52.

Manufacturers and distributors enjoy both actual and potential benefit from Electronic Data Interchange.[100] From a distributor's point of view, the potential savings in inventory carrying costs ought to be the primary motivation of adopting Electronic Data Interchange. Speed, accuracy and completeness of information permit both the distributor and the vendor to be more fully informed about their relationship. For a distributor, it is possible with Electronic Data Interchange to obtain reorder histories for products that are delivered directly to retail stores by vendors.[101]

---

100 (a) reduced order lead time, (b) higher service levels, (c) fewer out of stock situation, (d) improved communication about deals, promotions, price changes, product availability, (e) lower inventory costs, (f) better accuracy in ordering, shipping and receiving, (g) a reduction in labour cost.
LOUIS W. STERN, PATRICK J. KAUFMANN, ELECTRONIC DATA INTERCHANGE IN SELECTED CONSUMER GOODS INDUSTRIES: AN INTERORGANISATIONAL PERSPECTIVE, 56 (*Marketing in an Electronic Age*, Robert D. Buzzel ed. Harvard Business School, 1985).

101 LOUIS W. STERN, PATRICK J. KAUFMANN, ELECTRONIC DATA INTERCHANGE IN SELECTED CONSUMER GOODS INDUSTRIES: AN INTERORGANISATIONAL PERSPECTIVE, 56 (*Marketing in an Electronic Age*, Robert D. Buzzel ed. Harvard Business School, 1985).



Theoretical Model for EDI Use

Source: Connic W. Crook, Ram L. Kumar, Electronic Data Interchange: A Multi-Industry Investigation using Grounded Theory, Information and Management at 87 (34, 1998).

Fig-26

From the vendor's perspective, Electronic Data Interchange is viewed more as service and productivity enhancing tool than as a merchandising tool.[102] For manufacturer, real cost savings are that order processing costs will be reduced, sales person's role in the entire order taking process will be reduced (Fig-26). The increased accuracy, coordinated invoicing, shipment confirmation etc., which are provided by Electronic Data Interchange mark clear advantage over telephone ordering system. Crook and Kumar[103] in their research paper has pointed out that the chemical and tobacco companies perceived Electronic Data Interchange as something that major customers wanted and felt that it could provide financial benefit. Textile, chemical, Tobacco and Bank - all the four sectors have resulted in cost reduction after using Electronic Data Interchange. The tobacco company reported that they were able to reduce the staff in the purchasing department from 129 to 43 as a result of the use of Electronic Data Interchange. Information system personnel of all the four sectors have experienced increased interaction with the organisation's employees, with the help of Electronic Data Interchange.[104]

---

102 Supra note 101.

103 Connic W. Crook, Ram L. Kumar, *Electronic Data Interchange: A Multi-Industry Investigation using Grounded Theory,* INFORMATION AND MANAGEMENT at 85 (34, 1998) (ANNEXURE - G).

104 Id.

II.3. HOW DOES ELECTRONIC DATA INTERCHANGE WORK?

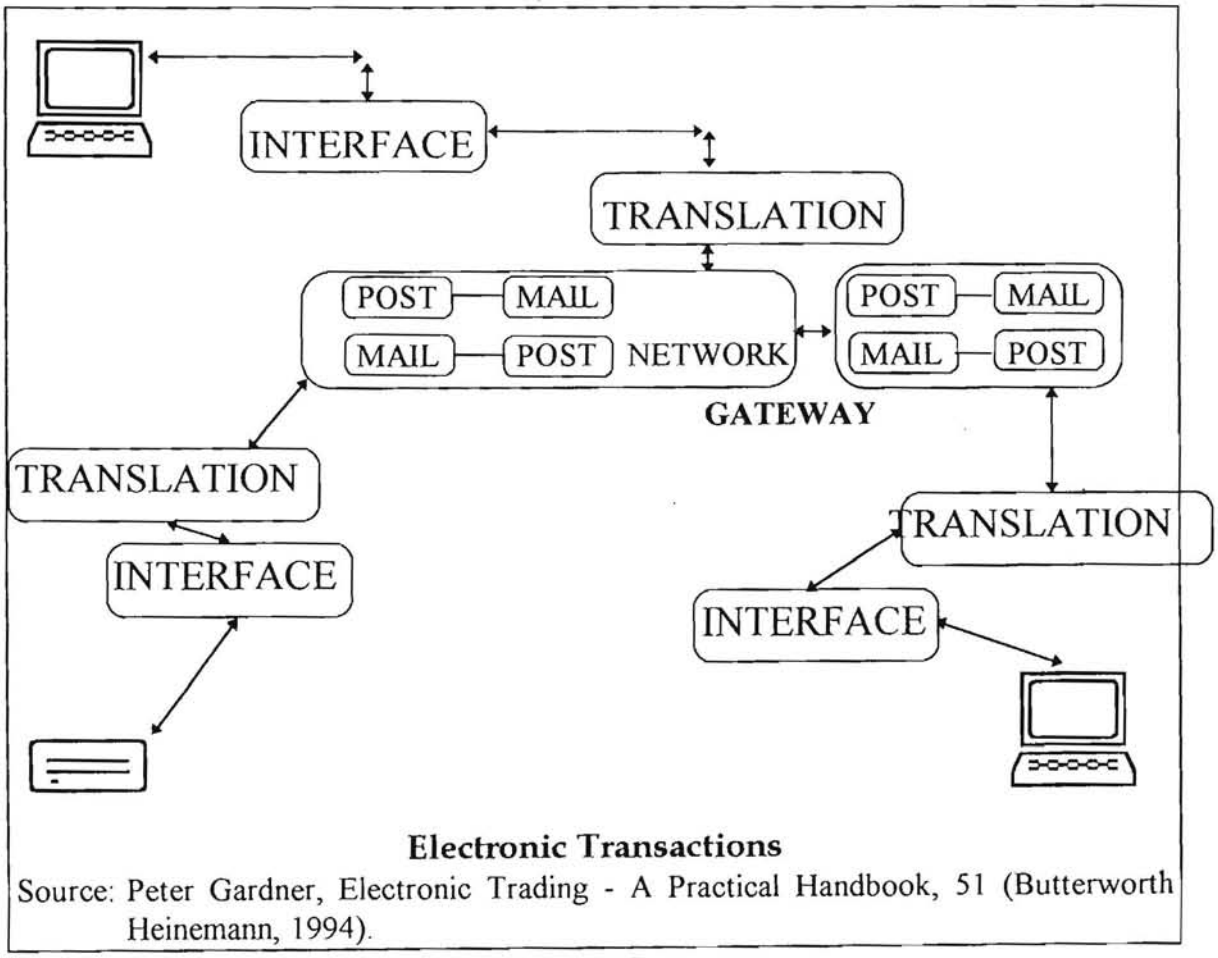
When a company decides to communicate via Electronic Data Interchange, it can generally choose between three methods -

a) physical transfer of computer media.

b) direct communication link via public data network.

c) by signing up to the service of a third party

d) Electronic Data Interchange network.

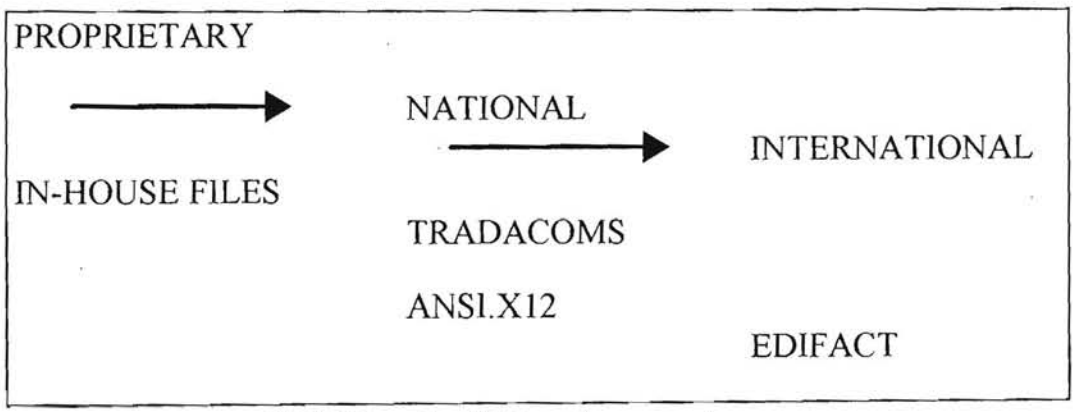


Electronic Transactions

Source: Peter Gardner, Electronic Trading - A Practical Handbook, 51 (Butterworth Heinemann, 1994).

Fig-27

To use Electronic Data Interchange as a tool to exchange message, a company has to enter into a trading agreement with the company with whom it wants to exchange document regarding the use of Electronic Data Interchange as an instrument of exchanging message. An Electronic Data Interchange service provider offers a range of services associated with electronic communication between a company's trading partners, such as message handling and translation as well as consultancy and project management (Fig-27). As the use of Electronic Data Interchange communications expands into all aspects of business communication, data users will increasingly need to submit messages to their network provider, to be passed on to their recipient trading partners via a different Electronic Data Interchange provides (Fig-28).



EDI Standard Development

Source: Peter Gardner, Electronic Trading - A Practical Handbook, at 51 (Butterworth Heinemann, 1994).

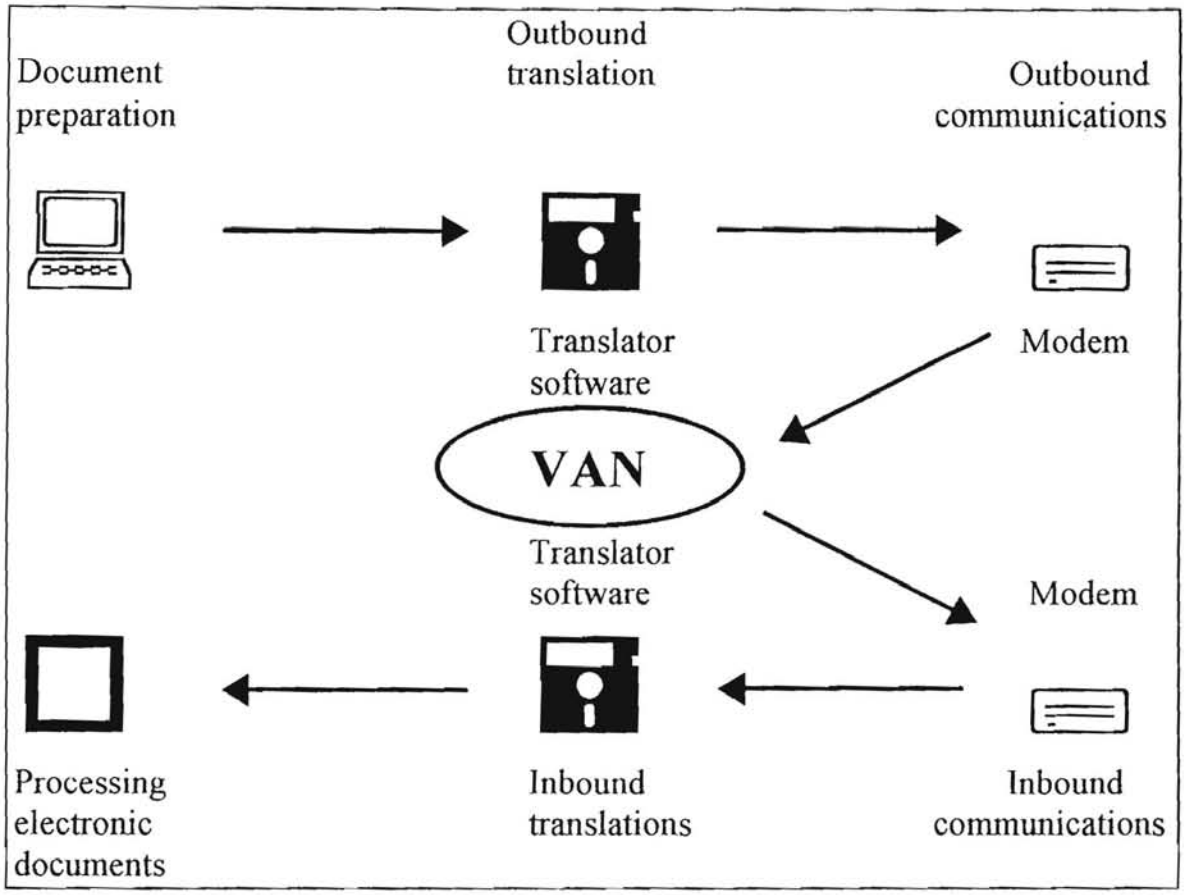
Fig-28

The company has to subscribe to a Value Added Network who will manage the flow of Electronic Data Interchange documents. A software is also required to interpret the message and to integrate into the existing software.[105] Then an Electronic Data Interchange document is to be created and sent to the trading partner through Value Added Network (Fig-29).[106]

---

105 There are three aspects to the successful transfer of data through a communication network - communication protocol, message standard and translation software. Communication protocol relate to the effective and efficient transfer of data between the various components within the network. Electronic Data Interchange message standards are concerned with the information content of the communication. An Electronic Data Interchange users will also need to have some form of translation software to convert the Electronic Data Interchange message standard into a format which can be used within company's internal applications. A message standard is usually drafted to reflect the options and alternatives regarding information content that the trading parties may wish to exchange. Electronic Data Interchange message standards have been created within industry groups, national standard organisations and at the international level. The proliferation of different proprietary standards has been seen as a threat to the growth of Electronic Data Interchange. A significant move towards the use of common international messaging standard in UN/EDIFACT.
ELECTRONIC TRANSACTIONS, § 5.2.

106 PETE LOSHIN, PAUL A. MURPHY, ELECTRONIC COMMERCE 250 (Jaico Publishing House, 1998).



Basic Steps of EDI

Source: Mohan Padmanabhan, Benefits of Speedy Implementation in Ports and Customs, Business Line, April 13, 1998 at 4.

Fig-29

The software which is connected to company's computer, puts the message in Electronic Data Interchange envelope. As the Value Added Network is connected with a modem,[107] so the message and envelope is uploaded to Value Added Network to send it to the trading partner. The

107 Modem is an instrument which called as modulator and demodulator. Its main function is to transform an analogue material into digital and vice versa.

corresponding Value Added Network of the trading partner will receive the message and with the help of the modem, it will reach the trading partner's computer where it will be integrated by translator software and the trading partner will have access of the message.[108] Electronic Data Interchange transaction requires strict compatibility between the data sent from buyer to seller and seller to buyer.[109] When establishing Electronic Data Interchange communications, network security is a key concern that companies need to take precaution to protect.[110]

II.4. MARKET APPLICATION OF ELECTRONIC DATA INTERCHANGE

The performance of electronic commerce is based on the harmonizing the network connectivity. One company's Unix

---

108 Supra note 106.

109 Supra note 95 at 51.

110 Within the Electronic Data Interchange messaging standard, UN/EDIFACT, each message contains an "Interchange Header Segment" which contains a sender identification field, a password field and control information. The control information is repeated in the "Interchange Trailer Segment" as a check. In addition, one of the most secure means of message authentication is with the help of cryptographic technique, which transforms plain text, by using complex algorithm, into "cipher text". This algorithm should be too complex to be able to discover and encryption key should be kept protected from unauthorised use. Commonly used encryption methods are symmetrical and asymmetrical. Symmetrical encryption method is using same secret key at both ends of communication link. In asymmetrical encryption, a matching pair of cryptographic keys are used, one for encryption and the other for decryption. The decryption key is kept secretly and other is made available to whom one wants to communicate.
ELECTRONIC TRANSACTIONS, § 5.2.

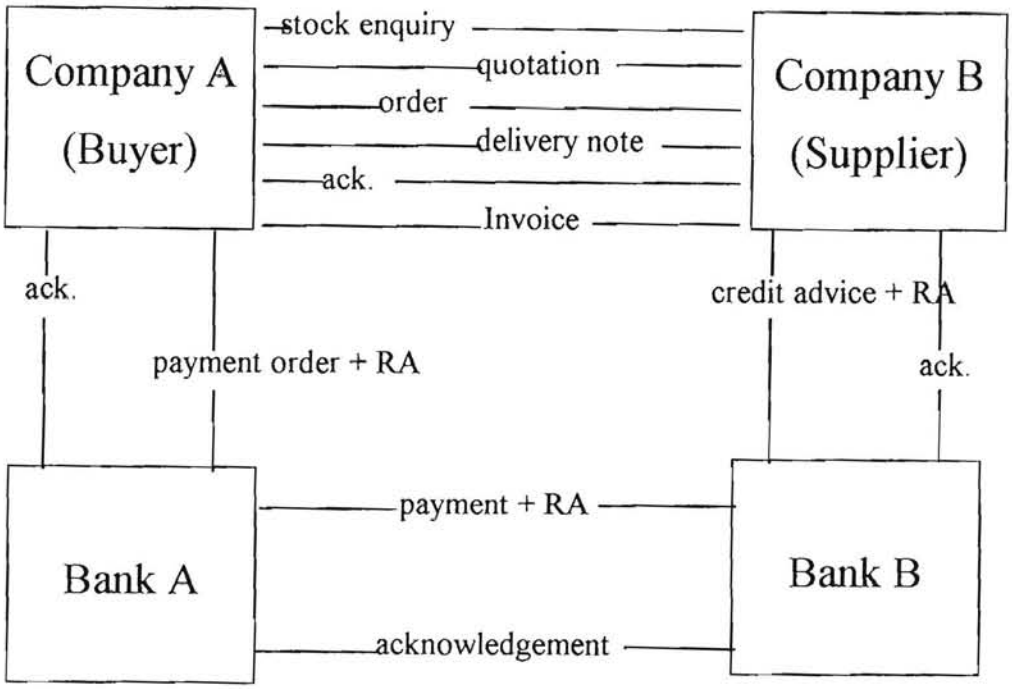
programmed computer has to communicate to the computer of the other company. Some companies prefer to use direct dial up link and some others prefer to route through Value Added Network. Because of these complexities, various industries have their own approach to Electronic Data Interchange.[111]

Initially, commercial Electronic Data Interchange users intended to focus on basic transaction documentation, such as invoices and purchase orders. Recently, companies have becoming increasingly interested in extending their Electronic Data Interchange implementation to a wider range of traditional commercial communication such as corporate payment messages (Fig-30).[112] Financial Electronic Data Interchange involves the bank offering a service enabling companies to complete the electronic trading communication loop, by sending payment information such as payment order and remittance advice information electronically.

---

111 Supra note 95 at 53.

112 There are currently estimated to be around 12000 companies using Electronic Data Interchange in the United States. In the U.K. there are some 6000 users, generating four million messages per month. It is also estimated that the user base growth of Electronic Data Interchange is about 30 per cent per annum in the U.K. while the message volume is growing at 100 per cent every year. Mandela Andrey, "*EDI Trends and Directions*" (Yankee Group Europe Seminar, April 6, 1992).



Commercial and Financial EDI

Source: Electronic Transaction, § 5.10.

Fig-30

The financial service industry uses Electronic Data Interchange in case of Electronic Fund Transfer. Although payment system is still based on cash or cheque, more and more financial service providers are moving towards Electronic Fund Transfer to control cost, reduce paper work, increase privacy and to improve cash management. Current Electronic Fund Transfer system is based on various networks.[113] Some banks are

---

113 Interbank transfer network is provided by the Society for World Wide Interbank Financial Telecommunications (SWIFT), payment network is

creating unique Electronic Data Interchange based system for their customers. Bank of America has created the Business connect service to give its business banking customers access to accounts with a personal computer to get account information, transfer fund and maximize cash flow.[114] The financial service provider's desire to give the service to the customers so that they can conduct financial transaction from their home and office with the help of computer network requires common language, electronic standard and connection protocol.

While large retailers, distributors and manufacturers have been using Electronic Data Interchange for years, the grocery products market, particularly time sensitive product areas have been slow to switch over to electronically managed transactions. But recently, many of these suppliers have realised that Electronic Data Interchange based information flow can be a powerful marketing tool.[115] The information that a particular item of product is selling better than other item, can help in advertisement campaign and can guide in product launching.

---

provided by Bankwire, settlement network is provided by Fedwire. Along with these, there is ATM network.
LEN KEELER, CYBER MARKETING 54 (American Management Association, 1995).

114 Supra note 95 at 54.

115 Supra note 95 at 55.

British Ports and Customs is accepting Electronic Data Interchange messages from shipping companies and importers to effect clearance of goods. In case of sea way bill, initial booking information is given to the carrier by the shipper's computer. The sea waybill is issued by the carrier's computer and need never take form of a piece of paper. Delivery instructions are given by the computer. In some trades a negotiable bill of lading must be issued. The speed and convenience of electronic communication have led to efforts to introduce systems for electronic production of negotiable bills.[116] The problem of authenticating Electronic Data Interchange bill of lading can be solved through digital cryptography.[117]

The shops that repair outdoor power equipment may seem to be unlikely group to be leaders in electronic commerce. New tools for

---

116 Among two systems - depository system and notification to carrier system, in the first case, paper bill is deposited with a third party who is then notified. Since the right to the possession of goods is changed by electronic transfer, he or she keeps a register of changes to which the carrier can refer to ensure that delivery is made to the correct party. The second system is entirely electronic and does not need existence of bill of lading. Using electronic message, the carrier issues an electronic bill to the shipper together with a private key, possession of which entitles the holder to control the goods. The right to control is passed after notification by the shipper to the carrier who cancels the original key and gives a new private key to the new person who is entitled to control the goods.
ELECTRONIC TRANSACTIONS, § 5.2.

117 DIANA FABER, SHIPPING DOCUMENTS AND EDI at 87-88, Computer and Law (Indira Carr, Katherine Williams eds., Intellect, Oxford, England, 1994).

electronic commerce may give new blood to the existing situation.[118] But recent tools are yet to gain popularity in the industry.[119] Apart from hesitation for technological upgradation, cost-benefit analysis of the dealers was also responsible for it, because dealers were not ready to purchase the system, unless it provides business management applications like accounting (Fig-31). The improved technology like POWERCOM-2000 have simplified the ordering process. Now dealers need not to search for right manual and right part for giving order. It requires a push to couple of buttons and then to click to send order automatically through Electronic Data Interchange.[120]

---

118 POWERCOM-2000 is a multi-application project which provides some best aspects of Electronic Data Interchange. It demonstrates how individual companies within an industry can work together, using technology to streamline the entire marketing process. It connects equipment manufacturer and distributors to the customer service departments of dealers. It enables service department to process orders efficiently. It handles everything electronically from preparing invoices and sales reports to provide catalogue of documentation stored on CD-ROM.
LEN KEELER, CYBER MARKETING 55 (American Management Association, 1995).

119 Although, Briggs and Stratton, American Yard Products, Atlas and Lawn Chief, etc., companies have opted for available Electronic Data Interchange tools, but according to a research in 1995, about 15 per cent of 26,000 power equipment dealers in America were computerised and only a fraction of those had CD-ROM drives or capability to connect to Electronic Data Interchange network.
LEN KEELER, CYBER MARKETING 55 (American Management Association, 1995).

120 Most importantly to send order through Electronic Data Interchange, costs ten cents, comparing to $2 in case of typical system of giving order.
LEN KEELER, CYBER MARKETING 56 (American Management Association, 1995).

Sub-categories	Concepts	Textiles	Chemical	Tobacco	Bank
Coercion	Threat of business	• Some small suppliers threatened by major customers	• EDI performance of trading partners determined continued business	• Grocery chains required EDI use	• Not observed
				• Suppliers forced to be EDI compatible by a cutoff date	
Support	Technical support	• Hardware, software, and VAN selection	• Hardware, software, and VAN selection	• Hardware, software and EDI Clearinghouse selection	• Advice on setting up EDI
		• Training	• Provided to small companies by trading partner	• Basic consultation	• Guidance and reference provided
			• Provided to cash management customers		
	Senior non-IS management support	• Senior marketing personnel	• Senior marketing personnel	• Senior personnel in accounting, purchasing	• Cash management personnel
	Incentives	Free, subsidized hardware/software	• Increased market share for EDI performance	Request letter detailing benefits of being EDI capable	• Benefits (cost reduction) through more efficient processing of payables of better cash management
Collaboration	Building long term relationships	• Evidence of mistrust in the area of inventory management	• Evidence of obligating long-term customers	• Conscious attempt to maintain relationship with small customers	• Conscious attempt to provide additional financial services
		• Simple contracts based on trust	• Storing inventory at the customer location		
			• EDI relationship with similar large customers		

Strategies for EDI use

Source: Connic W. Crook, Ram L. Kumar, Electronic Data Interchange: A Multi-Industry Investigation using Grounded Theory, Information and Management at 84 (34, 1998).

Fig-31

U.S. Government is aggressively moving away from paper to electronic transactions. The Internal Revenue Service has already accepted electronically delivered tax return. The Department of Treasury, Defence and Interior have a pilot Electronic Data Interchange purchasing programme.[121] Electronic Data Interchange has made it easier to do business with the government as it has removed the web of regulations and procedures. Government agencies can create a single Electronic Data Interchange format for registering vendors as government suppliers. A massive database can be formed to keep all information regarding all vendors.[122] The U.S. Postal Service which has suffered set back because of e-mail and fax, has adopted Electronic Data Interchange tool to regain its hold.[123] Tools like Secure Electronic Transaction, electronic public key which encrypt electronic document, digital signature which provides time, date and authenticity, will be very much helpful for this purpose. It is not just the corporate sector which needs well established Electronic Data Interchange tools but governmental

---

121 Supra note 95 at 56.

122 U.S. Department of Defence accounts for 14 million acquisition every year and it has taken a leading role in implementing Electronic Data Interchange and its goal is to conduct 80 per cent of its business transactions electronically by the end of this century.
LEN KEELER, CYBER MARKETING at 57 (American Management Association, 1995).

123 Supra note 95 at 57.

agencies of external trade such as Customs Departments and Ports also in desperate need of it.[124] In India while Electronic Data Interchange on a pilot basis has already made progress in Customs Houses and Head Quarter of Director-General of Foreign Trade but nothing has happened in the ports.[125] Various ministries are in the process of implementing National Information Infrastructure Plan.

II.5. ELECTRONIC DATA INTERCHANGE CONTRACT

a) Electronic Data Interchange program are used by business people who wants to deal often with each other electronically. Parties to an Electronic Data Interchange enter into an agreement which sets forth the condition under which both sides agree to deal electronically with each other in future.[126]

---

124 In a typical pilot study scheme say, for a port trust, a set of message exchanges between the Port and the container-handling companies concerning the arrival of the carrying vessel and containers to be discharged would include, a vessel arrival notice, the cargo manifest and container delivery confirmation.
Mohan Padmanabhan, *Benefits of Speedy Implementation in Ports and Customs*, BUSINESS LINE, April 13, 1998, at 4.

125 Mohan Padmanabhan, *Benefits of Speedy Implementation in Ports and Customs*, BUSINESS LINE, April 13, 1998, at 4.

126 An Electronic Data Interchange contract provides for the following -
- a) the purpose and subject of Electronic Data Interchange communication.
- b) the legal effect of Electronic Data Interchange transmission.
- c) the rights and obligations of both parties in connection with Electronic Data Interchange.
- d) the data protection afforded to Electronic Data Interchange communication.
- e) the confidentiality.
- f) the binding nature of electronic messages.

Considering standard agreements,[127] one gets impression that Electronic Data Interchange contracts an agreements in which two or more users in the switching role of senders and addressee, undertake to communicate by electronic means according to principles of Electronic Data Interchange.[128]

There are various types of contracts that are related to the use of Electronic Data Interchange.[129]

---

g) the applicable law and jurisdiction in case of dispute.
Dinesh Singh, *Electronic Commerce - Contractual Aspects* (1998) (unpublished project paper, National Law School of India University, Bangalore).

127 A Model EDI Contract has been attached as ANNEXURE-H.
- Standard Electronic Data Interchange Agreement of EDI Association.
- European Model EDI Agreement, Commission of European Communities Programme TEDIS.
- Dutch Ediforum Contract

SERGEJ H. KATUS, THREE TYPES OF EDI CONTRACT 29, *Computer and Law*, (Indira Carr, Katherine Williams, eds., Intellect, Oxford, England, 1994).

128 SERGEJ H. KATUS, THREE TYPES OF EDI CONTRACT 29, *Computer and Law* (Indira Carr, Katherine Williams, eds., Intellect, Oxford, England, 1994).

129

1. Interchange Agreement - between senders and users
2. Network Agreement - between users and networks
3. Third party Agreement - between users or network providers and third parties.

Interchange Agreement - This is the best known Electronic Data Interchange contracts. It governs the rights and obligations in relation to the way data are interchanged using electronic means. This agreement can be made either bilaterally or multilaterally. The primary intention of the parties to the agreement is the exchange of data according to the principles of Electronic Data Interchange.

In all three categories of contracts, it is obvious that the parties intend to do something with Electronic Data Interchange, either towards the process of communication or towards some kind of support. The Electronic Data Interchange contract is a legal document in which terms related to the use of Electronic Data Interchange can be found. In both Interchange and Network Agreement, rules are laid down for technical and legal matters with regard to the use of Electronic Data Interchange. In general Electronic Data Interchange contracts regulate various aspects of Electronic Data Interchange (Fig-32).[130]

Network Agreement	-	In this type of contract, the parties' intention is not to interchange data electronically. This agreement is regarding user's intention to get connection to a network to enable communication with other users. This agreement exists in different forms as users sometimes contract network provider directly and sometimes they enter a user group by consorting with the by-laws.
Third party Agreement	-	Third parties are those who are contracted by users and intermediaries to provide supporting service like software, hardware, maintenance service, security service. So the contract with third parties to provide supporting service are subcontract, arising out of other Electronic Data Interchange contracts.

SERGEJ H. KATUS, THREE TYPES OF EDI CONTRACT 29, *Computer and Law* (Indira Carr, Katherine Williams, eds., Intellect, Oxford, England, 1994).

130 Electronic Data Interchange contract regulates -
(a) That parties exchange Electronic Data Interchange message (Art.3 UNCID).

Regarding Interchange Agreement obligation, parties do not get responsibility regarding use of Electronic Data Interchange, automatically. These responsibilities are agreed upon by making contract. Interchange agreement is a contract between users and contains description of responsibilities of sender and addressee. It is important to recognise that the responsibilities in the use of Electronic Data Interchange are mainly relevant when users are actually dealing with message.[131] A sender has to transform data into an Electronic Data Interchange message, which means transforming the data into a message structured to agreed standard, in a computer readable format, capable of being automatically and unambiguously processed.[132]

(b) The agreement on the use of standard for data element, message structure, communication standard (Art.4, UNCID).
(c) That parties are capable to receive data transfers (Art.5, UNCID).
(d) That parties ensure the reliability of message by regulating integrity - message should be complete and correct, exclusivity - message can be secured against interference by unauthorised person, Verifiability - identification, verification, acknowledgement, confirmation of content and storage of data.
SERGEJ H. KATUS, THREE TYPES OF EDI CONTRACT 33, *Computer and Law* (Indira Carr, Katherine Williams eds., Intellect, Oxford, England, 1994).

131 From the sender's point of view, his responsibility is during preparing and transmitting of message and from addressee's point of view, his responsibility is during reception of processed data.
Paul J. Harts, Carol S. Saunders, *Emerging Electronic Partnership: Antecedents and Dimensions of EDI Use from the Supplier's Perspective*, JOURNAL OF MANAGEMENT INFORMATION SYSTEMS, at 35 (Spring 1998, Vol.14, No.4).

132 Article 1, Third definition, TEDIS Agreement.

Sub-categories	Concepts	Textiles	Chemical	Tobacco	Bank
Customer-initiated	Loss of market share	• Large retailers pressuring small companies	• Large industrial customers requesting increased sophistication of transactions (ASN)	• Retailers (grocery chains) requiring EDI	• Customer relationship loss to competitors
	Improved customer service	• Vendor managed replenishment (VMR)	• Warehousing of products for customers	• Automatic shipment notice (ASN)	• Better information on cash reserve and transactions
Organisation-initiated	Cost savings	• Inventory savings for retailers	• EDI sued with JIT	• Reduced paperwork and duplicate keying Inventory reduction	• Reduced paperwork and duplicate keying
Reaction to competition	Organisational level	• Other hosiery manufacturing EDI	• Market share based on EDI performance	• Forced to adopt by competitors	• Forced to adopt by competitors • New electronic banking products
	Industry level	• Establish quick response (QR) chain to compete with foreign competitors			• Discourage new entrants into the industry

Causal conditions for EDI use

Source: Connic W. Crook, Ram L. Kumar, Electronic Data Interchange: A Multi-Industry Investigation using Grounded Theory, INFORMATION AND MANAGEMENT at 81 (34, 1998).

Fig-32

If agreed, any measure to secure the message against the risk of unauthorised access by any person can be included. For evidential purpose, sender can keep a chronological record to store all Electronic Data Interchange messages. To establish authenticity of the message, the addressee has to convert, decode and verify it. Verification is also made by sending an acknowledgement to the sender.[133]

In case of Network agreement, when an original sender transmits a message, it is received by the intermediary and from that moment, the intermediary is responsible. The intermediary process the message as agreed and then forwards the message to the real addressee. Since intermediaries are neither the original sender nor the addressee, their responsibility is limited to the envelope of the message and thus they are not authorized to change the information it contains. When it is known that exchanged message may contain confidential data, an intermediary has to ensure that no unauthorised person have access to any transmitted Electronic Data Interchange message.[134]

For Third Party Agreement, users' and intermediaries' responsibility is to provide facility for the supporter to do their job.

---

133 Supra note 128 at 36.

134 Supra note 128 at 37.

So far as the contractual liability is concerned, every party has the obligation to perform according to their responsibilities within reasonable boundaries. In general situation, one is normally liable to the injured party. To determine lapse of contractual liability, two questions arise (1) whether the party perform insufficiently to fulfill his contractual obligation and (2) whether this non-performance cause damage to the other contracting party.[135]

In case of Interchange Agreement, the liability is imposed if a message lacks integrity and causes damage to the another user because of fault. In Network Agreement, the intermediaries will be liable for mistake in receiving and forwarding message. Since the intermediaries are experts in Electronic Data Interchange, so they have greater risk to be liable than users. In Third Party Agreement, which is a sub contract for performing contractual obligation by a third party, because of privity of contract, for any mistake of third party, causing loss to the users, the supporter becomes liable, because he cannot be relieved by delegating his responsibility.[136]

---

135 Supra note 97 at 38.

136 Supra note 97 at 39.

II.6. DISADVANTAGES OF CONVENTIONAL ELECTRONIC DATA INTERCHANGE

A trading partner can resist adoption of Electronic Data Interchange because of initial investment required or the effect that Electronic Data Interchange would have an well established procedures for exchanging information both between and within the organisation. Electronic Data Interchange applications require highly structured protocols and negotiated arrangements. Necessary agreements about the structure and meaning of data are time consuming to negotiate, inflexible and difficult to maintain in a dynamic environment.[137] For many users Electronic Data Interchange is not the ultimate solution because it involves some obvious deterrents as cost of setting up, sophistication required to set it up, lack of ability to do any spontaneous transaction and lack of connectivity of some customers.[138] Rigidity is another deterrent of conventional Electronic Data Interchange. Many company's business model call for increasing their customer and supplier bases. But setting up an Electronic Data Interchange link requires so much of time and money that it keeps the number of electronic partners in check. Conventional Electronic Data Interchange has shortcoming of

---

137 Supra note 97 at 90.

138 Pragya Bharati, *Can EDI provide solutions for E-Commerce*, EXPRESS COMPUTER at 11 (June 15, 1998).

painstakingly link their back office system to Electronic Data Interchange software and then synchronize protocols with their trading partners' system.[139]

II.7. INTERNET AND ELECTRONIC DATA INTERCHANGE

The conservative and conventional Electronic Data Interchange infrastructure is no match to the Internet.[140] Companies will try to conduct electronic commerce by experimenting with several combination of Electronic Data Interchange and the Internet. Trading partners can retain existing Electronic Data Interchange connections, find cheaper ways to send Electronic Data Interchange messages and use the web to reach out to new partners.[141]

---

139 Supra note 138.

140 The natural gas industry has been using traditional VAN based EDI since 1996. Recently, the Gas Industry Standard Board chartered a task force to study the use of the Internet as communication transport vehicle. But the question remains, (i) Whether public Internet or a private, industry based intranet will be used; (2) Which protocol should be used. The Internet based architecture requires both partner to have common infrastructure to support the common protocol, encryption and signature method and response transaction. The ongoing transaction cost in case of VAN based EDI can be replaced by one time development cost for Internet based EDI. Internet based EDI is cost effective alternative to VAN based EDI.
Daine Biegel, *EDI over the Internet: A Success Story from the Natural Gas Industry,* <http://www.ecresources.com/information/ jee/VIIn 4.5 html>.

141 Daine Biegel, *EDI over the Internet: A Success Story from the Natural Gas Industry,* <http://www.ecresources.com/information/ jee/VIIn 4.5 html>.

Electronic Data Interchange over the Internet can be faster than over Value Added Networks. To send Electronic Data Interchange messages through Value Added Network, these messages are stored in electronic mailbox until the next processing step, where as through Internet, the message will go immediately. Another vital benefit of conducting Electronic Data Interchange over Internet is that of attracting new partners to Electronic Data Interchange.[142] The better option for companies would be to use service which combines standard Electronic Data Interchange format with web based software. Companies can use their website to attract trading partners, exchange information and take orders, then they can link the website to back and order processing and financial system via Electronic Data Interchange. But the difficulty in using Internet is that the required software is proprietary. Trading partners need the same package at both end.[143]

Since an absolute requirement of any Electronic Data Interchange transaction is absolute security and guaranteed delivery of Electronic Data Interchange message, the Internet was not initially used as a part of Electronic Data Interchange process. However with the continued

---

142 Supra note 138.

143 Supra note 138.

development of Internet security protocols and systems capable of confirming e-mail messages, the Internet and Electronic Data Interchange will continue to overlap. This overlap is being fueled by new Internet based Electronic Data Interchange solutions.[144]

144 Premenos Corporation (http://www.premenos.com) has introduced several products that utilise the Internet to exchange Electronic Data Interchange messages.
PETE LOSHIN, PAUL A. MURPHY, ELECTRONIC COMMERCE, at 251 (Jaico Publishing House, 1998).

Chapter III: Digital Money: the New Concept of a New Age

III.1. What is Digital Cash

III.2. Digital Money Transaction

III.3. Smart Cards

III.4. Digital Payment System in Practice

III.5. Implication of Digital Cash

CHAPTER III

DIGITAL MONEY: THE NEW CONCEPT OF A NEW AGE

Change has taken place in the land of global finance with the help of rapid technological advances. The application of computer, telecommunication and software technology has enabled the birth of a whole new financial product and services. One of the methods of payment over Internet is digital cash[145] or electronic cash or electronic money, which is an example of such newly conceived product. Digital money is an electronic replacement for cash.[146]

---

145 The value in the form of suitably validated and protected binary digits, can be stored in computer. The stored value requires a standard scheme for encoding it in binary digits and an issuer. The concept is that the digits, representing value, would be loaded into the user's PC or chip storage by the issuer and user's conventional account with the issuer would be debited. The payment acceptor would receive digits corresponding to the value of the transaction. Digital cash consists of message that use a sophisticated version of public-key, private key encryption. It is stored on a computer's hard disk and is electronically transferred to payee. It may be electronically replenished by transfer from one's account at a participating bank. A digital cash system employs software held by the participating financial institutions, their customers and merchants. Using that software customer creates digital message that are authenticated by the issuing institution in a way that third party can recognise. The issuer's authenticated message is returned to the customer and acts as a substitute for cash. A merchant that receives the digital cash can send it as to its bank and have its account credited or it can spend the digital cash.
Banks Get the Green Light to Hit the Internet, BANK NETWORK NEWS, July 12, 1995.

146 History of currency provides that currency began in a primitive barter economy which is driven by the interest of the individual. The inconveniences caused by the barter system mooted for standardised medium of exchange. In

III.1. WHAT IS DIGITAL CASH

Digital cash or electronic money is units or tokens of monetary value that take digital form and are transmitted over electronic network. Digital Value Units are the basic units of denomination of electronic money which may or may not corresponds to units of national currency. The move to store value electronically is to substitute the traditional medium of exchange. This concept replaces paper, either cash or cheque, with digital signature that take on the same function.

The concept of digital cash has earned few question marks against it.[147] Digital money has no intrinsic value and the barest trace of physical existence. But it is potentially a perfect medium of exchange because it can transfer financial claims at incredible speed and it can create instant settlement of transactions (Fig-33).

---

modern societies, gold remained the generalised medium of exchange for centuries. Since gold is heavy to carry, gold coins gradually gave way to paper currency. Two main functions of currency are medium of exchange and store of value. National currency has got status of legal tender which, according to law, cannot be refused as settlement for debt. People are happy to leave their money in the bank as they are confident that they can get legal tender on demand.
DANIEL C LYNCH, LESLIE LUNDQUIST, DIGITAL MONEY, 99-101 (John Wiley and Sons Co. 1996).

147 Theses questions are not new. They were asked when first coins were struck, when first paper currency was circulated and when first credit cards were offered. Theses questions are quite obviously regarding intrinsic value of digital cash.
DANIEL C LYNCH, LESLIE LUNDQUIST, DIGITAL MONEY, 99 (John Wiley and Sons Co. 1996).

© Cyber Cash **Payment Cards**
• Approaching 10,000 merchants on-line • By end '98, there was 60,000-80,000 merchants active on the Internet • Moving from 100,000's to 1,000,000's of transactions per day • Dominant form of payment - Credit Cards • SET standard looming, but most transactions secured only by SSL

Fig-33

To create confidence, like that of cash, every unit of digital money must be guaranteed to convertible into legal tender on demand which requires to keep a unit of cash reserved in real economy, against every unit of digital money.[148] Because of its unique nature, digital money has raised some doubts.[149] Lynch and Lundquist, has identified that an ideal digital money system should have some general principles.[150]

---

148 DANIEL C LYNCH, LESLIE LUNDQUIST, DIGITAL MONEY, 101 (John Wiley and Sons Co. 1996).

149 If one unit of digital money represents an immobilised unit of money, then positive balance of digital money will earn no interest and so people will keep less amount of their asset as digital money. There will be no virtual lending in digital money system. This will undermine convertibility. As banks could not create new money by lending in the digital world, so they might see digital money as unproductive and they might charge a fee to convert money or take agency fee for issuing it.
DANIEL C LYNCH, LESLIE LUNDQUIST, DIGITAL MONEY, 101-103 (John Wiley and Sons Co. 1996).

150 (a) Independence - The security of digital money must not depend on its existence in any singular physical location.
(b) Security - Digital money must not be reusable. So it must not be possible to use digital money at a time in two different places.
(c) Privacy - Digital money must protect the privacy of its users.

III.2. DIGITAL MONEY TRANSACTION

In a typical digital money transaction, where A wants to send B some digital money, following steps are observed -

(i) A uses his computer to generate a random number worth $10 and he generates 10 digit number to represent $10.

(ii) A encodes the 10 digit number using his secret key.

(iii) A transmits this encoded number to his bank along with digital signature.[151]

(iv) The bank uses A's public key to decode the number and the signature, thus verifying that message is indeed from A.

(d) Off line payment - Digital money should be independent of the means of transporting it. So merchants who accept digital money must not depend on a connection to a network so that transaction can be made.
(e) Transferability - Digital money must be transferable to others.
(f) Divisibility - Digital money must be divisible into smaller amounts and again they must total up when recombined.
DANIEL C LYNCH, LESLIE LUNDQUIST, DIGITAL MONEY, 99-101 (John Wiley and Sons Co. 1996).

151 Digital money is possible because of cryptographic technology called digital signature. In fact, digital money is one of the most interesting application of digital signature technology. Digital signatures were first proposed by Whitfield Diffie of Stanford University in 1977. It is a code that allows absolute authentication of the origin and integrity of a document, cheque or electronic cash that has been sent over a computer network. A digital signature guarantees that any one who reads a digitally signed message, can be certain of who sent it. Digital signature uses a pair of keys - a private key, to sign a message and a public key, to unlock it. Only a message signed with a private key can be decoded and verified, using the public key.
DANIEL C LYNCH, LESLIE LUNDQUIST, DIGITAL MONEY 111 (John Wiley and Sons Co. 1996).

(v) Seeing that A has specified an amount of $10, the bank debits A's account for $10.

(vi) The bank signs A's number with its private key.

(vii) The bank sends the digitally signed number back to A.

(viii) Then A sends the number to B.

(ix) B verifies the bank's digital signature on A's number.

(x) B sends the number to his bank.

(xi) B's bank uses key of A's bank to re-verify A's number.

(xii) B's bank checks A's number against a list of already spend numbers.

(xiii) B's bank credits B's account for $10.

(xiv) B's bank adds A's number to the already spend list.

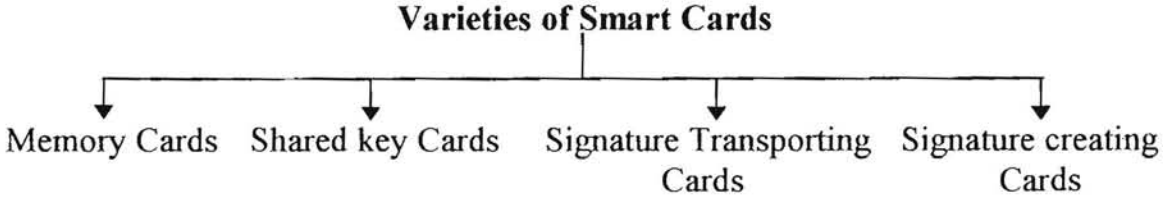
(xv) B's bank sends B a digitally signed deposit slip for $10.

III.3. SMART CARDS

Smart Cards are wallet size cards, much like credit cards, that contain stored value. Smart Cards are plastic 'credit' cards with an embedded microchip. They can be loaded with currency from an Automated Teller Machine or card reader or personal computer. The currency then can be spent at businesses, vending machines that have been equipped with appropriate devices. Smart Card is simply a debit

card that does not require bank approval for each transaction. Smart Cards are cards containing stored value on chip. Shops ranging from supermarkets to movie theatres to the local news stand could be equipped to receive, store and re-transmit the digital money from customers. Furthermore, many forms of public services, including pay phones, subways, buses, taxis, parking motors, tool booths and vending machines could also be equipped.[152]

Four basic types of micro circuit cards exist for use as smart cards.



Memory cards are the simplest of smart cards. They have data storage space and require a password for access.[153]

---

152 N. Richard Werthamers, Susan U. Raymond, *Technology and Finance: The Electronic Market*, TECHNOLOGICAL FORECASTING AND SOCIAL CHANGE, at 47 (No.55, 1997).

153 Shared-key cards store a secret key and can communicate with other cards that share this key. These cards require validation of the secret key at the point of sale which means there must be a relatively sophisticated piece of equipment at the point of sale.
DANIEL C LYNCH, LESLIE LUNDQUIST, DIGITAL MONEY, 116-117 (John Wiley and Sons Co. 1996).

Signature-creating cards contain a delicate co-processor which makes them capable of generating large random numbers. They are most complex cards and correspondingly most expensive card to produce.[154]

III.4. DIGITAL PAYMENT SYSTEM IN PRACTICE

Digital payment systems focus on getting a payment form a customer to a merchant. The emphasis is on the customer, so customer needs to acquire and install some software or make some kind of contact with the digital payment system provider in order to register as a user of that service.

Cyber Cash[155] (www.cybercash.com) provides digital payment system which uses straight forward interpretation of digital commerce,

---

154 Signature-transporting cards contain ready-made supply of blank cheques which are large pregenerated random numbers that can be assigned a denomination and signed to use as digital money. Since blank cheque smart cards are loaded in advance and cheques need not be re-verified, signature-transporting cards do not require point of sale validation. Therefore, not only the cards are reasonably priced, the point of sale system can be simpler and less costly.
DANIEL C LYNCH, LESLIE LUNDQUIST, DIGITAL MONEY, 116-117 (John Wiley and Sons Co. 1996).

155 Cyber Cash Inc. was founded in 1994. Its goal was to provide an accessible and acceptable payment system for the Internet. It offers safe, efficient and inexpensive delivery of payment between customers, merchants and banks, across the Internet. It makes available the software and services needed to exchange payments. Cyber Cash gives consumers a digital wallet. Customers are able to authorise payments out of their digital wallet.
PETE LOSHIN, PAUL A. MURPHY, ELECTRONIC COMMERCE 170 (Jaico Publishing House, 1998).

basing its service on the need for secure, private, reliable transactions. It offers a digital payment mechanism that uses modern cryptographic technologies, including public and private key encryption and digital signatures, implemented through special client and server software.[156]

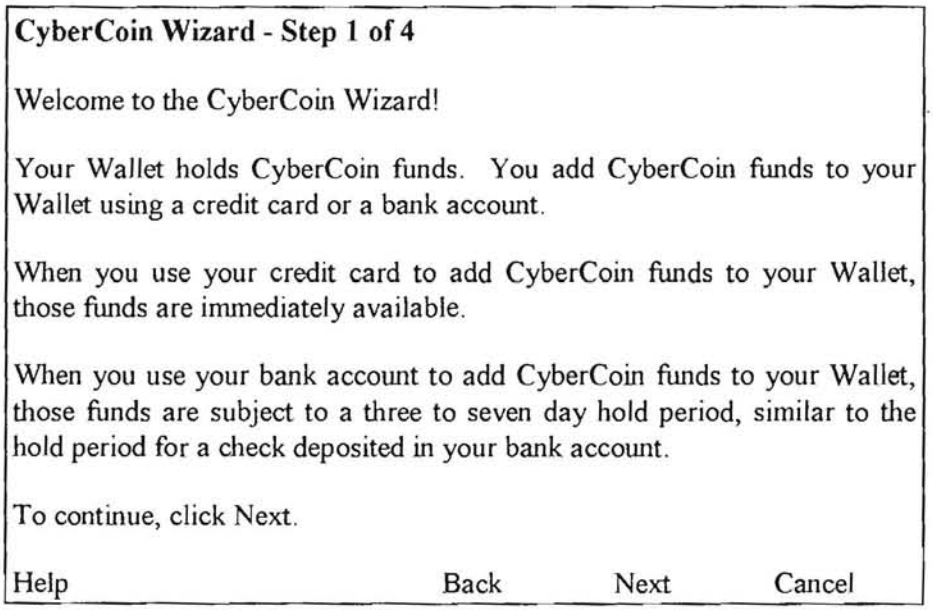


Fig-34

When the customer completes a purchase and begins a Cyber Cash transaction by clicking on the Cyber Cash Pay button of a merchant's World Wide Web site, the merchant receives information about the customer's order, as well as encrypted message from customer's Cyber Cash client (Fig-34). The encrypted data includes the customer's payment information (Fig-35).

---

156 Supra note 106 at 140.

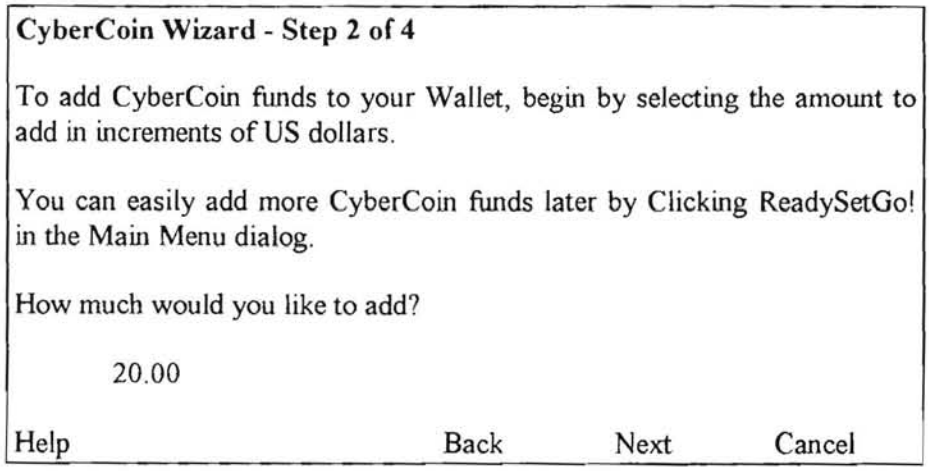


Fig-35

With Cyber Cash credit card transaction,[157] Cyber cash decrypt the message, forwards it to the merchant's designated bank or credit card processor. The bank or processor responds to Cyber Cash and Cyber Cash forwards the approval or refusal to the merchant's server. Once approval is received by the merchant's server, it notifies the customer (Fig-36).

---

157 The merchant's Cyber Cash software verifies that neither the order nor the encrypted payment information has been modified during the transmission and then forwards the encrypted message to Cyber Cash. Once Cyber Cash receives the encrypted payment message and verifies that no modifications have been made to it in transmit, Cyber Cash determines whether the transaction is a Cyber-Cash credit card based transaction or Cyber Coin transaction.
PETE LOSHIN, PAUL A. MURPHY, ELECTRONIC COMMERCE 140 (Jaico Publishing House, 1998).

Transactions - STLMURPHY57-03

History		Pending
Date and Time	Description	
02/06/1997-11:37:16	Wallet Registered	
02/06/1997-11:44:24	User Notification	
02/06/1997-11:44:24	Credit Card Added to Wallet	4237000000000000
02/06/1997-11:44:42	Credit Card Added to Wallet	4237000000000000
02/06/1997-11:49:04	Money Moved to Wallet	
02/06/1997-12:11:16	User Notification	
02/06/1997-12:11:16	CyberCoin Service Payment	EarthlyGoods-44
02/06/1997-16:12:47	Reconcile Wallet Balances	

Detail...

Help Close

Fig-36

With Cyber coin, electronic wallet essentially holds digital money and banks having the account can be requested to transfer dollars to Cyber Coin wallet. As some Cyber Coin transactions are made, money is pulled out from wallet and sent to Cyber Coin merchant's wallet (Fig-37).[158]

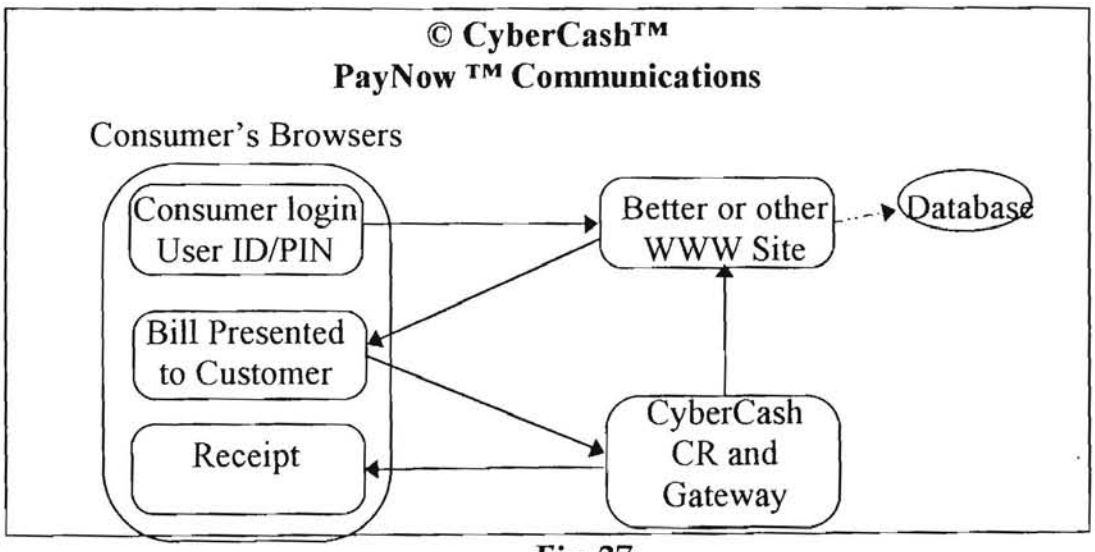


Fig-37

158 Supra note 106 at 171.

With the use of digital signature and encryption, Cyber Cash is able to keep transmissions secure for all purposes. Cyber Cash offers significant advantages to both the customer and the merchant.[159]

First Virtual is another company offering Cyber Cash services on the Internet.[160]

---

159 (a) It keeps payment information private, even from the merchant.
(b) It offers a convenient electronic wallet to store payment information, so that the information need not be reentered every time a purchase is made.
(c) It maintains a transaction log to handle, track and document every transaction.
(d) There is no extra charge for using Cyber Cash.
(e) It is a convenience for customers, who may prefer not to reenter credit card number on the Internet.
(f) It offers merchants useful tools for tracking and transacting business on the Internet.
(g) It is supported by banks and credit card companies.
PETE LOSHIN, PAUL A. MURPHY, ELECTRONIC COMMERCE 190 (Jaico Publishing House, 1998).

160 It is required that the buyer must complete an on-line application which does not call for the credit card number. For security reasons, the credit card number is transmitted by telephone and is then checked by bank. Upon satisfactory check of the credit card, buyer receives, an account identifier or PIN code. If the buyer comes across something that looks interesting on the Internet, he requests the merchandise to be shipped against providing his PIN code to the seller. The seller verifies the validity of the PIN, makes delivery. First Virtual before charging buyer's credit card account, sends him e-mail message asking if purchase was satisfactory. If the buyer replies in positive, credit card is charged and the money is transferred to the order. If the buyer replies in negative, no transfer occurs.
Dinesh Singh, *Electronic Commerce - Contractual Aspects* 13 (1998) (unpublished Master in Business Laws Project Paper, National Law School of India University, Bangalore).

III.5. IMPLICATION OF DIGITAL CASH

The introduction of digital cash system has implications on both legal and non legal side. Regarding its implication the question which comes first is about the institution which will issue electronic money. The issuer would need the status and credibility to make its electronic money widely accepted. Today's banks would qualify as they are within central and state infrastructure of banking laws and regulatory oversight. But non-banking institutions can also become issuer of charge cards like AT and T, General Electric, DigiCash, Cyber Cash, etc.[161]

Electronic cash and increasing importance of digital markets pose problems for central government's control over the economy.[162] Transfer of large sums of cash across border would be untraceable. There would be no audit trail. Digital counterfeits could work for any where in the world and spend currency in any and all places. New financial crimes

---

161 Supra note 152 at 47.

162 As transfer of Digital Value Unit across national border do not amount to official foreign exchange transaction, so national currencies may loose relevancy with the development of Digital Value Unit that have a universally accepted denomination. The widespread use of electronic cash will render national economic data much less meaningful. Both electronic commerce and electronic cash raise fundamental question about national market.
Stephen J. Kobrin, *Electronic Cash and the End of National Markets*, FOREIGN POLICY at 72 (Summer, 1997).

and forms of fraud could arise that would be hard to detect and it would be extremely difficult to locate perpetrator.[163]

Electronic commerce does not occur in any physical location but instead, it takes place in cyberspace.[164]

Internet commerce and digital money create the potential for better world by providing convenient shopping method. By promoting better communication and simplifying the logistics of life, the new era of Internet commerce offers us much more time for relaxation and enjoyment. There also exist possibility for misunderstanding, misdirection and misuse.[165] A digital world economy demands increasing international cooperation, harmonising of national regulations and legislations and strengthening the authority of international institutions.[166]

---

163 Stephen J. Kobrin, *Electronic Cash and the End of National Markets*, FOREIGN POLICY at 72 (Summer, 1997).

164 In digital economy, it would be difficult to link income stream with specific geographic locations. Electronic cash in manifestation of global economy and the problem electronic cash poses for governance results from the trend of disconnecting electronic market from political geography.
DANIEL C LYNCH, LESLIE LUNDQUIST, DIGITAL MONEY, 74 (John Wiley and Sons Co. 1996).

165 Supra note 148 at 245.

166 Supra note 148 at 76.

Chapter IV: Encryption - Saviour of Electronic Commerce?

IV.1. What is Encryption?

IV.2. Advantages of Encryption

IV.3. Kinds of Encryption

IV.4. Breaking of Encryption

IV.5. Key Management

IV.6. Encryption Standard

IV.7. Liability

IV.8. Government Regulation

IV.9. International Scenario

IV.10. Scenario in India

CHAPTER IV

ENCRYPTION - SAVIOUR OF ELECTRONIC COMMERCE?

Electronic commerce as a mass phenomenon is the certain outcome of the successful diffusion of Internet based services in recent years. But there are some doubts darkening the golden glow which lie in the security issues at the core of electronic commerce.[167] The growth of electronic commerce via the Internet depends on the security and privacy of transactions. Only if the buyers and sellers trust that orders and payments are conducted with minimal risk of deceit and abuse of information, they will accept Internet for electronic commerce purposes. If users fear that these orders may be changed on the way, their credit card numbers may be stolen and misused, their private information may be misdirected, they will revert back to the traditional instruments.

Paper records and files also threaten personal privacy or reveal other confidential and sensitive information. So in earlier days important and confidential files were kept under lock and key and access to these was restricted to maintain security. During the long history of paper-based "information system" for commerce and communication, a number of safeguards were developed to ensure the confidentiality; that is secrecy

---

167 James P. Backhouse, *Security: The Achilles Heel of Electronic Commerce*, SOCIETY, May-June, 1998, at 28.

of contents, integrity; that is without unauthorised changes, authenticity; that is coming from the stated sources. These traditional safeguards include secret code books and passwords, physical seals to authenticate signatures and auditable book keeping procedures.[168]

Computer-induced data is easily transportable, easier to copy and easier to manipulate and so in this era, controlling access has become much more difficult. With the emergence and growth of Internet, on-line banking, electronic commerce and other forms of network computing have come into existence and have changed the whole scenario. With the introduction of electronic commerce, lot of personal information like credit card number, transaction data, preference about choice of product, medical and insurance records, personal files will be available while travelling through Internet. Government, corporations and organisations are worried that hackers will manage to come in touch with these information and will engage in fraudulent activities and manipulation of records. This situation leads to some issues genetic to all electronic communications.[169]

---

168 *Information Security and Privacy in Network Environments*, Office of Technology Assessment, Congress of the U.S., 1994 at 112.

169 Issues are like, how to ensure the integrity of the message, how to authenticate the sender, how to ensure non-repudiation of receipt.
WTO Secretariat, Special Studies 2, *Electronic Commerce and the Role of the WTO*, 1998 at 38.

Modern cryptography[170] offers solution to the problems of an open network. The whole point of cryptography is to keep information out of the hands of anyone but its intended recipient. Even if the message gets intercepted, the meaning will not be apparent to the interceptor.[171] As a concept, cryptography is not a new thing to introduce as its use can be found in the history.[172]

IV.1. WHAT IS ENCRYPTION?

Encryption is basically a process in which a message is transformed from plain text to cipher text, by using a mathematical function. This

---

170 Cryptography is the technology to encode (encrypt) and decode (decrypt) information to prevent its being read by unauthorised party. It is the art and science of secret writing. Cryptography protects data against unauthorised disclosure. It can authenticate the identity of a user and it can disclose unauthorised tampering.
Cyber law series, Department of Electronics website,
URL: <http://www.doe.gov.in>.

171 Supra note 101 at 41-43.

172 Cryptographic use can be traced back to several thousand years back in Egyptian Hieroglyphics and in ancient India where it was used for communication with spies. The recorded history of cryptography is more than 4000 years old. Manual encryption method using code books, letter and number substitution and transpositions have been used for the hundreds of years - for example, the Library of Congress has letters from Thomas Jefferson to James Madison containing encrypted passages. Modern computer-based cryptography and cryptanalysis began in the World War II era, with the successful allied computational effort to break the ciphers generated by the German Enigma machines.
Information Security and Privacy in Network Environment, Office of Technology Assessment, Congress of the U.S. 1994 at 112.
James P. Backhouse, *Security: The Achilles Heel of Electronic Commerce,* SOCIETY, May-June, 1998 at 30.

process is a complicated version of coding[173] and decoding method. Cipher[174] and Key[175] are two main elements of encryption technology. Current encryption technology generates cipher text via computer hardware and software enjoying sophisticated mathematical formulae.

IV.2. ADVANTAGES OF ENCRYPTION

Since Internet is a distributed network and it is open to the public, so messages are exposed to the risk of intercepting. Encryption is used so

---

173 Code is a method of interchanging vocabularies so that each code word represents some other non-code word. Codes requires a special code book which acts like dictionary. If the code book is lost, encoded text cannot be interpreted.
PETE LOSHIN, PAUL MURPHY, ELECTRONIC COMMERCE, 44 (Jaico Publishing House, 1998).

174 Ciphers are the basis of encryption schemes. It acts on each character of a message, transforming it according to some algorithm. The encryption algorithm is the function with some mathematical foundations which performs the task of encrypting and decrypting the data.
PETE LOSHIN, PAUL MURPHY, ELECTRONIC COMMERCE, 44 (Jaico Publishing House, 1998).

175 Keys are special numbers which help to initialize the algorithm. Different keys used with same algorithm will produce different versions of encrypted text. The quality of security is dependent on the size of the key. Encryption keys are used by the encryption algorithm to determine how data is encrypted or decrypted. Encryption keys are similar to computer password. When a piece of information is encrypted, one needs to specify the correct key to access it again. But unlike a password programme, an encryption programme does not compare the key one provides with the key one originally used to encrypt the file and grant access if the two keys match. Instead, an encryption programme uses key to transform the cipher text back into the plain text. If one provides the correct key, one gets back his original message. If one tries to decrypt a file with a wrong key, one gets irrelevant and unreadable message.
PETE LOSHIN, PAUL MURPHY, ELECTRONIC COMMERCE, 44 (Jaico Publishing House, 1998).

that no one except the intended recipient can open the message. So encryption is the most practical and safest way to protect secret information. Encryption has various role to play.[176] Encryption can be used to create digital signatures.[177] Digital signatures are used to

---

176 a) Encryption can protect information stored on the computer from unauthorised access, even from people who have otherwise access to the computer.
b) Encryption can protect information while it is in transit from one computer system to another.
c) Encryption can be used to deter and detect accidental or intentional alteration in the data.
d) Encryption can be used to verify author of a document.
Cyber law Series, Department of Electorates Website,
URL: <http://www.doe.gov.in>.

177 Digital signatures provide a higher degree of authentication by allowing resolution of dispute. Although it is possible to generate digital signatures from symmetric cipher but most interest centers on system based on asymmetric cipher, known as public-key crypto-system. These asymmetric ciphers use a pair of keys, one to encrypt and another to decrypt, in contrast to symmetric ciphers in which the same key is used for both the operations. Each user has a unique pair of keys, one of which is kept private and the other is made public. The security of public-key system rests on the authenticity of the public key and the secrecy of the private key. In principle, to sign a message using a public key encryption system, a user can transform it with his private key and send both the original message and the transformed versions to the intended receiver. The receiver can validate the message by acting on the transformed message with the sender's public key and the result should match exactly with the original message. As because the signing operation depends on the sender's private key, so it is impossible for anyone else to sign message in sender's name. But everyone can validate such signed message, since the validation depends on the sender's public key. In practice, digital signatures sign shorter "message digest" rather than the whole message. For digital signatures based on public-key systems, sender first uses a cryptographic "hashing" algorithm to create a condensed "message digest" from the message. With the commercial Riveat-Shamir-Adleman (RSA) system, the signature is created by encrypting the message digest using the sender's private key. As because in the RSA system, each key is the inverse of the other, the recipient can use the sender's public key to decrypt the signature and recover the original message digest. The recipient compares with the one

authenticate message.[178] It also supports non repudiation.[179] Another use of encryption is to create digital certificate.[180] Application of

---

he or she has calculated using the same hashing function, if they are identical, then the message has been received exactly as sent and furthermore, the message did come from the supposed sender.
Information Security and Privacy in Network, Office of Technology Assessment, Congress of The U.S., 1994, at 124-125.

178 Message authentication techniques based on cryptography can be used to ensure the integrity of the message (that it has been received exactly as it was sent) and the authenticity of its origin (that it comes from the stated source). The oldest and simplest form of message authentication use "secret" authentication parameters known only to the sender and intended recipient to generate "message authentication codes". So long the secret authentication parameters is kept secret from all other parties, these techniques protect the sender and receiver from alteration or forgery of a message by all such third parties. As because the same secret information is used by the sender to generate the message authentication code and the receiver to validate it, these techniques cannot settle "dispute" between the sender and receiver as to what message was sent.
Information Security and Privacy in Network, Office of Technology Assessment, Congress of The U.S., 1994, at 124.

179 It is a legal term which means that sender of a message with digital signature cannot later deny having created the message and repudiate any terms or agreements contained in the message. Normal electronic mail is deniable, since it is relatively easily forged and easily modified. Electronic mail that has been digitally signed, is non repudiable.

180 A digital certificate is like a digital ID card. It proves that one is who he claims to be and contains the digital signature of a Trusted Third Tarty to back up his claim. Digital certificate and digital signature play an important part in secure credit card transactions on the Net. Most digital certificates used in Internet credit card transactions come from a company called Verisign (www.verisign.com). A merchant requesting a Verisign certificate must prove its identity and pay $300.
VINCE EMERY, HOW TO GROW YOUR BUSINESS ON THE INTERNET 197 (Coriolis Group Books, 1996).
The digital certificates which are currently in circulation, come with sweeping disclaimer of liability. Both the 40 and 128 bit Netscape SSL encryption that are used for secure web connections rely in part on digital signature to identify the server and the browser to each other. No one actually guarantees the server's public key. All that the user gets is the practical assurance that if the response back is the same each time one longs on, it is unlikely that he is communicating

cryptography have evolved along with cryptographic techniques. Cryptography was originally used to protect the confidentiality of communications, encryption is now also used to protect the confidentiality of information stored in electronic form and to protect the integrity and authenticity of both transmitted and stored information.[181] With the advent of public key technique,[182] cryptography came into use for digital signature which is used as a means of or electronically authenticating and signing commercial transactions like purchase orders, tax returns and fund transfer, as well as ensuring that unauthorised changes are detected.[183]

---

with importer. But no body is accepting liability for the user who is being misled. The same situation applies with other current Internet based certificates, including the "authenticode" certificates used to identify the authors of Java Active X programs.
Steward A. Baker, *International Developments Affecting Digital Signatures*, October 1997,
URL: <http://www.steptoe.com/webdoc.nst/law+&+The+Net-All/All>.

181 The necessity for authentication can be realised from the following illustration -
- A and B are two acquaintances who communicate by e-mail on occasion.
- C, impersonating A, sends a forged piece of e-mail to B, requesting a secure communication channel using public key encryption.
- C's public key was included in this forged message.
- B receives the message and encrypts a reply using what he believes as A's public key but which is actually C's public key.
- C receives the message, decrypts it with his private key and is able to communicate with B while pretending as A.

182 For further discussion, see §IV.3.

183 Supra note 168 at 113.

IV.3. KINDS OF ENCRYPTION

To ensure the privacy of message, encryption can be offered in two different forms, private key and public key. Private or symmetric key encryption is based on a key being shared between two parties. The same key both encrypts and decrypts the message (Fig-38). Data Encryption Standard (DES) follows the private key encryption technology.[184]

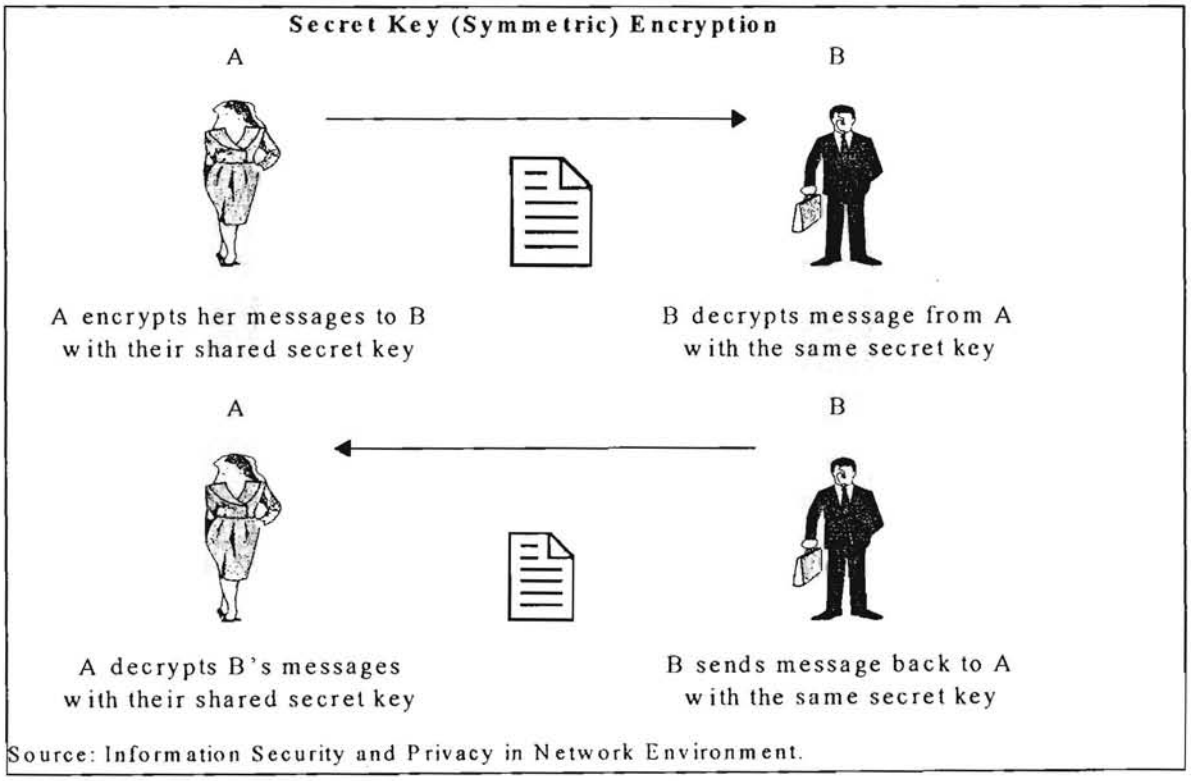


Fig-38

---

184 *Cyberlaw Series, Department of Electronics Website,* URL: <http://www.doe.gov.in>.

Here both the sending and receiving parties must know the secret key that they will use to communicate. A private key mechanism is relatively simple method of encryption. The main problem is in sharing the key, that is, how to transmit the key used for security over an unsecured network. The secret key becomes difficult to manage because it requires courier, registered mail or other secure means for distributing the key. The difficulties involved in generating, storing, transmitting keys can limit private key system over Internet.[185]

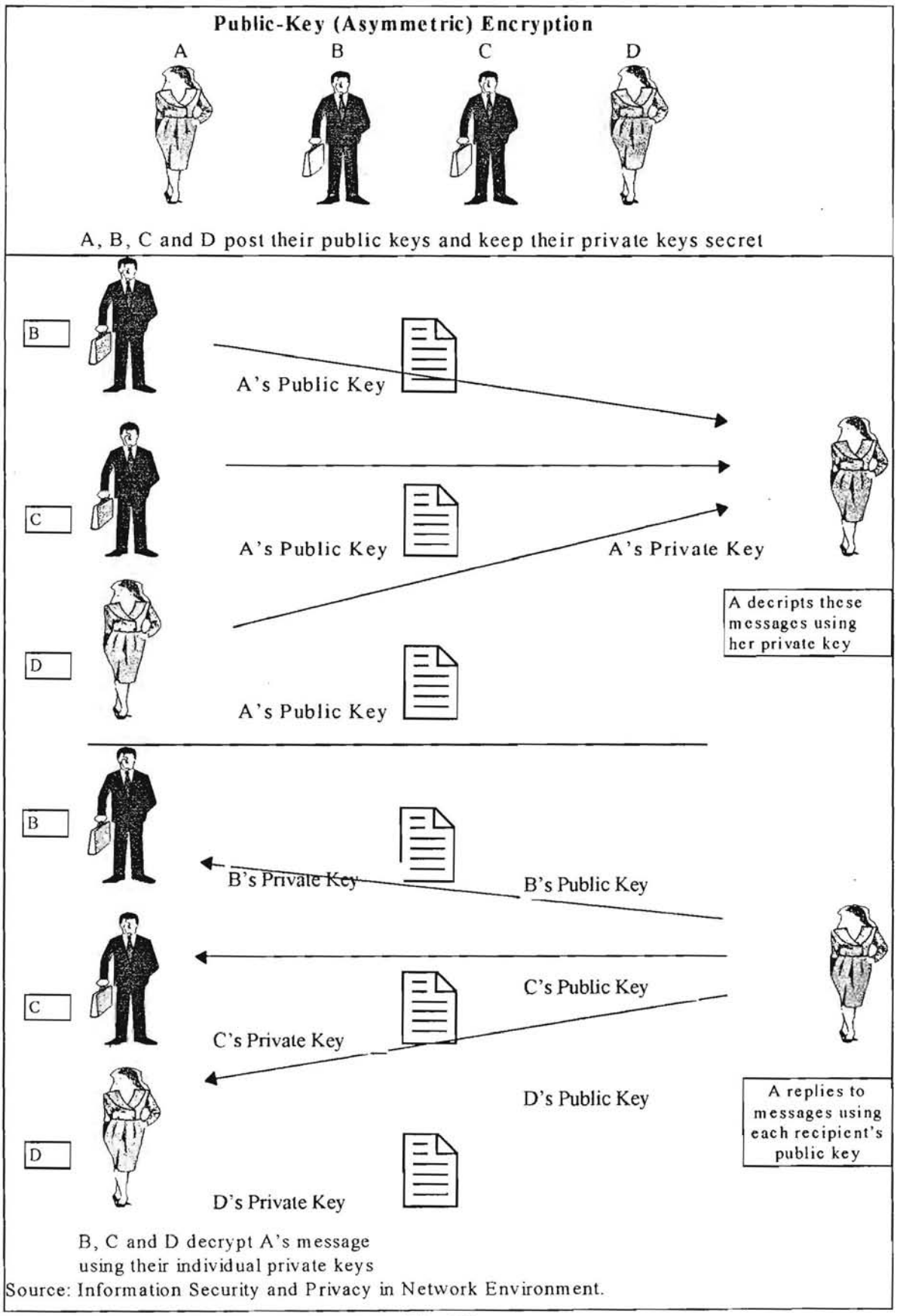
In a public key encryption[186] there are two keys - a private key and a public key. Private key is to encrypt a message and it is kept in secret. Public key is to decrypt a message and it is made public. This system is also known as Asymmetric crypto-system (Fig.39).[187]

---

185 Supra note 168 at 39.

186 In 1976, two computer scientists, Whitfield Diffic and Martin Hellman, developed a theory of public-key encryption that offered a solution to the problem of transferring private key. Later, RSA Data Security Inc., created an algorithm to make public key cryptography commercially viable.
VINCE EMERY, HOW TO GROW YOUR BUSINESS ON THE INTERNET at 197 (Coriolis Group Books, 1996).

187 Supra note 184.



Source: Information Security and Privacy in Network Environment.

Fig-39

The initiator needs to protect the confidentiality and integrity of his or her private key and the other key can be distributed more freely. These keys are mathematically related. The name comes from the fact that the encryption key can be made public without compromising the secrecy of the message.[188] The main advantage offered by public key encryption is increased security. Although slower than private key system, public key encryption generally is more suitable for electronic commerce.[189]

The third type of encryption is called Hybrid crypto-system, which is also known as one-time symmetric key system or one-way hash algorithm. One-time symmetric key is generated for each transaction. The sender first encrypts the message by using one-time symmetric key. This key is then encrypted, using recipient's public key. Thus it can be decrypted only with recipient's private key and it is now safe for transmission over Internet. When the message arrives, the recipient decrypts the one-time symmetric key, with his or her own private key

---

188 Supra note 168 at 39.

189 a) It is more sealable to very large systems.
b) It has a more flexible means of authentication.
c) It can support digital signature.
d) It enables non-repudiation.
Information Security and Privacy in Network, Office of Technology Assessment, Congress of The U.S., 1994, at 39.

and then by using the symmetric key, the recipient decrypts the message.[190]

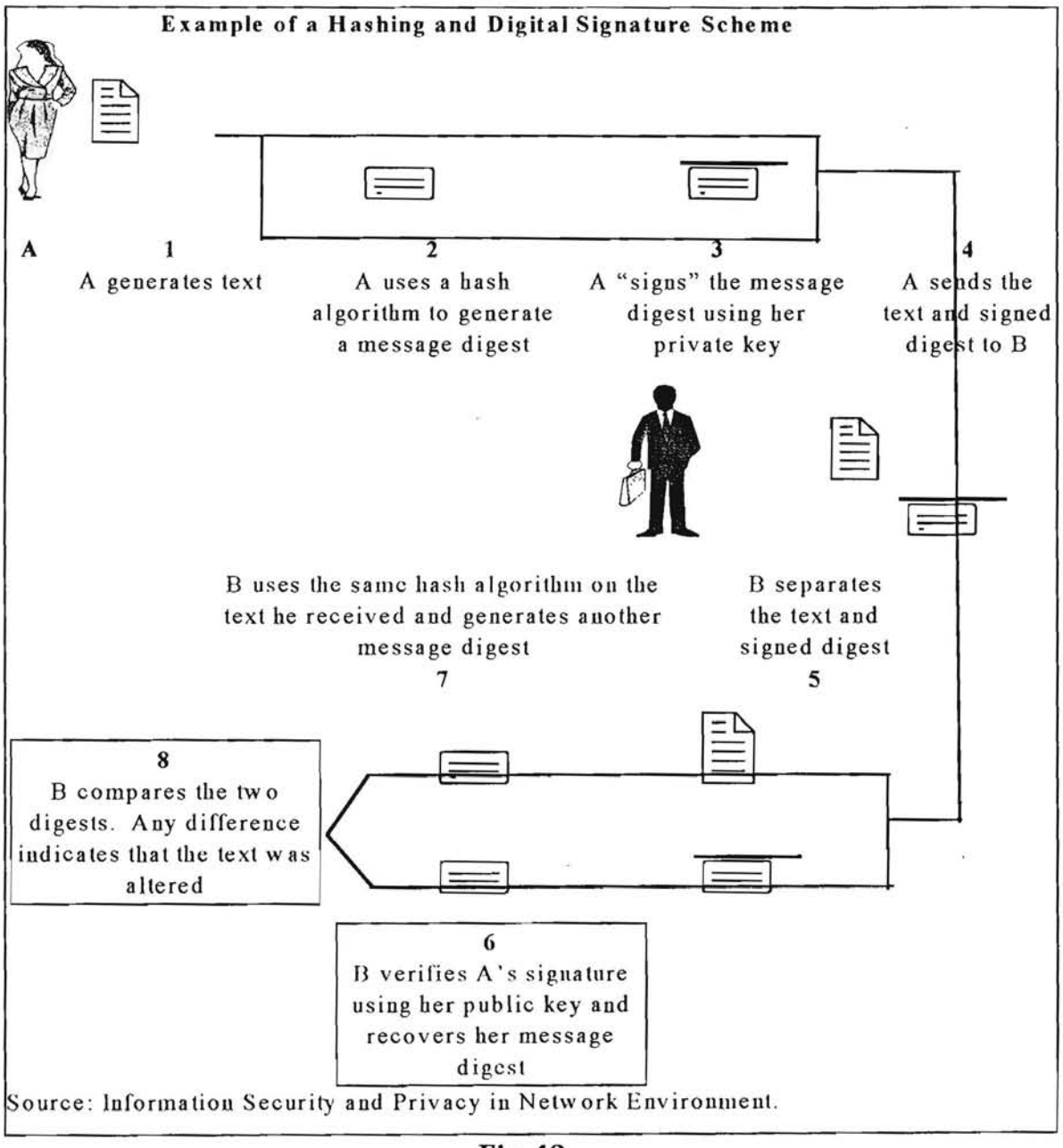


Fig-40

190 Supra note 184.

The message is processed with hashing algorithm which produces a shorter message digest. As the hashing method is one-way, so the message digest can not be reversed to obtain the message. The message and message digest is sent. The recipient processes the message with hashing algorithm and compares the message digest with message digest which came along with message. If the message was altered in any way during the transit, the message digests will be different which reveals the alteration (Fig-40).[191]

IV.4. BREAKING OF ENCRYPTION

Encryption scheme is vulnerable on several fronts. Encrypted text can be analysed for word and character frequencies to find out what the encryption algorithm is. Cryptographers accept that all ciphers are vulnerable to brute force attack. Security depends on the cipher key size.[192] A researcher at Lucent Technologies Inc., has discovered a

---

191 Supra note 168 at 39.

192 A cipher key can be compared with a combination lock. If one has the correct key, he or she can unlock the message. The three digit combination lock often found in luggage offer minimum protection, as there are only 1000 different options. Sometimes right combination can be hit after few attempts. Generally after trying half of the total possibilities, lock can be broke open. If per combination takes one second, then brief-case can be opened in eight minutes or at the most in seventeen minutes. Adding another digit to the lock increases the number of possible combination by a factor of ten, doubling the number of digits to six, increases the number of possible combination to one million. A brute-force attack at a six digit combination takes almost six to eleven days. If two more digits are added, it will take over a year and a half to break in.

software flaw that could allow a well-equipped computer hacker to break the encryption software code used for electronic commerce.[193]

IV.5. KEY MANAGEMENT

If there is the relevant key, the message can be read. One major weakness of the process is that, there has to be a dependable way to pass keys around to the people who need it. Key is to treated with same care which is given to the message. Losing a message is harmful but losing key means losing all messages. To send a secure message to a group, either to rely on every one involved, keeping a single key for all of them or to assign a separate key to each individual. On line commerce requires that message is to be exchanged securely with any one. Key solutions are available but by and large they require some degree of trust either in the parties exchanging the message or in some intermediary agency with access to both parties' secret key.[194]

One major problem with public key encryption is, that whether one correspondent has the right key for the other correspondent. If two individuals have secure channel over which they can pass a key, for

---

PETE LOSHIN, PAUL MURPHY, ELECTRONIC COMMERCE, 45 (Jaico Publishing House, 1998).

193 Reuters, *E-commerce open to hackers, finds study*, THE ECONOMIC TIMES, Bangalore, June 17, 1998 at 8.

194 Supra note 101 at 47.

example, by sealing a piece of paper or diskette in an envelope and sending it through mail, then they can communicate in confidence. But if they want to rely on electronic media, there is no such secure channel. No one can trust an e-mail message containing public key because the message itself can come from an eavesdropper. The problem arises when two people who do not previously know each other, wish to communicate. The solution may be possible through Trusted Third Party.[195] The Certification Authority can also solve the problem.[196]

Under Key Escrow, a copy of decryption key for each user is placed in a secure location of one or more trusted parties and is made available if warrant is issued for it. The concept of key splitting is used for escrowing

---

195 Trusted Third Party may be the solution that allows an initial contact to be made. If two correspondents are known by any intermediary and both entrust it with their public keys then each can obtain other's public key from this intermediary and start communication. For worldwide communication, the Trusted Third Party will probably be a large organisation with same public visibility, quality control, sense of responsibility as a bank.
MICHAEL CHISSICK AND ALISTAIR KELMAN, ELECTRONIC COMMERCE: LAW AND PRACTICE, 135 (Sweet and Maxwell, London, 1999).

196 A bank may wish to issue digital signature to its best commercial customers to represent that the customer maintained a substantial credit balance in its account over the last year. If a customer wants to do business on-line with another person, customer sends order to that person, signed with his bank issued digital signature. The person who receives the order, gets the reliable proof of the identity of the customer, on the basis of which, he can decide whether to do business with the customer. These type of banks are special kind of Trusted Third Party and are called Certification Authority. It should have license to show that it is conforming the procedural and technical standard.
MICHAEL CHISSICK AND ALISTAIR KELMAN, ELECTRONIC COMMERCE: LAW AND PRACTICE, 135 (Sweet and Maxwell, London, 1999).

of keys. Under this, key is splitted into several parts using appropriate algorithms and each part so splitted is deposited with several trusted parties. For decryption, all the splitted parts are to be combined.[197] Companies are likely to demand, as part of their employment term, that any employee has to place in escrow with the company, any private encryption key he may use in personal correspondence, as there would be a risk that an employee could pass confidential information and trade secrets to rivals secure in the knowledge that encryptography would hide the infamy from the employer.[198]

If any person uses cryptography confidential communication, he or she will be required to hand over his or her private key as receipt of a judicial warrant or a warrant issued by Secretary of State. Most customers will not generate their own encryption key but will obtain them from a special type of Trusted Third Party called Key Recovery Agent.[199] A major reason why Key Escrow schemes are necessary in the

---

197 Supra note 184.

198 MICHAEL CHISSICK AND ALISTAIR KELMAN, ELECTRONIC COMMERCE: LAW AND PRACTICE, 135 (Sweet and Maxwell, London, 1999).

199 Key Recovery Agent will keep in escrow a copy of the customer's private key. He will be required to hand over a copy of it's customer's private encryption key within one hour of the receipt of judicial warrant or a warrant issued by Secretary of State.
MICHAEL CHISSICK AND ALISTAIR KELMAN, ELECTRONIC COMMERCE: LAW AND PRACTICE, 136 (Sweet and Maxwell, London, 1999).

commercial world is recovery of information, when a private key has been lost, stolen or hidden.

IV.6. ENCRYPTION STANDARD

One of the most widely used encryption system is Data Encryption System (DES).[200] Automatic Teller Machine network uses DES to encrypt Consumer's Personal Identification Number when they are transmitted through shared network. DES can be implemented efficiently for bulk encryption like that required by electronic commerce applications.

IV.7. LIABILITY

When a digital signature is incorporated in a document, it signs every single part of it and links the authority of the signer with every single comma and colon. Digital signature, unlike a physical signature does not come from a human hand but from an artifact. Unauthorised

---

200 DES was invented by IBM in 1970s. It was endorsed by US Government and was adopted as American National Standard. It is basically a bit permutation, substitution and recombination function performed on block of 64 bits of data and 56 bits of key. The 64 bits of input are permitted initially and then input to a function using static tables of permutation and substitution. The bits are permuted in combination with 48 bits of the key in each round. This process is interacted 16 times, each time with a different set of tables and different bits from the key. The algorithm then performs a final permutation and 64 bits of output are provided.
Cyber law series, Department of Electronics website,
URL: <http://www.doe.gov.in>.

access to this artifact can lead to the production of signed contractual document and payment order which are the same as the genuine articles. The obvious way of controlling such abuse is to make the holder of the digital signature liable for all signatures generated by the artifact unless and until the key holder has revoked the digital signature's authority with Certifying Authority.[201]

IV.8. GOVERNMENT REGULATION

The main problems regarding regulation of cryptography is balancing between privacy and free trade on one hand and national security and law enforcement on the other. Many governments are concerned about widespread use of cryptography, thinking that strong encryption is used by criminals and terrorists and encryption interferes with law enforcement and intelligence gathering.

The U.K. Government in 1996 announced its support for key escrow in the form of a system of Trusted Third Party. This was aimed at protecting commercial sector, giving authorities some ability to obtain decryption where deemed necessary.[202] In 1998, through a White Paper,

---

201 Supra note 193 at 137.

202 URL: http://www.coi.gov.uk/coi/depts/GTI/coi9303b.ok.

Government proposed a new legislative framework for strategic export control and export licensing with particular emphasis on export of military equipment and technology.[203]

The Wassenaar Agreement[204] controls the export of cryptography as a dual-use good, that is, one that has both military and civilian application. According to it, software containing cryptography may be subject to control but it provides exemption from export control for mass market software.

In United States, prior to 1997, jurisdiction over export of encryption software was split between State Department and Commerce Department. But from 1997, it came completely under control of Commerce Department without liberalizing the level of control.[205] The

---

203 Supra note 193 at 133.

204 Coordinating Committee on Multilateral Export Control was replaced by Wassenaar Agreement in 1994 which has been signed up by Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Luxembourg, Netherlands, New Zealand, Norway, Poland, Portugal, Republic of Korea, Romania, Russian Federation, Slovac Republic, Spain, Sweden, Switzerland, Turkey, Ukraine, United Kingdom, United States.

205 "... because of the increasingly widespread use of encryption products for legitimate protection of privacy of data and communications in non-military contexts, because of the importance to US economic interest of the market for encryption products and because [the new commerce controls] can be accomplished without compromising US foreign policy objectives and national security interests."
White House Memorandum, *Encryption Export Policy*, 15 November, 1996.

new rule make it a condition of obtaining export approval of strong encryption products.[206]

IV.9. INTERNATIONAL SCENARIO

Group of 7 countries have jointly identified that data security and privacy are one of the key principle, on which Global Information Infrastructure must be built.[207] The Organisation for Economic Cooperation and Development (OECD) has adopted a set of guidelines for cryptography policy.[208]

---

206 Under the new regulation, low level encryption products - those with an algorithm with a key length of 40 bits or less - are eligible for export after one time review by commerce. Export of Recoverable products (Key escrow products) at any encryption item containing 56 bit key length data encryption standard may be eligible if it provides commerce, a business and marketing plan to develop, produce or market encryption item with recoverable feature. Foreign-origin encryption item can be imported freely to United States.
Jeffrey L. Synder, U.S. Export Control on Encryption Software, *The Journal of World Intellectual Property*, No.1, 1998, pp.37-44.

207 The paper proposed by G-7 countries suggests -
a) That government, industry and users must agree on the cryptographic technique to be used in the Global Information Infrastructure.
b) That agreed technique must be made public.
c) That agreed technique must be based on private-sector led, voluntary, consensus, international standard.
d) That product implementing agreed technique should not be subject to import control and restriction.
e) That product implementing agreed technique should be exportable to all countries.
Cyber law series, Department of Electronics website,
URL: <http://www.doe.gov.in>.

208 a) Cryptographic method should be trustworthy.
b) Users should have right to choose cryptographic method.
c) Market-driven development of cryptographic method.

Chapter V: Legal Issues in Electronic Commerce

CHAPTER V

LEGAL ISSUES IN ELECTRONIC COMMERCE

Laws develop in response to society's needs. They evolve in the context of the culture, business practices and contemporary technologies. The law currently governing commercial transactions was largely developed at a time when telegraphs and typewriters were commonly used office technologies and business was conducted with paper documents and by mail. Technologies and business practices have dramatically changed but the law has been slower to adopt.[210] Computers, electronic networks and information systems are now used commonly to process business transactions, store and transmit digital data in the commercial field. As the speed of use of information technology in the business world has quickened, the failure of current laws both substantive and procedural to meet the needs of trade, commerce and industry has become apparent.[211]

Electronic commerce has opened a new way of doing business. A variety of new challenges have come up for those who use Internet for

---

210 Information Security And Privacy In Network Environment, Office of Technology Assessment, Congress of the U.S. 1994, p.69.

211 Id.

business purposes. A new stream of law - Cyberlaw has emerged. Activities in cyberspace have influenced almost all branches of law, like Commercial law, Banking law, Intellectual Property law, Evidence law and others. Unique situations has been created due to tremendous growth of Internet use. While legal system of different countries are grappling with the question of developing Cyberlaw by applying existing law with the need arose out of technological growth or through innovations designed to meet the novel challenges posed by the Internet, time alone can tell whether the progress will be adequate to meet the evolving business needs of the global community.[212]

V.1. WEBVERTISEMENT

Trade or business begins with marketing or advertisement. It is same in the case of electronic commerce. Here it is called webvertisement. More and more companies are advertising on the Net, as it provides global audience at a low cost.

Advertising on the world wide web has received a real break through with phenomenal growth of Internet users. Business have different opportunities in on-line advertisement.[213] Theoretically,

---

212 P.P. Kanthan, *Challenges to Transacting Business on the Net*, BUSINESS LINE, August 4, 1998.

213 On-line publication, banner advertising, website advertising incorporating advertiser's brand name, linking a website with an e-mail, spamming.

webvert is subject to laws of every country in which it is accessed by Internet users but the problem arises when electronic commerce system apply national framework of law to something which is disseminated to the world at large.

In U.K., webvertiser have to comply with number of legislations.[214] Jurisdiction is the most important matter in webvertising. The initial question that is raised is whether the content of a website is subject to law of the country of origin of advertisement or is it subject to every foreign law where advertisement is capable of being accessed and downloaded. Generally laws of the country of "publication" will apply. Technically, advertisement should not violate the law of the country where it is published. But in the context of Internet, the publication is made to the entire world without any control.[215] If an advertisement is not intended to generate business in particular country, then a statement to that effect should be included in the advertisement. When advertisement of some

---

214 Trade Description Act 1968, Consumer Protection Act 1987, Control of Misleading Advertisements Regulations 1988, Prices Act 1974, Unsolicited Goods and Services Act 1971, Trade Marks Act 1994, Copyright, Designs and Patents Act 1988, Data Protection Act 1984, Defamation Act 1952 and 1996, Obscene Publications Acts 1959 and 1964, Lotteries and Amusements Act 1976.

215 When a US securities firm offered its financial service through website, U.K. Regulatory Authority served a notice to the U.S. securities firm for offering financial service in U.K. without license.
LILIAN EDWARDS & CHARLOTTE WAELDE, LAW AND THE INTERNET, 48 (HART Publishing, Oxford, 1997).

product or service is illegal in certain jurisdiction, like gambling or pornography, an appropriate notice or disclaimer should be included on the website.[216]

Unauthorised hyperlink to web was held to constitute breach of copyright, trademark and business reputation.[217] There being no consensus among countries regarding regulations on webvertisement and as there is no case law in this direction, an international convention in this regard, protecting interest of the majority is desirable.

V.2. WEBVERTISEMENT: OFFER OR INVITATION TO OFFER

Generally speaking websites advertise products and services but sometimes it assists supplier to complete the sale. Websites can be

---

216 Sec. 292(2) - Indian Penal Code, 1860 - Whoever, sells, lets to hire, distributes, publicly exhibits or in any manner puts into circulation or for the purpose of sale, hire, distribution, public exhibition or circulation, makes, produces or has in his possession any obscene book, pamphlet, paper, drawing, painting, representation or figure or any other obscene object whatsoever, or import, export or conveys any obscene object for any of the purposes aforesaid or knowing or having reason to believe that such object will be sold, let to hire, distributed or publicly exhibited or in any manner put into circulation... shall be punished.....
Council Recommendation on the Protection of Minors and Human Dignity in Audio-visual and Information Service had aim to provide guidance on issues like parental control and development of self regulation. European Council adopted in 1998.
Tobacco Advertising Directive proposed a ban on all forms of advertising and sponsorship. Directive 98/43.

217 Shetland Times Limited v. Wills (1997) F.S.R. 604.
Ticket Master v. Microsoft (1997) U.S. Case No.97.

designed to advertise the features of a product and to allow a viewer to examine the product in a restricted form.[218]

The display of articles with price in a shop window is an "invitation to treat" and when customer approaches the shop, it is an offer to buy. The shop has option to accept it and complete the contract or to return it. Website is electronic equivalent to shop window. Websites can have disclaimer that it is an offer to treat and not an offer by itself, so that electronic commerce business can select the customer and manage the supply of goods.[219] Electronic commerce is based on highly automation of process. Now the question which is to be addressed is whether a computer can accept an offer and make the contract! Generally, action of a machine is attributed to the person who instruct it to execute a particular routine work.[220] In State Farm Mutual Auto. Ins.

---

218 Software can be downloaded from a website in a crippled form, like a word processor, but may be prevented from printing or saving. It provides a test drive. If the user is happy with the product, he may re-access the website to form a contract and receive the uncrippling key.

219 Supra Note 198 at 8.

220 In Thornton v. Shoe Lane Parking Ltd. [(1971) 1 All E.R. 686], Court held that customer contracted with a car park machine, when he fed his money and received a claim ticket. "The customer was committed at the very moment when he put his money into the machine. The contract was concluded at that time. It can be translated into offer and acceptance in this way: the offer is made when the proprietor of the machine holds it out as being ready to receive the money. The acceptance takes place when the customer puts his money into plot."

Co. v. Brockhurst,[221] court held that since the computer only operated as programmed by the insurance company, it was bound by the contract. So Websites can be regarded an agent of the on-line business and can make both offers and accept offer to create a contract.[222]

Generally contracts are bilateral where both the parties are bound. In on-line contract also merchant promises to send the goods and in exchange, the consumer promises to pay. Sometimes on-line advertisement can create unilateral contract where only advertiser is bound.[223] On-line advertisement has to be carefully drafted so that consumers interpret them as advertisement or invitation to offer but not an offer or unilateral contract. Theoretically, on-line contracts should be subjected to only specified terms. But Court in J. Evans & Son (Portsmouth) Ltd. v. Andrea Merzario Ltd.,[224] ruled that on-line statements made by e-mail or on web pages prior to contract formation may be interpreted as express contractual terms, despite their absence from the actual contract written or otherwise.[225] On-line merchants do

221 453 F 2d. 53 (10th Cir. 1972).

222 Supra note 193 at 70.

223 See 12, Restatement of Contract (1932).

224 (1976) 1 W.L.R. 1078 at 1083.

225 "The court is entitled to look at and should look at all the evidences from start to finish in order to see what the bargain was that was struck between the parties."

not want to sell goods or services to every one - there may be trade restrictions and embargoes, there may be prohibition to sell certain goods to minors.[226] But the problem is for electronic commerce organisation to know whether the other party has authority to buy or transact? Digital signature, smart card can provide solution for this. Any lapse in these regards may compell electronic commerce organisation to face some legal hazards.[227] On-line merchants should regulate access to their sites and excludes users from unwarranted jurisdiction.[228]

The owner of the website can state that it will not be bound by any communication from the viewer but the site owner will inform him if it

---

J. Evans & Sons (Portsmouth) Ltd. v. Andrea Merzario Ltd. (1976) 1 W.L.R. 1078 at 1083.

226 Many products like encryption software are subject to export restriction. U.S. Department of Agriculture regulates import of fruits and vegetables. Some businessmen like to avoid some countries to deal with because of poor public relation. On-line business sometimes want to avoid some countries because of their consumer protection law is unfavourable to foreign merchants. Some on-line activities like financial service, gambling, pornography which may be legal in some places and illegal in some other places.

227 A number of Minnesota residents accused the Website advertising a forthcoming international gambling site. Minnesota court held that Granite Gate Resorts purposefully availed themselves of privilege of conducting commercial activities in Minnesota. v. Granite Gate Resorts, 568 N.W. 2d 715.

228 Electronic Commerce organisers can do server check for preliminary verification. Although it is not foolproof as customer's country of origin can only be marked. Site disclaimer can exclude unwarranted jurisdiction as it expressly mentions that it is intended for whom.
MICHAEL CHISSICK AND ALISTAIR KELMAN, ELECTRONIC COMMERCE, LAW AND PRACTICE, 62 (Sweet and Maxwell, London, 1999).

accepts the communication. This creates two factors in favour of website owner. First, it prevents any reasonable person from thinking that owner has made an offer. Second, it provides evidence that the site owner did not intend to make offer.[229]

V.3. OFFER

Formation of contract requires offer, acceptance, consideration and intention to create legal relation. Offer can be made using any medium post, tax, telex, telephone, electronic mail and World Wide Web.

V.4. AT WHAT POINT OF TIME AN OFFER IS MADE

A contract can only be formed by accepting an offer. An offer can be revoked at any time before acceptance. The issue to be discussed is when is at what point of time an offer is made. Sometimes, offer gets delayed in course of transmission, so it is very important to decide at what point of time an offer is made. Court has a choice that either offer may be deemed to be made at the time of sending or at the time of receipt. In Adams v. Lindsell,[230] court held that delayed offer is valid. Despite the technology, e-mails can get delayed.[231] Further technological

---

229 CLIVE GRINGRAS, THE LAWS OF THE INTERNET, 15 (Butterworths, London, 1997).

230 (1818)1 B & A 681.

231 E-mail is not instantaneous. An e-mail message is sent to a Service Provide who tries to deliver it as quickly and as accurately as possible. E-mails can arrive inconsistent, late or even not arrive at all. E-mails are passed between

advancement can come for help sometimes.[232] Offer through e-mail can be made subject to a date on which the offer will lapse. Court can assume time of offer at the time it should have arrived or a reasonable period after that.

V.5. ACCEPTANCE

Acceptance must unequivocally express assent to all the terms of the offer.[233] Acceptance can be made via any communication method. Generally it should be sufficient to receive the offer by same means by which it was originally communicated. Offer can even be accepted by "click-wrap".[234] On-line supplies can accept by sending the ordered goods, by transmitting data.

---

many carriers to arrive at the final destination. Some e-mails are delivered to an electronic pigeon hole, called 'in-box' for collection. Many users of e-mail must dial their Service Provider to check about the arrival *of e-mail. Often* users must collect e-mail, it is not delivered to them. On arrival, recipient must act to retrieve e-mail. E-mails can be lost, delayed by server or router without any fault of sender.
CLIVE GRINGRAS, THE LAWS OF THE INTERNET, 18 (Butterworths, London, 1997).

232 In some e-mail system, on arrival of e-mail, 'read' and 'receive' receipt is sent to sender, where 'receive' receipt indicates e-mail has not been received by the addressee, rather it has been received by the service provider and 'read' receipt indicates that it has been received by the addressee.
CLIVE GRINGRAS, THE LAWS OF THE INTERNET, 18 (Butterworths, London, 1997).

233 So in case e-mail, "read" or "receive" receipt will not constitute acceptance of an e-mailed offer.

234 A 'click-wrap' is where the contract is presented in a window on-line and the customer is asked to click an "offer" or "I accept" button. U.S. District Court

V.6. TIMING OF ACCEPTANCE

Acceptance of valid offer results in valid contract. Depending upon the context, like *inter praesentis* (when the contracting parties are face to face with each other) or *inter absentes* (when the contracting parties are not face to face each other), communication of acceptance becomes very significant.[235] In electronic commerce, generally acceptance is made by e-mail or by pressing the "Accept" or "Buy" buttons. Here the question that would arise is: when has the acceptance been conveyed.

- when the e-mail was sent or
- when it was received by the addressee or
- when it reaches the 'host computer' which provides the e-mail facility to the addressee.

When acceptance is made over the Internet by clicking "Accept" or "Buy" button, the question - where did the offeror actually receive acceptance? still remains open. Would the acceptance be deemed to have been communicated at the place where the offeree clicks the button or

---

held it enforceable in Hot mail Corporation v. Van Money Pic Inc. et al, C98-20064 (N.D. Cal., April 20, 1998).

235 Vaibhav Parikh, *Legal Issues in Electronic commerce with Special Reference to India*, 6 (A paper presented in Electronic commerce Seminar, organised by Confederation of Indian Industries; February 19-20, 1998).

would it be deemed to have been communicated where the server is located or would it be the place where the offeror actually reads the acceptance on his computer.

The instant of acceptance is the instant of contract creation. In Byrne v. Van Tienhoven[236] court used the Postal Rule (Expedition Theory) which was initiated in Adams v. Lindsell.[237] The Court has used the Receipt Rule (Information Theory) in case where both the parties have continuous communication, for example, over telephone and in these cases contract is created when the offeror hears the acceptance. This rule has been used in case of telex.[238]

Even as an offer has to be communicated, acceptance also should be communicated.[239] When by agreement, course of conduct, usage of

---

236 "It may be taken as settled that, where an offer is made and accepted by letters sent through the post, the contract is completed the moment the letter accepting the offer is posted, even though it never reaches the destination. Byrne v. Van Tienhoven, (1880) 5 C.P.D. 344 at 348.

237 (1818) 1 B & A 681.

238 Entores Ltd. v. Miles Far East (1955) 2 QB 327. This ruling was confirmed in Brinkibon v. Stahag Stahl. und. Stahlwar en handels gese llschaft mbH (1983) 2 A.C. 34 where it was decided that if both parties are in continuous communication during acceptance, then burden of notification falls on accepting party as he has immediate feedback regarding transmission. If it is faulty, he can resend the message.

239 Sec.4 - Indian Contract Act, 1872 - The communication of a proposal is complete when it comes to the knowledge of the person to whom it is made. The communication of an acceptance is complete as against the proposer, when it is put in a course of transmission to him so as to be out of the power of the

trade, acceptance by post or telegram is authorised, the bargain is struck and the contract is completed as soon as the acceptance is put into the course of communication by the offeree by posting a letter or sending a telegram.[240]

Where a contract is made through the telephone, the place where the acceptance of the offer is communicated is the place where the contract is made.[241] Strictly speaking, a consensus does arise, the moment an acceptor decides to accept but law cannot take note of the status of mind as such, unless as expressed. So it is necessary that this fact of acceptance should come to the knowledge of the offeror. Such communication is for the benefit of the offeror, it is open to him to waive the communication or to prescribe some act instead which if complied with would be sufficient to give rise to a contract. On this principle, where an offeror asks the acceptor to send his reply by post, it has been held that it is sufficient if the acceptor posts his letter and the contract would be concluded as from that moment.[242] This is so irrespective of whether letter of acceptance reaches the offeror late or never reaches him

---

acceptor, as against the acceptor, when it comes to the knowledge of the proposer.

240 Bhagwandas v. Girdharilal and Co. AIR 1966 SC 543.

241 Id.

242 Adams v. Lindsell (1818) 106 E.R. 750.

at all. If the offeror to whom several methods of communication are equally open, starts his negotiation by post, it has been construed to be an implied authority for the acceptor to post his acceptance[243] and such acceptance concludes the contract irrespective of whether the letter reaches the offeror or not.[244] According to the ordinary habits of society or according to the usage of mankind, the post is likely to be resorted to as a method of communication in which case posting a latter would conclude the contract.[245] But where the offeror prescribes a method different from posting, mere posting of acceptance would not be sufficient.[246]

The Contract Act was passed in 1872 when the law had not been completely settled in England as to whether a letter which is posted but which does not reach the offeror and is altogether lost in transit would conclude a contract or not. So authors of Indian Contract Act thought it prudent to provide for a dual effect in case of letter of acceptance.[247]

---

243 Dunlop v. Higgins (1848) 9 E.R. 805.

244 Household Fire Insurance Co. v. Grant (1889) 4 Ex.D 216.

245 Hinthan v. Fraser (1892) 2 Ch.27.

246 Eliason v. Henslaw (1819) 4 Wheaton 225.

247 An acceptance concludes into contract when it is put in transmission as against offeror. However an acceptance binds when it reaches offeror. This gives acceptor a chance to revoke his acceptance. But due to this acceptor gets double advantage - once he puts the letter he is freed from further responsibility and at the same time gets an opportunity to revoke the acceptance.

V.7. ACCEPTANCE BY E-MAIL

E-mail is not like the post and it is certainly not like instantaneous communication by the telephone.[248] It is best for the offer to contain as much detail as possible about the acceptance which is sought. The offer should be explicit on how acceptance must be communicated, where it is to be received and when it must be in the place of receipt.[249]

In case of electronic mail, once offeree clicks the 'send' button, control over the message is lost. The electronic mail is sent off to the Internet and goes through various computers, before it reaches its

---

VENKATESH IYER, INDIAN CONTRACT ACT, 68 (Asian Law Book House, Hyderabad, 1982).

248 In case of e-mail, there is no direct connection between sender and receiver. In telephone call, it is possible to check that the intended recipient has heard the acceptance but in case of e-mail, this is next to impossible. E-mails are send using protocols, which allow one computer to pass on information accurately to another. But sometimes these protocols are used incorrectly and e-mail may arrive entirely inconsistent or missing. Some e-mail user are permanently connected to their Service Provider, as soon as an e-mail arrives for them, they are notified and can immediately view the message. What is more common is that when a user's e-mail arrives to a server, the user must contact server to access any message. These connections are not permanent. These users will not be notified that an e-mail awaits them. An e-mail acceptance will not be received if the recipient does not retrieve it. This may be because the person does not check e-mail in-box. In this situation e-mail will constitute acceptance because offeror's recklessness will not prevent the contract formation. Fax machine reports if a fax cannot be sent with sufficient quality but if an e-mail is inconsistent, it is impossible for offeree to know before it is too late.
CLIVE GRINGRAS, THE LAWS OF THE INTERNET, 23-25 (Butterworths, London, 1997).

249 Supra note 229 at 25.

destination. Now the issue to be discussed is when the acceptance through electronic mail is effective - whether at the time of sending or at the time of receipt. According to Postal Rule,[250] on-line contract would form when offeree send the message of acceptance. So when the merchant sends the electronic mail acceptance, the contract is formed within merchant's jurisdiction. In cyberspace, electronic mail can get lost and rejected by firewalls.[251] Sometimes electronic mail is received in so incoherent manner that it goes beyond the comprehension of receiver. Because of increased risk of non-delivery and less reliability, of electronic mail, the Postal Rule creates undue burden on offerer. According to Receipt Rule,[252] the contract would form at offeror's place. In Schelde Delta Shipping B.V. v. Astrate Shipping Ltd.,[253] court decided the time of receipt of acceptance depending on expected time of receipt. Receipt will usually occur when the offerer downloads the message. Alternatively,

---

250 Supra note 235.

251 The function of firewall is to control traffic entering or leaving their network. It acts as an intermediary between internal network and Internet. An external viewer will not have an access to see internal source addresses because the firewall system appears as the source for all client requests. When an organisation embraces the Internet and Extract paradigms, it becomes imperative to provide some form of network and usage protection. That is the primary reason of using firewalls in networked environment today.
Pragya Bharati, *Of Firewalls And Security*, EXPRESS COMPUTER, June 29, 1998.

252 Supra note 235.

253 (1995) 2 Lloyd's Rep. 249.

receipt occurs when it arrives at a computer under offerer's control.[254] According to Receipt Rule, contract is formed when acceptance reaches to offeror's place, i.e., when customer receives merchant's acceptance. So contract is formed in customer's jurisdiction. On-line merchant does not welcome this prospect of forming and enforcing contract in scattered jurisdiction throughout the world.[255]

V.8. ACCEPTANCE OVER WORLD WIDE WEB

Unlike e-mail communication, on the World Wide Web the client and server are in simultaneous communication for most purposes. The communication between the two has the quality of a telephone conversation but between computers rather than human beings. Either party will be immediately aware if the other party goes off line. If the client loses contact with server, the server will know of this situation within seconds and "received data" will not arrive. If the server loses contact, message will arrive that "server not responding". This "knowledge of non-transmission" is determining factor in law. Lord Denning's hypothetical case throws some light in this regard.[256]

---

254 Trystan C.G. Tether, "*Contracting on the Internet*", IBC Conference, January 28, 1998.

255 Supra note 198 at 75.

256 When one person, in the earshot of another, shouts an offer to the other person. The person hears the offer and replies but his reply is drowned by

In Germany, judicial practice has established that a message sent by e-mail is deemed to be received when it reaches the host computer of the addressee.[257]

In South Africa, when the acceptance is by way of post, contract will be concluded at the time when and at the place from where the acceptance is posted, and where the acceptance by means of fax or telegram, the contract is concluded at the time and place where offeror learns of the acceptance and the same rule applies in case of acceptance via e-mail.[258]

In India, the communication of acceptance is complete as against the offeror, when it is put in the course of transmission, the communication of acceptance is complete as against the offeree, when it reaches the knowledge of offeror.[259] The Supreme Court held that in case

---

noise from an aircraft flying overhead. There is no contract at the moment of reply. The accepting person must wait until the noise has gone and repeat the acceptance so the other can hear it. Again when a contract has been attempted to be made over telephone, an offer is made and in the middle of reply of acceptance, the line goes dead, so no contract at this point as the acceptor knows that the conservation has abruptly been taken off. In case of telex also, if the line goes dead in the middle of the sentence of acceptance, teleprinter motor will stop and the person sending the acceptance will know that it has not been received.
Entore Ltd. v. Miles Far East Corpn. (1955) Q.B. 327.

257 Dr. Alexander Loos, *Electronic Contracting with Suppliers under German Law*, p.5.

258 Werksmans Attorneys, *The South African Business Guide to Internet Law*, p.26.

259 Sec.4, Indian Contract Act, 1872.

of oral communication or by telex or by phone, an acceptance is communicated when it is actually received by the offeror.[260] It is to be seen how Indian judiciary treats acceptance through e-mail and Internet.

V.9. CONSIDERATION

Consideration creates no threat for on-line contracts. The goods, service, digitised service provided by merchant and payment made by the customer form consideration. But in case of free software where a click-wrap agreement wants customer to agree to certain terms before down-loading the software, what forms consideration is to be addressed.[261]

If a click-wrap contract is properly constructed, it seems there is a consideration to form a binding contract with the viewer. The programmer of the web is required to create a set of mutual promise that will form the consideration of the contract. It can actually prevent a viewer who does not click "I agree" button, and viewer will also promise to abide by the terms of license.[262]

---

260 Bhagwandas v. Ghirdharilal and Co. (1966) 1 S.C.R. 656.

261 Supra note 198 at 79.

262 Supra note 229 at 28.

V.10. INTENTION

Generally in on-line contract, there will be intention to create legal relation. But when a website which displays product and provide "save" and "download" button but does not provide any purchasing information, customer will think that it is free website and there is no intention to create contract. Afterwards merchant cannot demand any payment for digitised service on the ground that there was intention to create legal relation.[263]

In Thornton v. Shoe Lane Parking[264] it was held that the automatic reaction of the car park, turning a light from red to green and thrusting a ticket was enough to create a contract. It is of no legal consequence that the contract was physically completed by a machine and it is also of no legal consequence that a computer program completes the contract over Internet.[265]

V.11. PAYMENT

After offer and acceptance, payment is another vital factor in electronic commerce. Payment in electronic commerce, is generally done

---

263 Supra note 198 at 80.
264 (1971) 2 Q.B. 163.
265 Supra note 229 at 29.

by credit card and digital cash. The risk involved in these type of payment is that passing payment information through different computers on their way to destination is unsafe and as digital cash consists of zeros and ones in a long string, there is every possibility of getting duplicate of it.

Issues like how should one pay for the goods or services and what happens if that payment does not arrive, are to be discussed. Customer knows his obligation under the contract is over by using his credit card. Here a further contract comes into existence between card company and the user to pay to the card company the full sum under the vendor's contract.[266] If the card company does not pay the vendor, although the card is valid, vendor's right of action is against the card company and not the individual.[267] The best way to receive payment over Internet is to insist on receiving payment and validating of it before supplying goods or services.

Digital cash is of two types - in one case sum is withdrawn from user's account and transferred to vendor's account. This is known as Third Party Digital Cash. In other case, digital cash provider allows the

---

266 Supra note 229 at 31.

267 Re Charge Card Services Ltd. (1988) 3 All E.R. 702.

customer t send encrypted message which represents money to vendor. Vendor can reuse it or can ask the issuing bank to exchange it into cash.[268] In case of Third party digital cash, although court regards issuing company liable for payment rather than user in case of payment dispute but court also held that merely because third party has agreed to make payment to a vendor does not automatically mean that the risk of non payment is removed from user.[269] In case of pure digital cash, if digital cash is intercepted or lost, vendor will claim that payment has not been made as in case of sending bank note by post, if it does not reach, it will not constitute payment.[270] But if the vendor permits the payment by digital cash and customer follows that then he will not be liable for the consequence. So it should be stipulated in the terms of the contract that the contract will be honoured only after receipt of digital cash.[271]

Payment may be complete[272] -

(1) When payer's instruction is transmitted by transferring bank.

(2) When instruction reaches recipient bank.

---

268 Supra note 229 at 31.

269 Supra note 253 at 707.

270 Luttges v. Sherwood (1895) 11 TLR 233.

271 Supra note 229 at 32.

272 EDWARD L. RUBIN & ROBERT COOTER, THE PAYMENT SYSTEM: CASES, MATERIAL AND ISSUES 790 (American Casebook Series, West Publishing Co., 1989).

(3) When recipient bank sets into motion the internal machinery for crediting payee's account.

(4) When payee's account is credited with amount.

(5) When payee is notified of receipt of fund.

In Fedwire transaction, execution by Switch results in transfer of funds, between Federal Reserve account of sending and receiving bank.

Judicial pronouncement like Delbrueck and Co. v. Manufacturers Hanover Trust,[273] provides that EFT payment is final when the order hits Switch.

V.12. JURISDICTION

Every contract may form the basis of a dispute. Effectiveness of a legal system is limited by its political and geographical boundaries. But cyberspace is unconstrained by such limits. Internet allows an owner of a website to form contract with customer from anywhere on the planet. The lack of balance between limitlessness of cyberspace and limited jurisdiction of legal system has exposed the ineffectiveness of national legal system to tackle the issue of jurisdiction. The issue of jurisdiction seems always to have connection with place of contracting, place of

---

273 U.S. Court of Appeal, 2nd Circuit 1979, 609.

negotiation, place of performance, location of subject matter, domicile, residence, nationality, place of incorporation, place of business. So the question remains, which country is going to hear the dispute, resolve it and enforce contractual terms?

V.13. INTERNATIONAL CONVENTION

In U.K., Brussels Convention on Jurisdiction and the Enforcement of judgments in Civil and Commercial Matters, 1968[274] governs jurisdictional matters. The determination of jurisdiction depends on the factor whether party to the contract is domiciled in a contracting state or not. So key determinant for jurisdiction is domicile.[275] According to Brussels Convention, jurisdiction will usually lie in the court of defendant's domicile. The ownership, control or access to a website any where in the world is wholly irrelevant for the purposes of jurisdiction

---

274 This convention is implemented by Civil Jurisdiction and Judgments Act, 1982.

275 Brussels Convention leaves rules framing of regarding domicile to domestic law. Under English law, Sec.41-46, Civil Jurisdiction and Judgments Act, 1982 defines domicile. A person is domiciled in U.K. if he is resident of U.K. and the nature of residence shows a "substantial connection" with U.K. [Sec.41(2)]. It is presumed that being resident for last three months will constitute requisite substantial connection [Sec.41(6)]. Corporation's domicile is dependent on seat of corporation. The seat of corporation is in U.K. if it is incorporated under U.K. law or its central management and control is exercised in U.K. If the corporation is not domicile of contracting state, then its jurisdiction will be guided according to common law.
MICHAEL CHISSICK & ALISTAIR KELMAN, ELECTRONIC COMMERCE: LAW AND PRACTICE, 103 (Sweet and Maxwell, London, 1999).

over an individual under the Convention. So if a customer wants to sue other party domiciled in France, French court will have jurisdiction. It has certain exceptions.[276] Expected place of performance is another exception to the general rule.[277] Consumer contracts offers another exemption to the defendant's domicile rule.

V.14. CONSUMER CONTRACT

According to the convention consumer may sue defendant merchant in either defendant's domicile or consumer's own domicile but consumer can be sued only in his own domicile.[278] But the question remains what is consumer contract?[279]

---

276 It does not apply to contracts on insurance, land, intellectual property. Art.7-12, 16, Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters (1968).

277 Another exception to defendant's domicile rule is that defendant may be sued in the place of performance of the obligation in question. Dispute involves the fact that defendant has failed to perform his contractual obligation that is either the merchant has not delivered the goods or has delivered defective goods or the customer has not paid for the goods. When a customer pays on-line merchant, the place of performance is merchants' place. So when a customer has not paid, he can be sued in merchant's place. In Johnson v. Taylor (1920) A.C. 144, court held that when merchant has failed to deliver goods, place of performance is not customer's place because substantive part of performance occurs in merchant's place where it ships the goods and thus merchant cannot be sued in customer's place.

278 Art.14, Convention on Jurisdiction and the Enforcement of Judgment in Civil and Commercial Matters (1968).

279 Consumer contract includes contract for sale but it also includes contract for supply of service if merchant has solicited in customer's domicile and customer has completed contract formation there [Art.13(3)(a)]. Now what constitutes solicitation. E-mail solicitation can be considered as it is specific invitation but web pages are not directed to any particular jurisdiction, rather it is spread all over the world.

Many contracts made over the Internet are not for the supply of goods or services, they are licences in which it is expressly stated that no sale is taking place.[280] According to the Convention, consumer contract includes only contract for sale of goods or supply of service.[281] So although the download of digital material is a consumer contract in wide sense of the term, in the strict sense contract in dispute may not be consumer contract for the Convention.[282] So if web-wrap licence over digital material is not consumer contract, then for its jurisdictional dispute, general rule of Brussels Convention will apply and consumer in this case will loose the protection provided by Brussels Convention. If a website owner wants to sue a consumer domiciled in U.K., English court will have jurisdiction and if a consumer wants to sue a website owner not domiciled in U.K., consumer shall have to move to website owner's place to start litigation. In case of consumer contract, even specific mention of

---

MICHAEL CHISSICK & ALISTAIR KELMAN, ELECTRONIC COMMERCE: LAW AND PRACTICE, 103 (Sweet and Maxwell, London, 1999).

280 A web-wrap licence passes to the consumer only rights over the digital materials and never title to it. So licence is not a contract for sale of goods. The computer program is not goods as per definition. So transfer of program over Internet does not constitute transfer of goods and it is not contract for sale of goods.
St. Alban's City and District Council v. International Computers Ltd. (1998) 4 All E.R. 81.

281 Art.13(1). The Brussels Convention on Jurisdiction and Enforcement of Judgment in Civil and Commercial Matters, 1968.

282 Supra note 229 at 39.

jurisdiction in contract itself cannot affect the protection given to consumers.[283]

V.15. COMMON LAW

When the defendant's domicile is not in contracting state, Brussels Convention will not apply and common law will guide the jurisdiction matter.[284] If the defendant can be physically served with a writ in England then English Court can claim jurisdiction. If any individual conducts business in England, writ may be moved at the place of business in England. In case of partnership, firm, corporation, writ can be served at the place of business in England.[285]

In case of individual, the person must be physically present at the time of service of writ and in case of corporation place of business can be either registered office or other place of business.

Now whether writ can be moved to web serve taking it as place of business is to be discussed.[286]

---

283 Art.17(1). The Brussels Convention on Jurisdiction and Enforcement of Judgment in Civil and Commercial Matters, 1968.

284 Art.4. The Brussels Convention on Jurisdiction and Enforcement of Judgement in Civil and Commercial Matters, 1968.

285 "We have only to see whether the corporation is "here", if it is, it can be proved." South India Shipping Co. Ltd. v. Export-Import Bank of Korea, (1985). All E.R. 219.

286 If a foreign company set up a web server physically based in England and directed at English customers, server might constitute place of business

Re Oriel Ltd.[287] provides different notion. There are certain businessmen operating on World Wide Web who has nothing more than a server to conduct business, they advertise, take order, deliver service through that server. So server can be a place of business. To make a place of business, what is required is to have "local habitation of its own at or from which it carries on business".[288] The writ can be served to the server through e-mail, addressing it to the web controller of the web site. If possible, e-mail can be sent with "deliver" and "read" receipt for better proof of defendant's knowledge.[289]

V.16. STAYING

In the interest of justice, proceeding can be stayed whenever it is necessary.[290]

---

because advertising and business transaction take place here. The real issue of jurisdiction is to find out applicable forum to maximise justice for both the parties. Companies set web server to facilitate Internet access. So to treat web server as place of business would not be justifiable.

287 (1985) 3 All E.R. 216.

288 Id.

289 Supra note 229 at 118.

290 "The basic principle is that a stay will only be granted on the ground of forum non convenient where the court is satisfied that there is some other available forum, having competent jurisdiction, which is appropriate forum for the trial of the action, i.e., in which the case may be more suitably for the interest of all

V.17. CHOICE OF LAW

Jurisdiction deals with issues of forum where as applicable law deals with what legal principles that forum applies. The issue of applicable law is governed by the Rome Convention, 1980 which has been implemented in U.K. by Contracts (Applicable Law) Act 1990. The Convention covers almost all contracts.[291] Before it, disputes regarding applicable law was decided according to common law principles. Determining applicable law is very important because it governs some very relevant issues.[292] Even if applicable law governs interpretation and

---

parties and the end of justice." Spiliada Maritime Co. v. Consulex Ltd. (1987) A C 460 at 476.

291 The Convention is not applicable in case of legal capacity, land, family matters, trusts, procedural law, proprietary right, issues of intellectual property. Art 1(2), Rome Convention 1980.

292
- Material Validity - Court, using applicable law, will examine validity of the contract. Areas like mistake, misrepresentation, contract formations are looked at.
- Public policy - According to applicable law, the contract becomes unenforceable if it is against public policy.
- Formal validity - Applicable law will look into the formal requirements like writing, signature.
- Capacity - Applicable law is required to note legal capacity of minor, natural persons etc.
- Performance - Applicable law determines condition for performance, that is, diligence required, place, reasonable time etc.
- Damages - Applicable law has to provide quantification of damages, limitations of damages, principles used in measuring damages.
- Presumption of law - Applicable law will govern presumption of law and burden of proof in case of contractual dispute.
- Illegality - Court will not enforce a contract if it is illegal under applicable law.

Art 8, 9, 10, 11, 14 Rome Convention, 1980.

enforcement of contract, court may refuse to accept it. Court will not enforce a contract, even if it is valid, if it is illegal in country of performance.[293] The Rome Convention allows freedom of choice in selecting applicable law.[294] The standard law should expressly mention the law which governs the contract. The selected law need not necessarily have connection with the contract per se and with the place where contract was created.[295] In case where there is no explicit choice of law, the implied choice of law can be inferred from the circumstances if it is demonstrated with reasonable certainty.[296] Rome Convention does not allow to infer a choice of law if the parties had no intention to choose.[297] To infer intended choice of law, pre contractual circumstances can be looked into but not the post contractual circumstances.[298] In the absence of a choice of law, contract is governed by law of the country most closely

---

293 Ralli Bros v. Compania Naviera Sota Y Anzar (1920) 2 K.B. 287.

294 A contract shall be governed by the law chosen by the parties. The choice must be expressed or demonstrated with reasonable certainty by the terms of the contract or circumstance of the case. Art 3(1), Rome Convention, 1980.

295 Vita Food Products Inc. v. Unus Shipping Co. Ltd. (1939) A.C. 277 at 290.

296 Art 3(1), Rome Convention, 1980.

297 In the following cases intended choice may be more apparent -

- In case of standard form of contract when applicable law is known.
- When choice of law for previous contract is known.
- Where contract grants jurisdiction to a specific forum.
- If a contract makes reference to a particular country's legal system.

MICHAEL CHISSICK & ALISTAIR KELMAN, ELECTRONIC COMMERCE: LAW AND PRACTICE, 116 (Sweet and Maxwell, London, 1999).

298 Whitworth Street Estates (Manchester) Ltd. v. James Miller and Partner Ltd. (1970), A.C. 583.

connected to the contract;[299] barring some exception.[300] To illustrate a country which is closely connected, a presumption has been used in Rome Convention.[301] In on-line contract, characteristic performance includes delivery of goods, supply of service, digitised service when these goods and services constitute issuance of contract. When vendor executes characteristic performance, applicable law will be law of his country, not customer's. When all elements of contractual situation is related to one country but the practice to the contract have chosen a foreign law as applicable law, the contract will be subject to mandatory rules of that country also.[302] Consumers get protection of mandatory rules if it satisfies these conditions.[303] In case of on-line contract, if judgement

---

299 Art 4(1), Rome Convention 1980.

300 In case of consumer contract, if there is no choice of law, contract will be governed by the rule of the country, where consumer is habitually resident. Art. 5(3) Rome Convention, 1980.

301 It shall be presumed that the contract is most closely connected with the country when the party who is to effect the performance which is characteristic of the contract has, at the time of conclusion of the contract, his habitual residence or in the case of a body corporate or unincorporate, its control administration. Art.4(2) Rome Convention, 1980.

301 Choice of law made by the Parties shall not have the result of depriving the consumers of the protection offered to him by mandatory rules of the law of the country in which he has his habitual residence." Art.5(2), Rome Convention, 1990.

302 Art.7(2) of Rome Convention, 1980.

303
- First condition - Consumer contract was solicited by the Vendor in consumer's domicile and consumer completed all contract formation steps there.
- Second condition - Vendor received the consumer's order through an agent in consumer's country.
- Third condition - Cross border excursion for the purchase of goods.

is obtained in one country and it will be required to enforce in another country, Brussels Convention comes in rescue for it.[304] Enforcing court cannot review the merit of the case and enforcement can be denied if it is contrary to the public policy. In countries outside the scope of Brussels Convention, the enforcement depends on reciprocal enforcement agreement.

V.18. SALE OF GOODS OR SERVICE

On-line contract is basically concerned with sale of goods and supply of services and digitized services. Goods are defined as all personal chattels other than things in action or money.[305] Electronic sale of consumer goods involve ordering over Internet and e-mail and shipment of goods by port or courier to the purchaser. Service is where the substance of the contract is the skill and labour which have been

---

MICHAEL CHISSICK & ALISTAIR KELMAN, ELECTRONIC COMMERCE: LAW AND PRACTICE, 116 (Sweet and Maxwell, London, 1999).

304 A judgement given in a contracting state and enforceable in that State shall be enforced in another contracting state when, on the application of an interested party, the order for its enforcement has been issued there.
Art 31, Brussels Convention on Jurisdiction and Enforcement of Judgement in Civil and Commercial matters, 1968.

305 Sec 61(1), Sale of Goods Act, 1979.
Sec. 18, Supply of Goods and Services Act, 1982.
Sec. 14, Torts (Interphase with Goods) Act,1977.
Indian Sale of Goods Act, 1930 - See 2(7) - goods means every kind of workable property other than actionable claim and money and includes stocks, shares, growing crops, grass and things attached to or forming part of the land which are agreed to be severed before sale or under the contract of sale.

exercised. Purchasing a standard software from a shop is a sale of goods whereas contract with a firm to write a particular programme is sale of service. Services includes on-line banking, financial service, on-line travel agency etc., these are governed by Supply of Goods and Services Act, 1982.[306] Now the question to be considered is whether sale of a digital product through Internet is sale of goods or sale of services? In Beta Computer (Europe) Ltd. v. Adobe Systems (Europe) Ltd.,[307] court regarded contract for standard, non-customized software as sui-generis.[308] In St. Albans City and District Council v. Internation Computers Ltd.,[309] Court of Appeal decided that while a Computer program on a disk clearly falls within the definition of "goods", a computer program per se does not.[310] This leads to a peculiar situation where an identical digital product falls under different category merely because they are sold using a different medium. Computer program sold

306 Supra note 198 at 55.

307 1996 S.L.T. 604.

308 "It was not an order for the supply of disk as such. On the other hand, it was not an order for the supply of information as such. The subject of the contract was a complex product comprising the medium and the manifestation within it or on it of the intellectual property of the author." Beta Computers (Europe) Ltd. v. Adole Systems (Europe) Ltd., 1996, SLT 608.

309 (1966) 4 All E.R. at 493.

310 "In both the Sale of Goods Act 1979, Sec. 61 and the Supply of Goods and Services Act 1982, Sec.18, the definition of goods includes 'all personal chattels other than things in action and money'. Clearly, a disk is within this definition. Equally clearly, a program, of itself, is not." St. Albans City and District Council v. International Computers Ltd. (1996), 4 All E.R. at 493.

to the licensee on a floppy disk would be good, whereas program transmitted directly over Internet would constitute service. The U.S. Court of Appeal for the Third Circuit viewed software as goods in Advent Systems Limited v. Unisys Corporation.[311] Conceptually placing software into digital form is equivalent to placing it in compact disk. So intellectual property available in digital package can also be regarded as merchantable commodity.[312]

V.19. FORMALITY

Generally contracts can be formed quite informally. Writing and signature is not necessary. Only in few cases, statutes require it to be in writing and signed.[313]

---

311 (1991) 925, F.2d 670, U.S. CA, Third Circle, LEXIS 2396.

312 "Computer Programme are the products of an intellectual process but once implanted in a medium, are widely distributed to computer owners ..... Similarly, when a professor delivers a lecture, it is not a good but when transcribed as a book, it becomes good." Advent Systems Limited v. Unisys Corporation (1991) 925, F.2d 670, U.S. CA, Third Circle, LEXIS 2396.

313
- A contract for the sale or other disposition of an interest in land can only be made in writing and only by incorporating all the terms which the parties have expressly agreed in one document or where contracts are exchanged, in cash.
  Sec.2(1), Law of Property (Miscellaneous Provisions) Act, 1989.
- Lease for over three years.
  Sect.52, Law of Property Act, 1925.
- An unconditional order any form of notation or code whether by hand by the person giving it.... Sec.1, Bill of Exchange Act, 1882.
- An insurance policy must be signed by the insurer.
  S.22-24, Marine Insurance Act, 1906.

So most of the electronic commerce will not be affected. Writing is required to reduce dispute, to make parties aware of consequences, to enable third party reliance.

- In United States, writing and signature requires for sale of goods over $500 and contract lasting over a year.

"... a contract for the sale of goods for a price of $500 or more is not enforceable by way of action of defence unless there is some writing sufficient to indicate that a contract for sale has been made between the parties and signed by the party against whom enforcement is sought..." Sec.2-201(2) Uniform Commercial Code.

Uniform Commercial Code - Sec.5-104 - A credit must be in writing and signed by the issuer and a confirmation must be in writing and signed by the confirming bank.... A telegram may be sufficiently signed and writing if it identifies its sender by an authorised authentication.

Indian Evidence Act 1872 - Sec.91 - When the terms of a contract or of a grant or of any other disposition of property, have been reduced to the form of a document, and in all cases in which any matter is required by law to be reduced to the form of a document, no evidence shall be given in proof the terms of such contract, grant or other disposition of property or of such matter, except the document itself or secondary evidence of its content in cases in which secondary evidence is admissible under the provisions herein before contained.

The Limitation Act, 1963 - Sec.18 - Where before the expiration of the prescribed period for a suit or application, in respect of any property or right, an acknowledgement of liability in respect of such property or right has been made in writing signed by the party against whom such property or right is claimed or by any person through whom he derives its title or liability, a fresh period of limitation shall be computed from the time when the acknowledgement was so signed.

Indian Sale of Goods Act, 1930 - Sec.5(2) - Subject to the provisions of any law for the time being in force, a contract of sale may be made in writing or by word of mouth or partly in writing and partly by word of mouth or may be implied from the conduct of the parties.

Companies Act, 1956 - Sec.46(1) - (a) a contract which, if made between private persons, would by law be required to be in writing, signed by the parties to be charged therewith, may be made on behalf of the company, in writing signed by any person acting under its authority, express or implied and may in the same manner be varied or discharged.

Writing is defined as typing, printing, lithography, photography and other modes of representing or reproducing words in a visible form.[314] Whether recording and transmission of electronic impulses within a data communication system falls within the definition of writing is to be found out. Now digital contract displayed on a computer screen is in visible form but neither tangible nor permanent.[315] In recent times, there is a move to expand the definition of writing so as to include digital documents.[316] The expression "under the hand of" can be regarded to

---

314 Sch.1, Interpretation Act, 1978.

315 "There is a document whenever there is writing or printing capable of being read, no matter what the material may be upon which it is impressed or inscribed" - this was held in R. v. Daye (1908) 77 LJKB 659 at 661.

316
- Documents not necessarily has to be original (in writing) in order to be admissible.
  Sec.8, Civil Evidence Act, 1995.
- Writing includes any form of notation or code whether by hand or otherwise and regardless of the method by which or medium in or on which it is recorded.
  Sec.178, Copyright, Design and Patent Act, 1988.
- The database so far as it contains information capable of being retrieved and converted into readable form is a document.
  Derby & Co. Ltd. v. Weldon (Wo.9) (1991) 1 W.L.R. 652 at 654.
- Writing includes printing, typewriting or any other intentional reduction to tangible form.
  Sec.1-201(46) Uniform Commercial Code.
- Technologies such as telexes and faxes were held to be writing.
  Basak International Co. v. Mast Industries Inc. 73 NY 2d III, 7 UCC Rep. Serv. 2d 1380 (1989).
- In today's paperless society of computer generated information, the court is not prepared, in the absence of some legislative provision or otherwise, to find that a computer floppy diskette would not constitute a writing within the meaning of the Statute.
  Clyburn v. Allstate, 826 F. Supp. 955.

denote use of signature.[317] In English law, there is no formal legal definition of signature.[318]

The concept of signature has been broadened.[319] In case of electronic mail, signature can be done by typing the name of the sender at

---

317 General Clauses Act 1897 - Sec.3(56) - Sign with its grammatical variations and cognate expressions, shall with reference to a person who is unable to write his name include mark with its grammatical variations and cognate expression.

318 Bills of Exchange Act 1882 - Sec.91 - Signature - (1) Where by this Act, any instrument or writing is required to be signed by any person, it is not necessary that he should sign it with his own hand but it is sufficient if his signature is written there on by some other person by or under his authority. (2) In the case of a corporation where, by this Act, any instrument or writing be sealed with the corporate seal. But nothing in this section shall be construed as requiring the bill or note of a corporation to be under seal.
Uniform Commercial Code - Sec.3-401 - A signature is made by use of any name, including any trade or assumed name, upon an instrument or by any word or mark used in lieu of a written signature.
Companies Act, 1956 - Sec.229 - Only the person appointed as auditor of the company or where a firm is so appointed in pursuance of the proviso to sub-section (1) of Sec.226, only a partner in the firm practising in India may sign the auditor's report or sign or authenticate any other document of the company required by law to be signed or authenticate by the auditor.

319
- Where an Act of Parliament requires that any particular document be signed by a person, then prima facie, the requirement of the Act is satisfied if the person himself places on the document an engraved representation of his signature by means of rubber stamp... The essential requirement of signing is the affixing in same way, whether by writing with a pen or pencil or by otherwise impressing upon the document, one's name or signature so as personally to authenticate the document.
  Goodman v. J. Eban Ltd. (1954) 1 Q.B. 550.
- Fax copy of a signature satisfies relevant statutory signature requirement.
- If a signature is digitised and then appended to the fax, the document should be regarded as signed.
  Re a Debtor (No.2021 of 1995) (1996) 2 All E.R. 345.
- The signature... may be in handwriting, printed or facsimile, perforated, stamped, in symbols or made by any other mechanical or electronic means, if not inconsistent with the law of the country where... the document is issued.

the end of the mail or by appending the signature file with the mail. As it can be easily exposed to the fraud, technologies like digital signature can come for help. In case of web contract, customer accepts contract by clicking button which is no way equivalent to signature. The on-line contract form has input boxes in which customer types name, address, e-mail address which can be construed as signature.[320] Though signed contract is not generally required by law, it is used for greater legal weight.[321] UNCITRAL Model Law on Electronic commerce have tried to remove writing and signature requirement to facilitate on-line contract and electronic commerce.[322]

Art.14(3), United Nations Conventions on the Carriage of Goods by Sea, 1978.

320 If the name of the party to be changed in printed or written on a document intended to be a memorandum of the contract, either by himself or his authorised agent, it is his signature, whether it is at the beginning or middle or foot of the document.
Durrell v. Evans (1862) 1 H & C 174 at 191.

321 "When a document containing contractual terms is signed, then, in the absence of fraud.... the party signing it is bound and it is immaterial whether he has read the document or not".
L'Estrange v. Graucob (1934) 2 K.B. 394.

322
- It has developed concept of 'data message' which is electronic equivalent to written document which includes EDI, E-mail, telex.
  Art.2(a), UNCITRAL Model Law on Electronic Commerce.
- "Where the law requires information to be in writing, that requirement is met by a data message if the information contained there in accessible so as to be usable for subsequent reference."
  Art.6(1), UNCITRAL Model Law on Electronic Commerce.
- "Where the law requires a signature of a person, that requirement is met in relation to a data message if:

In India digital signature is so far not valid. Signature has not been defined under Indian Law. The General Clauses Act 1897 does not define the term sign but extends its meaning with reference to a person who is unable to write his name to include a mark with its grammatical variations and cognate expressions.[323] So if a mark or thumb expression has been affixed to a document by a person who is able to write his name, it would not be considered as signature.[324] If name were inserted into a document of acknowledgement in such a way as to signify that the acknowledgement was intended to be his own, such a name whether written or printed would constitute his signature.[325] Many countries like several States of US, Germany, Australia, Singapore have enacted law on digital signature which validate digital signature and articulate role of Certification Authority. India's Information Technology Bill speaks about digital signature.[326]

(a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message, and
(b) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all circumstances, including any relevant agreement".

Art.7(1), UNCITRAL Model Law on Electronic Commerce.

- "Contracts shall not be denied validity or enforceability on the sole ground that a data message was used for that purpose."

Art.11(1), UNCITRAL Model on Electronic Commerce.

323 Sec.3(56) of General Clauses Act, 1897.

324 Raghubir Singh v. Thakwain Sukhraj Kaur, AIR 1936 Oudh 96.

325 Sec.18, Limitation Act, 1963.

326 Sec.3, Information Technology Bill, 1998.

V.20. DEMATERIALISATION OF BILL OF LADING

One of the most difficult areas to replicate in an electronic environment is the function that paper-based document does in commercial context. Physical possession of a document confers certain legal rights. These legal documents are used for international trade transaction, many transmission and securities within financial arrangement. For dematerialisation of these documents electronically, following steps are required.[327]

(a) Amendment of relevant legislation (b) Establishment of electronic procedure which replicates symbolic function (c) Encourage commercial practice to change.

Bill of lading is a quasi-negotiable instrument and it can be seen to perform three functions[328] -

(1) Evidence of condition of goods at the time of shipment signed by the career as evidence for any future dispute, (2) terms of the contract of carriage, (3) document of title.

---

327 ELECTRONIC TRANSACTION §5.1.

328 Negotiable instruments have three distinct features - (1) full legal title is passed upon delivery of instrument, (2) no notice of transfer is required to be given to the issuer of the instrument, (3) title is passed unfettered. But in case of bill of lading title remains subject to the prior claim from third parties. So it is classified as quasi negotiable instrument.
ELECTRONIC TRANSACTION §5.1.

In modern international trade, its use creates significant obstacle. Developments in transportation like containerisation has created a situation where goods move faster than associated paper document. This happens if bill of lading has been traded several times during transportation. Such problems have compelled international trader to resort to other techniques designed to overcome delay but this seriously undermines legal validity of the bill of lading. The break down in the reality of bill of lading as a secure legal instrument has encouraged the drafting of scheme designed to dematerialise bill of lading.[329] Art.17(1) of

---

329 The first attempt to establish a practical electronic trading system for bill of lading was set up by INTERTANKO through SEADOCS scheme. Under this scheme, the Chase Manhattan Bank was to act as central registry for the bill of lading and acting as an agent for all parties, would transfer ownership under electronic notification. In 1990, Comite Maritime International (CMI) decided to formulate an alternative electronic communication procedure and published a set of rules that can be contractually adopted between internationally trading partners to permit the electronification of the bill of lading. These rules operated on the basis that bill of lading is held by carrier who transfers the registered ownership of the bill upon electronic notification. Here the parties agree that electronic message shall have the same effect as paper bill of lading, they waive the right to raise the defence that bill of lading is not in writing. In U.K., the Carriage of Goods by Sea Act 1991, in Commercial.1(5) provides - "The Secretary of States may by regulation make provision for application of this Act to cases where a telecommunication system or any other information technology is used for effecting transactions corresponding to - (a) the issue of a document to which this Act applies, (b) the endorsement, delivery or other transfer of such a document, (c) doing of anything else in relation to such a document". In 1990, ICC's INCOTERM - CIF (Cost, Insurance, Freight) has recognised the use of electronic mode of communication - "Where the seller and buyer have agreed to communicate electronically the document may be replaced by an equivalent electronic interchange message".

UNCITRAL Model Law on Electronic Commerce, 1996 provides that subject to paragraph (3) where the law requires that any action referred to in Art.16 be carried out in writing or by using a paper document, that requirement is met if the action is carried out by using one or more data message.

V.21. DOMAIN NAME

Trade mark is very important in business and commerce. Goodwill built up under a brand is extremely valuable. When commerce is done through Internet domain name[330] becomes equally important.

Gronfers, *The Paperless Transfer of Transport Information and Legal Functions*, SCHMITHOFF & GOODE (ed.), INTERNATIONAL CARRIAGE OF GOODS: SOME LEGAL PROBLEMS AND POSSIBLE SOLUTIONS, 1998.
Todd P., *The Effect of Letters of Credit of New Documentation and the Introduction of Electronic and Paperless Transactions* (A paper submitted to IBC's International Letter of Credit Conference, July 3, 1990).
Rule 1, 4, 5, 10, CMI Rules.

330 A domain name is an easier alternative to Internet Protocol address which is a collection of some numbers like 211.526.60.66 and which is used by the webservers to identify each other on the Internet. Usually these domain names start with the prefix "www" and end with two or three letter suffix that indicates which type of organisation owns the website. For example, the website of The Times, "www.thetimes.co.uk" indicates that the owner of the website is a company registered in United Kingdom. these suffix can be "org", "gov", "com" representing organisation, government, company, respectively. The corresponding Internet Protocol number of the domain name represents the computer that stores digital materials. If these materials are moved to other computer, that number will be changed but the domain name will remain the same. Because of the global reach of the Internet, domain name can reach every part of the world and it can be accessed from every part of the world. Domain name can be received through registration and it is allocated on first come first served basis, without checking whether the applicant has

Though domain name can be owned by only one entity in the world and it has global presence but trade mark can be owned by two companies in respect of different products and is protected within a defined territory. This leads to the situation where two users of the same trade mark in different countries, fighting for same domain name.[331] The most common form of dispute is where a person with a legal right to a trade mark seeks to use it within a domain name but discovers that some one already has registered that name as domain name.[332] In One in a Million decision, the issue of cybersquatting was settled and trade mark holders were assured

---

right to use the name. One domain name can be owned by one entity at a time. This loads to the domain name controversy.
MICHAEL CHISSICK AND ALISTAIR KELMAN, ELECTRONIC COMMERCE, LAW AND PRACTICE, 18 (Sweet and Maxwell, London, 1999).
CLIVE GRINGRAS, THE LAWS OF THE INTERNET, 128 (Butterworths, London, 1997).

331 Supra note 229 at 130.

332 Prince Plc v. Prince Sportswear Group Inc. CH-1997-PNo.2355 (July 18, 1997) demonstrates an example for domain name dispute. Here Prince Sportswear Group Inc. complained against Prince Plc, U.K based information technology company that it had infringed the name "prince.com" as the sports group had number of PRINCE trade mark registration, although the information technology company had genuine registration of domain name. National Standard Institute of U.S issued Domain Name Resolution Policy by which any U.S federal trade mark holder or holder of a foreign trade mark can preempt the right of pre-registered genuine domain name holders. The losing of domain name can be stopped if the company has U.S federal trade mark registration or foreign trade mark registration or has commenced proceeding in a court of appropriate jurisdiction to protect domain name. Prince Plc could not show any of these but, according to NSI's direction Prince Plc filed suit in High Court in London alleging that, statement made by Prince Sportswear Group Inc., that Prince Plc was infringing its trade mark, constituted groundless threats. Court granted injunction and Prince Plc continues to have "prince.com" domain name.

of protecting their rights on Internet.[333] Recently WIPO has taken a decision to take measures to prevent cybersquatting. In MTV Networks v. Adam Curry,[334] the only right which the defendant had over the site was a technical one, he was the owner of the domain name and he was not owner of any legal right to use the name MTV in relation to his business. According to English law, assuming "MTV" as registered trade mark, this case would have become a case for infringement of trade

---

333 Marks and Spencer Plc, Stainsbury Plc, Vergin Enterprises Ltd., British Telecommunication Plc alleged that One in a Million Ltd. was passing off and infringing their trade mark. Actually One in a Million Ltd. has registered the trade names such as Marks and Spencer, Stainsbury, British Telecom as domain name like marksandspencer.co.uk, stainsbury.com, virgin.org, britishtelecom.com. The intention of One in a Million Ltd. in registering these domains was to make a profit by selling them to the owner of the goodwill and thus pleaded that it did not amount to passing off. The Court of Appeal held that the registering of distinction name as domain name made false representation to the people who consulted the register to find out connection between the person who got registration and the name registered. Court also held that after registration, any realistic use of those name would lead to passing off. Court granted permanent injunction against One in a Million Ltd. Court observed that the systematic registration of popular trade marks as domain names were actually blocking the registration by the trade mark owner and were process to extract money from trade mark owner by exploiting their goodwill. The judgment stopped the abusing trade marks by domain name pirates. It reassures that domain names act as trade mark and trade mark owners can expect that their rights will be protected on the Internet.
Marks and Spencers Plc. and Others v. One in a Million Ltd., Court of Appeal, July 23, 1998.

334 Adam Curry registered a website with the domain name "www.mtv.com" before August 1993. This site provided information about the music business. MTV eventually realised the potential of the Internet and sought to acquire the domain name owned by Adam Curry in 1994. MTV Networks v. Adam Curry (867 F. Supp. 202, SDNY 1994).

mark.[335] Some protective measures can be taken to avoid this dispute, like to make a search whether any other party is using the intended domain name, to enquire from Registering Authority whether the intended domain name has been already registered or not, to take trade mark registration of the domain name. Trade and Merchandise Act of India is to be amended to include service mark within its ambit so that domain name of all organisations dealing with service or digitised service can be registered as trade mark. A convention is required to be convened by major concerned countries to make a framework for global protection of trade mark.

V.22. HYPERLINKS

Hyperlink is another topic which has much relevance in electronic commerce world. It allows link to different pages at the same or different

---

335 Adam Curry was offering service under the sign "www.mtv.com" where www and com are generic and not part of the name. So the similar sign has been used in the course of trade by Adam Curry, which was registered trade mark of MTV Networks. After a prima facie case of infringement is established, as remedies in case of domain name, MTV would prefer to ask Adam Curry stop using the domain name and allow MTV to take over the domain name. If the case is not fit for trademark infringement then, common law right - passing off claim can be used. Adam Curry's using of domain name "www.mtv.com" can be shown as using existing goodwill in the name MTV and potential customers will be mislead by thinking it as under control or licence of MTV Networks. The damage suffered by MTV Networks is not regarding lost sale rather it is dilution of the distinctness of the name "MTV".
CLIVE GRINGRAS, THE LAWS OF THE INTERNET, 136-150 (Butterworths, London, 1997).

websites. Shetland Times v. Dr. Jonathan Wills & The Shetland News Ltd.[336] provides that there is copyright in a link to one's site. although unexpectedly, it was held in this case that there is copyright in newspaper headline and it is infringement to copy it in electronic form or to incorporate in cable program. The valid position is that a page of a text on a website will be protected by copyright as a literary work. To infringe copyright, the whole or substantial part of the work is to be copied. One line or link does not constitute substantial part. A link is like a reference to other material. There cannot be copyright to a link as it does not require skill, labour and judgment to create it.[337]

V.23. FRAMING

Framing is a technique by which multiple windows can be created on computer screen where each window is independent and information

---

336 Shetland News has website. It provides its readers access to webpages of other sites by including links to those pages. These included link to CNN's website and websites of other major newspapers. The website of Shetland news does not provide copies of articles rather it simply provides links as series of headlines from other websites. Like this, it has included some headlines appeared in Shetland Times' website. Headlines of Shetland Times' website were identical to those of Shetland News' list of links. The Shetland News did neither copy nor provide the copy of relevant article. The Shetland Times sought for declaration that Shetland News's action constitute infringement of copyright in the headlines.
Shetland Times Ltd. v. Dr. Jonathan Wills & Shetland News Ltd. (Scottish Court of Session, 24 October, 1996).

337 Supra note 229 at 179.

can be downloaded from one window without affecting the other. This framing sometimes create a situation where it appears that copyright is getting infringed.[338] Technically and legally, no copyright violation case emerges out of these situations.

V.24. ON-LINE BANKING

With the emergence of Internet as highly potential medium for conducting business, banks have also started with on-line operations. Internet is affecting banking activities by sending payment instruction, receiving bank statements and transferring funds electronically. Now the question is whether institutions who are offering financial service on the Internet are bank or not.[339]

---

338 In a practical fact situation, company ABC has an website which has two frames, one is containing the company's logo and other is containing hyperlink to some copyrighted article of company XYZ. Now if one user, browsing through the website of Company ABC and if clicks the hyperlink, he will reach the copyrighted article of Company XYZ. In this particular moment, Company ABC's logo is on the screen of the user's computer and company XYZ's copyrighted article is also on the screen of the user's computer. This create situation where the hyperlinked article appears to belong to Company ABC. It prompts Company XYZ to charge Company ABC for infringing its copyright. Vaibhav Parikh, *Legal Issues in E-Commerce with Special Reference to India*, 17-18 (A paper presented in E-Commerce Seminar and Exposition, conducted by Confederation of Indian industries, 19-20 February, 1998).

339 Bankers' Book Evidence Act, 1891 - Sec.2(2) - bank means any company carrying on business of banking.
Banking Regulation Act, 1949 - Sec.5(b) - "banking" means the accepting, for the purpose of sending or investment, of deposits of money from the public, repayable on demand or otherwise and withdrawable by cheque, draft, order or otherwise.

Only an authorised institution can accept deposit and for this it has to be licenced and it will come under strict regulations of Banking laws.[340] So by avoiding accepting deposit, institutions offering financial service on the Internet can escape from stringent regulations under Banking laws. This technical escaping is to be checked.

V.25. ELECTRONIC MONEY

Money is medium of exchange having purchasing power.[341] Companies like Digital Cash Inc. and Cyber Cash Inc. have come out

---

340 "No person shall accept a deposit in the course of carrying on (whether or elsewhere) a business which for the purposes of [the Banking Act] is a deposit - taking business unless that person is an institution for the time being authorised by the Bank of England under the following provisions of ... [the Banking Act]".

Sec.3, Banking Act 1987.

- "A deposit is a sum of money (whether denominated in a currency or in ECUs) paid on terms -

(a) under which it will be repaid, with or without interest or a premium and either on demand or at a time or in circumstances agreed by or on behalf of the person making the payment and the person making the payment and the person receiving it, and

(b) which are not referable to the provisions of property or service for the giving of security."

Sec.5, Banking Act, 1987.

- "A business is deposit taking business if

(a) in the course of business money received by way of deposit is lent to others, or

(b) any other activity of the business is financed, wholly or to any material extent, out of the capital of or the interest on money received by way of deposit."

341 The Dictionary of Finance defines money as a means of facilitating exchange of goods and accumulation of financial wealth, commonly recognisable as bank

with electronic cash. Although electronic cash has been treated like physical cash but it has not received the status of legal tender.[342]

It is neither included within the definition of 'deposit' not it is regarded as "negotiable instrument".[343] Digital cheque and electronic fund transfer has also not been recognised by the existing legal frame work.[344] This electronic cash has tremendous impact on total monetary

---

notes, coins, bank deposits and (i) a medium of exchange, (ii) a unit of value (iii) a store of wealth.

342 Foreign Exchange Regulation Act, 1973 - Sec.2(f) - Currency includes all coins, currency notes, bank notes, postal notes, postal orders, money orders, cheques, drafts, traveller's cheque, letters of credit, bill of exchange, promissory notes.

343
- Negotiable Instrument Act 1881 - Sec.13(1) - A negotiable instrument means a promissory note, bill of exchange or cheque, payable either to order or to bearer.
- Reserve Bank of India Act 1934 - Sec.45l(bb) - 'deposit' shall include and shall be deemed always to have included any money received by a non-banking institution by way of deposit or loan or in any other form but shall not include amount raised, by way of share capital or contributed as capital by partners of a firm.
- Companies Act 1956 - Sec.58A - Explanation - For the purpose of this section 'deposit' means any deposit of money with and includes any amount borrowed by a company but shall not include such categories of amounts as may be prescribed in consultation with Reserve Bank of India.

344 Reserve Bank of India had set up K.S. Shere Committee to formulate guidelines for framing law on electronic fund transfer. The Shere Committee presented its report in 1996. The report examines the different types of EFT, existing technology, existing legal provision for EFT in India and different legislation relating to EFT in various countries. The Committee has provided proposed amendment to RBI Act, proposed amendment to Bankers Book Evidence Act. With the implementation of this report, shortcomings of existing legal framework will be removed and transfer of fund via electronic medium will be boosted.
Vaibhav Parikh, *Legal Issues in E-Commerce with Special Reference to India*, 19 (A paper presented in E-Commerce Seminar and Exposition, conducted by Confederation of Indian industries, 19-20 February, 1998).

system of a country. Electronic cash is issued by institutions who are not so called "Bank" and does not come under strict regulations of Banking laws, which requires sufficient capital adequacy and liquidity for the sake of customer's interest.[345] The unrestricted issuing power of these institutions will snatch the control of central bank over monetary system.[346] Electronic cash will be issued by depositing hard cash. Then electronic cash will be exchanged by the merchant and consumers and the hard cash also will be put into circulation by the issuing institution. So total amount of cash which is in circulation in the market will increase so much that it will lead to inflation.[347] The central bank will not be in a position to control the monetary condition of the country. As the electronic cash can be changed into any currency, so it will affect foreign exchange regulation and Foreign Exchange Regulation Act is not efficient in tackling the issue.[348] Huge amount of cash can flow across the border

---

345 Supra note 235 at 17-18.

346 The Coinage Act 1906 - Sec.6(1) - Coins may be coined at the Mint for issue under the authority of the Central Government of such denomination not higher than one thousand rupees, of such dimensions and designs and of such metals or mixed metals of such composition as the Central Government may by notification in the Official Gazette determine.

347 Supra note 163 at 72.

348 Foreign Exchange Regulation Act, 1973 - Sec.13(1) - The central bank may by notification in official gazette, order that subject to such exemption, if any, as may be specified in the notification, no person shall except with general or special provision of the Reserve Bank and on payment of fee, in any, prescribed, bring or send into India any foreign exchange or any Indian currency.

through electronic cash which can collapse any country's economy any time.[349] Cross border movement of cash as supported by electronic cash can help tax evasion, money laundering, etc. A legislative initiative is required to adopt electronic cash and for that purpose necessary amendments are to be made in Negotiable Instrument Act and Banking Regulation Act.

V.26. ELECTRONIC MINT

Institutions which are issuing electronic cash are equivalent to electronic mint. It is a threat for the existence of government issuing currency. Electronic cash has potential to become global currency. The institutions issuing electronic cash are required to come under same kind of strict regulatory measure as conventional banks, so far as capital adequacy and liquidity are concerned. More over these institutions are required to be connected to central banks so that central banks remain in a position to control the monetary system of a country.[350] If these electronic mints (Digital Cash Inc., Cyber Cash Inc.) and electronic cash continues to run like today without any regulatory mechanism and legal frame work, the fact of running two parallel currency side by side can

---

349 Supra note 152 at 48.

350 Supra note 152.

lead to a situation where in one point of time hard currency may lose its validity and relevancy which can be a disaster to the economy of the world.

V.27. ENCRYPTION SOFTWARE

The problem faced by encryption software is problem of balancing between privacy and free trade on one hand and national security and law enforcement on the other.[351] According to National Research Council, encryption has four major uses - ensuring data integrity, authenticating users, facilitating non repudiation and maintaining confidentiality.[352] In U.S., prior to 1 January, 1997, jurisdiction over export of encryption software was split between State Department and Commerce Department and from that day Commerce Department was in sole charge of it.[353] The reason for shift from military to commercial control is "... because of the increasingly widespread use of encryption products for legitimate protection of the privacy of data and communications in non-military context, because of the importance to

---

351 Jeffrey L. Snyder, *U.S. Expert Controls on Encryption Software*, THE JOURNAL OF WORLD INTELLECTUAL PROPERTY, p.37.

352 National Research Council, National Academy of Sciences, *Cryptography's Role in Securing the Information Society* (1996).

353 Supra note 229.

U.S. economic interest of the market for encryption product".[354] According to the present condition, export approval is to be obtained in case of strong encryption product and low level encryption product - algorithm with a key length of 40 bits or less are eligible for export after one time review by Commerce Department.[355] In Bernstein v. the United States[356] it was held, "... the Export Administration Regulations, 15 C.F.R. part 730.... (1977) and all rules, policies and practices promulgated or pursued thereunder in so far as they apply to or require licensing for encryption and decryption software and related devices and technology are in violation of the First Amendment on the grounds of prior restraint and are therefore unconstitutional...".[357] The enforcement of this order was stayed on an emergency basis.[358]

---

354 White House Memorandum, Encryption Export Policy, 15 November 1996.

355 61 Fed. Reg at 68573.

356 Bernstein developed an encryption algorithm called "snuffle" which he describes as a "zero-delay private-key encryption system. He has also written a paper, The Snuffle Encryption System" and has generated source code in the C programming language for both encryption and decryption. Bernstein sought classification of the export control status of his work. The Department of State determined that the source code was controlled as a munition and therefore was restricted under ITAR. Bernstein then sued the Department of State claiming that ITAR Control Violated First Amendment because they limited his ability to teach.

357 Bernstein v. the United States, 974 F. Supp. 1288.

358 Order No.97-16686, 22 September, 1997.

V.28. EVIDENCE

The system of commerce depends on the fact that agreements between the parties are documented. These documents containing terms of agreement are used as evidence. In case of electronic commerce, the problem is that the documents are computer generated. Computer generated documentary evidences are of three types. The first type is real evidence which are calculations and analysis generated by computer itself through running a software and receipt of information from other devices. For example, when bank automatically calculates bank charges due from a customer depending on tariffs, transactions on account and credit balance, it is a real evidence. Finger prints, DNA samples, blood stains are real evidences. The second type of computer generated evidence is hearsay evidence which are copies made by computer of information supplied to the computers by human beings. Cheques drawn and paying-in-slips are hearsay evidence. The third type of computer generated evidence is derived evidence which combine both real evidence and information supplied to the computer by human being. For example, daily balance column of a bank statement is derived evidence.[359]

---

359 Supra note 229.

The fundamental difference between a paper based payment system and a paper less payment system lies in the absence of any written record of the transactions in later case. In the paper based transactions, at present in India, the counterfoil normally serves as evidence. In the U.S., by law, system or service providers are required to give written records of transactions. When EFT is introduced in India, especially EFTPOS and other card based transactions like ATMs, a provision requiring service providers to ensure furnishing authenticated records of transactions need to be made.[360] The United Nations Commission on International Trade Law had made a survey which showed that in most countries records kept in computer can be used as evidence in case of litigation subject to proponent of record establishing certain facts about the record and computer system. The proponent will have to establish that the system was properly designed and sufficiently well managed and the possibility that the data stored in the record being incorrect, was reduced to minimum.[361] In U.K. subject to certain conditions, a statement contained in a document produced by computer

---

360 Report of the Committee for Proposing Legislations on Electronic Fund Transfer and other Electronic Payments, Reserve Bank of India, January 1996, p.50.

361 Id. at 51.

will be admissible as evidence in civil proceeding.[362] Apart from this, a document produced by computer print out will be admissible as evidence in any proceeding if it is shown that the statement is reasonably accurate and that the computer was working properly at the relevant time.[363]

R v. Wood[364] also held that computer printouts are admissible as real evidence if the computer has worked as calculator. In R. v. Spiby[365] telephone printout from PBX computer was admissible as real evidence. The only negative side of computer evidence is that there is possibility that aggregation of small errors can make high probabilities of error. Civil Evidence Act, 1995 gives a major break through to computer generated evidence.[366] In case where computerised data-base which contain details of transactions, court held that computer data base which forms part of

---

362 Sec.5, Civil Evidence Act, 1968.

363 Sec.69, Police and Criminal Evidence Act, 1984.

364 (1982) 76 Cr. App. Rep. 23.

365 (1990) 91 Cr. App. Rep. 186.

366 Sec 8(1) - where a statement contained in a document is admissible as evidence in civil proceedings, it may be proved -
(a) by the production of the document, or
(b) whether or not that document is still in existence, by the production of a copy of that document or of the material part of it authenticated in such manner as the court may approve...
Sec. 12 - 'document' means anything in which information of any description is recorded.
'copy' in relation to a document, means anything onto which information recorded in the document has been copied, by whatever means and whether directly or indirectly.

the business records of a company, in so far as it contains information capable of being retrieved and converted into readable form, is a document.[367] Technology has created new ways of keeping business records other than bound books. Legislation has also made a way for it.[368] If an accounting record has been digitally signed, company needs to be able to associate the digital signature with a particular person. A smart card or PIN is unlikely to solve this problem as the signing will be done by artifact and it can sign unauthorised accounting records if it is in wrong hand.[369]

In India, although the Evidence Act which generally governs the proof in civil and criminal proceeding has not yet adopted itself to the computer age.[370]

---

367 Derby & Co. Ltd. v. Weldon (1991) 2 All E.R. 901.

368 Companies Act 1985 -

Sec. 722(1) - Any register, index, minute book or accounting records required by the Companies Act to be kept by a company may be kept either by making entries in bound books or by recording the matters in question in any other manner.

Sec 722 (2) - Where any such register, index, minute book or accounting records is not kept by making entries in a bound book but by some other means, adequate precautions shall be taken for guarding against fabrication and facilitating its discovery.

369 Supra note 198 at 159.

370 • Indian Evidence Act 1872 - Sec.3 - document means any matter expressed or described upon any substance by means of letters, figures or marks or by more than one of these means, intended to be used, or which may be used for the purpose of recording that matter.

Records kept in disk, microfilm and other electronic memory system are made admissible as evidence in Customs and Excise Laws.[371] The issues relating to amending the Banker's Books Evidence Act so as to make computer printouts used in banking transactions, replacing the traditional ledgers as primary evidence and including the banker's record stored in electronic media within the definition of Bankers Books Evidence Act had been examined by the Reserve Bank and the proposals

---

- Under the term "document" are properly included all material substances on which the thoughts of men are represented by writing or any other species of conventional mark or symbol. -
  RATANLAL & DHIRAZLAL, THE LAW OF EVIDENCE (Wadhwa and Company, 19th ed. 1997).
- Indian Penal Code - Sec. 29 - The word 'document' denotes any matter expressed or described upon any substance by means of letters, figures or marks or by more than one of those means, intended to be used or which may be used as evidence of that matter.
- General Clauses Art 1897 - Sec 3(18) - document shall include, any matter written, expressed or described upon any substance, by means of letters, figures or marks or by more than one of those means, which is intended to be used or which may be used for the purpose of recording that matter.
- The Commercial Documents Evidence Act 1939 - certain commercial documents of various kinds are by the practice of merchants accepted as evidence and taken as prima facie correct but in a court of law they cannot in the absence of consent by the parties, be admitted in evidence without testimony as to their genuineness or the correctness of the statement made therein. Such documents are not admissible in evidence u/s 32 or any other provision of Evidence Act without further proof. So a party desirous of delaying the proceeding can insists on the other side getting commissions issued to take evidence as to fact which are for all practical purposes sufficiently established by the documents in question. This Act is to provide that commercial documents which are accepted as prima facie correct in commercial circles may be admitted in evidence without formal proof.

371 The Customs and Central Excise Laws (Amendment) Act 1988 - Sec. 138 Customs Act 1962, Sec.36B Central Excise and Salt Act, 1944.

made by Reserve Bank for amending Bankers Books Evidence Act is under consideration of Government of India.[372] Books, accounts and other documents as well as instruments handled by Banks, apart from their evidentiary value, have special significance from supervisory angle.[373]

The legal issues which have emerged due to introduction of electronic commerce, reflects the urgency in adopting new laws and modifying existing laws and for which reviewing legislations of other countries are utmost necessary.

---

372 Supra note 360 at 52.

373
- Records have to be kept for six years by public company and three years by private company.
  Sec. 222, Companies Act 1985.
- Central Government, through promulgation, prescribed that banking companies are required to preserve specified ledgers, registers and other records for a period of five to eight years.
- Banking Companies (Period of Preservation of Records) Rules, 1985.
- Companies Act, 1956 - Sec 209 (4A) - The Books of account of every company relating to a period of not less than eight years immediately preceeding the current year, together with the vouchers relevant to any entry in such books of account shall be preserved in good order.

Chapter VI: Legislative Initiatives

CHAPTER VI

LEGISLATIVE INITIATIVES

With the exploding popularity of the Internet, it is almost a requirement that a business have a presence on the Internet. The Internet has made electronic commerce one of the most effective and reliable methods for conducting business. The emerging information and communications network is likely to have an important impact on economic development and world trade. The users of information technology must have trust in the security of information and communications infrastructures, networks and systems regarding the confidentiality, integrity and availability of data on them and in the ability to prove the origin and receipt of data. The data is vulnerable to sophisticated threats to its security. Ensuring security of data through legal, procedural and technical means is fundamentally import national and international information infrastructure to exploit their full potential. There is need for varied legislative initiatives to manage issues like entry to cyberspace, access to cyberspace, hardware and software which enables people to access cyberspace or use their own computers to go "on line" and enter cyberspace. Some of the key players in this area includes

phone companies, regulatory agencies, personal computer companies, software companies, Internet service providers, schools, colleges, universities, all persons and companies that have established their presence on the Internet.

Existing legal regime is based on paper transaction. Authenticities of these transactions are established through signature. In electronic environment, when paper and signature have been replaced, legal rules are required to define under what circumstances a person can be bound in respect of an electronic instruction issued to him. In electronic medium, authentication is achieved through safety procedures which are based on identification number, call back procedures, encryption, etc. From legal perspective, these security procedures are required to be recognised by law as substitute for signature. Data integrity, non-repudiation, evidentiary standards, choice of technology, liability standards, contractual freedom, consumer protection, cross border recognition of electronically signed documents are some of the issues related to electronic authentication which are required to be addressed.

Most of the electronic and digital signature initiative fall into three categories - perspective, signature enabling and criteria based.[374]

---

374 Based on material downloaded from the website http://www.doe.gov.in.

Perspective approach - It seeks to enable and facilitate electronic commerce with the recognition of digital signature through a specific regulatory framework. It provides licensing scheme, allocates duties between contracting parties, prescribes liability standard, creates evidentiary presumption and standard for signature or document authentication. 18 states in U.S.A. have considered digital signature law.

Criteria based approach - It provides broader criteria which may apply to digital signature. 11 states in U.S.A. have incorporated the criteria-based approach, among whom California, Indiana, Illinois, New Hampshere, Rhodes Island, Virginia are some whose name can be mentioned.

Signature enabling approach - It permits any electronic mark that is intended to authenticate a writing to satisfy a signature requirement. Massachusetts is representative of this approach.

VI.1. ARIZONA - Arizona Session Laws 1996 provides that Secretary of State shall approve for use by all other state agencies and accept digital signature for document filed with the office of the Secretary of State.[375]

VI.2. CALIFORNIA - California has adopted legislation on digital signature which provides that digital signature shall have the same effect as manual signature, it

---

375 Supra note 374.

(1) it is unique to the person using it

(2) it is capable of verification

(3) it is under the sole control of persons using it

(4) it is linked to data in such a manner that if the data are changed, the digital signature is invalidated.

(5) it conforms to regulations adopted by Secretary of State.

Secretary of State shall license Certification Authorities only for State agencies, State employees and for individuals who will be submitting digitally signed documents to the State.[376]

VI.3. CONNECTICUT - General Statutes of Connecticut has provided direction to Commission of Public Health and Addiction Services to adopt regulation for the use of electronic signature for certain medical records.[377]

VI.4. DILAWARE - Dilaware enacted legislation in 1996 to allow the use of electronic signature with respect to document related to state budget, accounting and pay roll policies and procedures.[378]

---

376 Supra note 374.

377 http://www.mbc.com/legis

378 Id.

VI.5. FLORIDA - Electronic Signature Act 1996 authorises Secretary of State to be Certification Authority to verify electronic signature.[379]

VI.6. IOWA - It permits electronic signature for voter registration form once the State Voter Registration commission shall prescribe by rule the technological requirement for guaranteeing the sanity and integrity of electronic signature.[380]

VI.7. NEW MEXICO - The purpose of Electronic Authentication of Documents Act 1996 was to provide a centralised, public electronic registry for authenticating electronic document by means of private and public key system, promote commerce, facilitate electronic information and document transaction.[381]

VI.8. UTAH - Utah Digital Signature Act was first to authorise commercial use of digital signature. It governs the use of public-private key encryption and Certification Authorities. Certification Authorities are to be licensed by Utah Department of Commerce. The legislation also protects subscriber's private key as property. Utah Senate Bill 1996 provides certification requirements, procedures, duties, performance,

---

379 Supra note 377.

380 Supra note 374.

381 Supra note 377.

audit, investigation, outlines enforcement responsibilities, provides for warranties and obligation of Certification Authorities, specifies signature requirements and presumption in adjudication.[382]

VI.9. VIRGINIA - Trade, Commerce and Digital Signatures 1996 establishes regulatory framework for the use of digitized signature. It provides basis by which individuals and businesses can electronically authenticate business contracts and other agreements exchanged over computer network.[383]

VI.10. WASHINGTON - The object of Washington Digital Signature Act was to facilitate commerce by means of reliable electronic messages, to minimize incidence of forged digital signature and fraud in electronic commerce.[384]

VI.11. GERMAN DIGITAL SIGNATURE LAW, 1997[385]

The Digital Signature Law is a technical law. It does not deal with legal validity of digital signature rather its purpose is to provide condition for secure infrastructure for the use of digital signature in Germany.

---

382 Supra note 377.
383 Supra note 374.
384 Supra note 377.
385 Supra note 377.

The purpose of this law is to create general condition for digital signature under which they may be deemed secure and forgeries of digital signature can be ascertained.[386]

The Act defines digital signature as a seal on digital data created with private signature key, which seal allows to ascertain the owner of the signature key and the unforged character of data by using associated public key.[387]

According to the Act, certificate means a digital attestation concerning the attribution of a public signature key to a natural person to which a digital signature is affixed.[388]

The Act provides that certifier requires license from the authority to operate. The license shall be denied if the applicant does not posses reliability. The reliability depends on the guarantee that it will comply as license-holder with relevant legal requirement. The Authority issues certificate for signature key that are used to sign certificates.[389]

For issuing certificate, the certifier shall reliably identify the person who apply for certificate. It confirms attribution of public signature key

---

386 Sec.1, German Digital Signature Law 1997.
387 Sec.2, German Digital Signature Law 1997.
388 Supra note 387.
389 Sec.4, German Digital Signature Law 1997.

to an identified person by a signature key certificate. Certifier records information regarding applicant's power of representation for third party. The certifies takes measures so that data for certificate can not be forged.[390]

The Act provides that a signature key certificate shall contain name of the signature key owner, attributed public signature key, algorithm with which public key of signature key owner as well as public key of the certifier can be used, number of certificate, beginning and end of certificate's validity, name of the certifier.[391]

A certifier can block a certificate if requested by signature key owner if certificate was issued based on false information. A certifier shall affix a time stamp to digital data upon request.[392]

The Act provides that certifier can collect personal data only from the concerned person and only if it is necessary for the purpose of certificate. This data can be used for other purposes only if it is permitted by this law or other law.[393]

---

390 Sec.5, German Digital Signature Law 1997.

391 Sec.7, German Digital Signature Law 1997.

392 Sec.8, 9, German Digital Signature Law 1997.

393 Sec.12, German Digital Signature Law 1997.

The Authority can take steps with regard to certifier for ensuring compliance with the law. Non compliance with the duty arising under law can be ground for refusing license. The validity of certificate shall be unaffected by withdrawal of a license.[394]

The Federal Government is empowered to promulgate ordinance for necessary implementation of the digital signature system.[395]

VI.12. UTAH DIGITAL SIGNATURE ACT[396]

This Act is to minimize the incidence of forged digital signature, to provide reliable authentication of computer based information, to enable verification of digital signature on compute based document, to facilitate commerce by means of computerised communication.[397]

The Act defines Digital Signature as a sequence of bits which a person intending to sign creates in relation to a clearly delimited message by running the message through a one-way function, then encrypting the resulting message digest using an asymmetrical cryptosystem and the person's private key.[398]

---

394 Sec.13, German Digital Signature Law 1997.
395 Sec.16, German Digital Signature Law 1997.
396 Supra note 377.
397 Sec.46-3-102, Utah Digital Signature Act.
398 Sec.46-3-103(10), Utah Digital Signature Act.

The Act provides that following presumptions are established by digital signature[399] -

1) A certificate is presumed to be an acknowledgement of any digital signature verified using the public key listed in the certificate if the certificate is in the repository and the certificate was not revoked or suspended or expired.

2) A digital signature verified using a public key is presumed to have been affixed with the intention of the subscriber to authenticate the message and to be bound by the content of the message if the public key is listed in a certificate and the certificate was not revoked, suspended or expired.

3) If a signature is time stamped by the division or a recognised repository and unless the message otherwise provides, the time stamp is prima facie evidence that the time stamped signature took effect as of the date and time indicated in the time stamp.

Regarding the effect of digital signature, the Act has provided that a digitally signed document is as valid as if it had been written on paper.[400]

---

399 Sec.46-3-101, Utah Digital Signature Act.

400 Sec 46-3-402, Utah Digital Signature Act.

The Act also provides that a digital signature which would make a negotiable instrument payable to bearer is void unless the digital signature effectuates either a fund transfer or a transaction between banks or other financial institutions.[401]

According to this Act, a licensed certification authority may issue a certificate to a subscriber if[402]

(1) the Certification Authority has received a signed request for issuance of certificate by the prospective subscriber, and

(2) the Certification Authority confirms that the prospective subscriber is the person identified in the request, he bears a distinguished name and he rightfully holds the private key corresponding to the public key to be listed in the certificate.

(3) The Certification Authority confirms that the prospective subscribers hold a key pair capable of fixing a digital signature by the private key corresponding to public key listed in the certificate.

The Act provides that, by accepting certificate, issued by a licensed Certification Authority, the subscriber identified in the certificate

---

401 Sec.46-3-403, Utah Digital Signature Act.

402 Sec.46-3-302, Utah Digital Signature Act.

assume the duty to exercise reasonable care in retaining control of the private key and keeping it confidentially.[403]

The Act provides duty of the licensed Certification Authority in issuing Certificate.[404] By issuing certificate, a licensed Certification Authority warrant subscriber named in the certificate that certificate contains no information known to the Certification Authority to be false. Licensed Certification Authority, in absence of contract to the contrary, can suspend certificate for 48 hours.[405] It can also revoke certificate after reviewing the request of revocation by the subscriber.[406] A certificate expires on the date mentioned in the certificate which is generally three years from the date of issuance.[407]

VI.13. GEORGIA ELECTRONIC RECORDS AND SIGNATURE ACT, 1998[408]

This Act is to promote the development of electronic government and electronic commerce.

---

403 Sec.46-3-303, Utah Digital Signature Act.
404 Sec.46-3-304, Utah Digital Signature Act.
405 Sec.46-3-305, Utah Digital Signature Act.
406 Sec.46-3-306, Utah Digital Signature Act.
407 Sec.46-3-307, Utah Digital Signature Act.
408 Supra note 377.

The Act defines electronic signature as electronic or digital method executed or adopted by a party with the intend to be bound by or to authenticate a record which is unique to the person using it, is capable of verification, is under the sole control of the person using it and is linked to data in such a manner that if the data are changed, electronic signature is invalidated.

This Act also provides that where a person or other entity accepts or agrees to be bound by an electronic record, then any rule of law which requires a record of that type to be in writing shall be deemed satisfied and any rule of law which requires a signature shall be deemed satisfied.

According to this Act, a person whose electronic signature is used in an unauthorised fashion, may recover or obtain any or all of the following against the person who engaged in such unauthorised use provided the use of such electronic signature is an unauthorised fashion was negligent, reckless or intentional - (1) actual damages, (2) equitable relief, (3) punitive damages, (4) reasonable attorney's fee and expenses, (5) any other relief which the court deems proper.

VI.14. SINGAPORE ELECTRONIC TRANSACTION ACT, 1998[409]

This Act provides a framework for the legal recognition and usage of electronic signature, digital signature, electronic records. This is to facilitate electronic commerce, electronic filing of document with government agencies, minimize fraud and forgery in electronic record and to promote the use of electronic signature to give authority to electronically transmitted document. This Act is modelled on UNCITRAL MODEL Law on Electronic Commerce, Illinois Electronic Commerce Security Act and Utah Digital Signature Act.

The Act has defined Electronic signature as any letters, characters, numbers or other symbols in digital form attached to or logically associated with an electronic record and executed or adopted with the intention of authenticating or approving the electronic record.

Regarding the effort of electronic signature, the Act provides that when the law requires a signature or provides for certain consequences if a document is not signed, electronic signature satisfies that rule of law. However, it also provides that electronic signature is not valid for use in wills, negotiable instruments, transactions involving immovable property interest or document of title.

---

409 Supra note 377.

According to this Act, Certification Authorities are to be regulated by an appointed Controller of Certification Authorities who will be responding for licensing, certifying, monitoring certification activities. If a licensed Certification Authority conforms to the requirement of the Act, it shall not be liable for any loss due to reliance on a false or forged digital signature and shall not be liable for any amount in excess of the recommended reliance limit.

VI.15. UNCITRAL MODEL LAW ON ELECTRONIC COMMERCE[410]

This law is a step towards providing a broader idea of legislation on electronic commerce - the area which desperately needs a legal regime because the existing legal framework is unable to adopt electronic commerce system.

Interestingly, this Law clearly mentions the area of its application. It provides that the law applies to any kind of information in the form of data message used in commercial activities.[411] Here the expression "commercial" as matters arising from all relationship of commercial nature, whether contractual or not. Relations of commercial nature includes but not limited to the following transactions - any trade

---

410 Full text of the Model Law is given in ANNEXURE-I.

411 Art.1, UNCITRAL Model Law on Electronic Commerce.

transaction for the supply of or exchange of goods or services, distribution agreement, commercial representation or agency, factoring, leasing, investment, financing, banking, insurance, exploitation agreement, joint venture and other forms of industrial or business corporation, carriage of goods or passengers by air, sea, rail or road.

The law defines 'data message' as information generated, sent, received, stored by electronic, optical or similar means including but not limited to EDI, e-mail, telegram, telex and telecopy.[412]

This law serves a very positive role for facilitating electronic commerce by removing the uncertainty caused by electronic medium of communication. It provides that information shall not be denied legal validity, solely on the ground that it is in the form of data message.[413]

The requirement of existing legal regime to be of certain things in writing, signed and original which stand as obstacle for implementation of electronic commerce are satisfied by this law, if they are in data message form.[414]

---

412 Art.2, UNCITRAL Model Law on Electronic Commerce.

413 Art.5, UNCITRAL Model Law on Electronic Commerce.

414 Art.6, 7, 8, UNCITRAL Model Law on Electronic Commerce.

This law also facilitates electronic commerce by recognising evidential weightage of data message and validity of contract, formed by means of data message.[415]

This law provides that despatch of data message occurs when it enters information system outside the control of originator. The receipt of data message takes place, if addressee has designated an information system then at the time data message enters designated information system, if data message is sent to an information system which is not designated by addressee then at the time when data message is retrieved by addressee, if addressee has not designated an information system then at the time when data message enters information system of the addressee.[416]

To facilitate electronic commerce, the Law recogises that any transport document in case contract on carriage of goods can be in the form of data message.[417]

---

415 Art.9, 11, UNCITRAL Model Law on Electronic Commerce.

416 Art.15, UNCITRAL Model Law on Electronic Commerce.

417 Art.17, UNCITRAL Model Law on Electronic Commerce.

VI.16. INFORMATION TECHNOLOGY BILL, 1998[418]

The object of the Bill is to provide provisions for the security and use of electronic transaction.

The Bill defines "electronic signature" as any letters, characters, number, other symbols in digital form attached to or logically associated with the intention of authenticating or approving the electronic record.[419]

The Bill also defines "digital signature" as electronic signature consisting of a transformation of an electronic record using an asymmetric cryptosystem and a hash function such that a person having the initial untransformed electronic record and the signer's public key, can accurately determine (a) whether transformation was created using the private key that corresponds to the signer's public key and (b) whether initial electronic record has been altered since the transformation was made.[420]

The Bill provides that provisions regarding electronic records, signature and electronic contract will not apply in case of will, negotiable

---

418 Full text of the Bill is given in ANNEXURE-J.

419 Sec.2, Information Technology Bill, 1998.

420 Sec.3, Information Technology Bill, 1998.

instrument, contract for sale of immovable property and interest in such property, conveyance of immovable property, document of title.[421]

According to the Bill, information shall not be denied legal effect, validity or enforceability solely on the ground that it is in the form of electronic record. A duplicate of a computer program or computer data file which is produced by the same impression or in the same matrix or by mechanical or electrical recording, shall be admissible in evidence as original.[422]

The Bill provides that where law requires information to be in writing or signed. This requirement is satisfied by electronic document and electronic signature. Even where law requires certain documents be retained, such requirement can be satisfied by retaining them in electronic form if the document is accessible for subsequent reference and if it is retained in the format in which it was originally generated and if it identifies origin and destination of electronic record and data and time when it was sent and received.[423]

---

421 Sec.4, Information Technology Bill, 1998.

422 Sec.6, Information Technology Bill, 1998.

423 Sec.7, 8, 9, Information Technology Bill, 1998.

According to this Bill, network service provider shall not have civil or criminal liability for any material in electronic form to which it has only provided access if the liability is based on making, publication, dissemination, distribution of such material.[424] This will not affect obligation based on contract or license.

The Bill provides that where electronic record is used in formation of contract, that contract shall not be denied legal validity or enforceability on the sole ground that electronic record is used for this.[425]

The Bill also contains provisions regarding acknowledgement of receipt.[426]

Regarding time and place of despatch and receipt, the Bill provides that, in absence of contract to contrary, despatch of electronic record occurs when the electronic record enters information system outside the control of originator. Receipt of electronic record takes place, in case addressee has designation information system, when electronic record enters that designated information system and if the record is sent to other information system which is not designated then receipt occurs

---

424 Sec.10, Information Technology Bill, 1998.

425 Sec.11, Information Technology Bill, 1998.

426 Sec.14, Information Technology Bill, 1998.

when the addressee retrieves it and if the addressee has no designated information system, receipt occurs when electronic record enters information system of addressee. Unless there is contract otherwise, electronic record is deemed to be despatched and received at a place where the originator and addressee has place of business respectively.[427]

The Bill provides a presumption that in absence of contrary evidence, information listed in a certificate provided by licensed Certified Authority is correct.[428]

According to the Bill, in absence of contrary agreement, if a person relies on digitally signed electronic record, he assumes the risk that digital signature is invalid as a signature to authenticate the content of electronic record if reliance on digital signature is not reasonable.[429]

The Bill provides punishment in terms of fine and imprisonment for publishing certificate for fraudulent purpose or making false request for certificate or suspension, revocation of it.[430]

As per the terms of the Bill, a Certification Authority may issue certificate to a prospective subscriber if it has received a request for

---

427 Sec.15, Information Technology Bill, 1998.
428 Sec.21, Information Technology Bill, 1998.
429 Sec.22, Information Technology Bill, 1998.
430 Sec.25, 26, Information Technology Bill, 1998.

insurance and certification practice statement, complying with all procedures and practices. It also provides for revocation and suspension of certificate by Certificate Authority.[431]

The Bill provides that by accepting certificate issued by Certification Authority, the subscriber assumes a duty to exercise reasonable care to retain control of private key, corresponding to public key listed in the certificate.[432]

The Central Government shall appoint Controller of Certification Authority for the purpose of licensing, certifying, monitoring, overseeing activities of Certification Authority. The Central Government may make regulations for the purpose of ensuring quality of repository and the service they provide.[433]

The Bill provides that any department or ministry of Central Government, State Government, statutory corporation under Central and State Government which accepts filing of document, issue permit or license, provides for method and manner of payment, may do all these in electronic form.[434]

---

431 Sec.29, 31, 32, Information Technology Bill, 1998.
432 Sec.39, Information Technology Bill, 1998.
433 Sec.46, Information Technology Bill, 1998.
434 Sec.47, Information Technology Bill, 1998.

The Bill also confers power to Controller of Certificate Authority to give direction for compliance with the provision of the Act, to investigate and to access to data and computers.[435]

District Court of Magistrate shall have jurisdiction to hear and determine all offences under this Bill and to impose full penalty or punishment.[436]

The Bill, in detail provides situations which amount to computer crime and provides for the punishment for that.[437]

Interestingly, the bill provides that the provisions regarding computer crime shall apply to every body irrespective of nationality, citizenship, place of occurrence of crime whether within India or outside.[438]

The Bill has removed legal impediment regarding evidential weightage of computer output by providing that computer output shall be admissible as evidence if there is no reasonable ground to believe that the computer output is incorrect because of improper case of computer

---

435 Sec.51, 52, 53, Information Technology Bill, 1998.
436 Sec.58, Information Technology Bill, 1998.
437 Sec.63-66, Information Technology Bill, 1998.
438 Sec.67, Information Technology Bill, 1998.

and computer was all along working property.[439] Any certificate identifying computer output and describing the manner in which it was produced, shall also be admitted as evidence.[440]

Proposed amendment in Evidence Act -

- new Sec.67(2) - this section shall not apply in case of electronic record and electronic signature under I.T. Bill.

- new Sec.3(f) - Electronic Document/Data/Record/Data Message information generated, sent, received, stored by electronic, optical, computer or similar means including but not limited to EDI, e-mail, telegram, telex or telecopy.

This same explanation is to be inserted after Sec.63(5) and Sec.74(1)(iii) of Evidence Act[441] and after Sec.29 of Indian Penal Code,[442] Sec.3(18) of General Clauses Act.[443]

---

439 Sec.70, Information Technology Bill, 1998.
440 Sec.71, Information Technology Bill, 1998.
441 Sec.74, Information Technology Bill, 1998.
442 Sec.75, Information Technology Bill, 1998.
443 Sec.76, Information Technology Bill, 1998.

The Bill provides for detailed provision for amendment in Reserve Bank of India Act to implement Electronic Fund Transfer System.[444]

Proposed amendment in Bankers' Book Evidence Act 1891.[445]

Sec.2(3) - bankers' book includes ledgers, day books, account books and other records used in ordinary business of bank whether records are kept in written form or in micro film, magnetic tape, any other form of mechanical or electronic data retrieval mechanism.

Sec.4(2) - Any entry in Bankers' book shall be deemed to be primary evidence of such entry and such bankers' book is document under Sec.62 of Evidence Act.

A notification is required under Sec.58 of R.B.I. Act for EFT system.[446]

The Bill provides for Regulation for Reserve Bank EFT system.

These foreign legislations and India Bill reflect features of law in digital age.

---

444 Sec.77, Information Technology Bill, 1998.
445 Sec.78, Information Technology Bill, 1998.
446 Sec.79, Information Technology Bill, 1998.

Legislation on Digital Signature/Electronic Transaction/Electronic Commerce/Information Technology

Organisation/Country ⇨ Indicator ⇩	Arizona	California	Connecticut	Delaware	Florida	Iowa	New Mexico	Virginia	Washington	Singapore	Georgia	German	Utah	UNCITRAL	India
Def'n of Electronic Signature										✓	✓				✓
Def'n of Digital Signature												✓	✓		✓
Def'n of Certificate												✓			
Def'n of Commercial Activity														✓	
Def'n of Data Message														✓	
Effect of Electronic Signature										✓					
Effect of Digital Signature													✓		
Controller of Certificate Authority					✓					✓					✓
Liability of Licensed Certificate Authority															
Condition for Issuing Certificate												✓	✓		✓
Content of Certificate												✓			
Warranty under Certificate													✓		
Suspension and Revocation of Certificate															✓
Presumption of Digital Signature													✓		
Subscriber's Duty													✓		✓
Recognition of Data Message as Alternative to Paper Document														✓	✓
Requirement of Writing, Signature, Original, Retention to be satisfied in Data Message		✓									✓			✓	✓
Evidential Weightage of Data Message														✓	✓
Time of Despatch and Acceptance of Data Message														✓	✓
Recognition of Transport Document in Data Message														✓	
Liability of Service Provider															✓
Governmental Work in Electronic Record	✓	✓	✓	✓		✓	✓	✓							✓
Forum															✓
Computer Crime															✓
Proposal for Amendment in Existing Laws															✓
Trade and Commerce in Electronic Record							✓	✓	✓	✓					✓

The rapid development of electronic commerce is making a new era of global communication and trade. Electronic commerce has implications for many facets of economic and social life because it has the potential to fundamentally change the way commercial transactions, business of government, delivery of services and host of other interactions conducted. How these changes will impact upon law is to be addressed. The extent to which existing laws needed to be updated to adopt electronic commerce is to be pointed out.

CONCLUSION

A. Principles

B. Policy

C. Recommendation

D. Task Ahead

E. Further Scope of Research

CONCLUSION

The virtues of the Internet revolution have been widely documented in the popular press. Through widely recognized success stories, it is readily exhaled that businesses of every kind have found that communicating through the World Wide Web is a great way to get information to customers/consumers, suppliers, associates or investors. More recently, the focus has been on Internet technology applied internally to organizations. These so-called "intranets" promise to dramatically improve the inner-workings of an organization and fundamentally transform it. To keep pace with competitors, they are now faced with a significantly more complex world of computing processing power and global communications which implies potential new business opportunities and a shifting business paradigm.

To compete in the global marketplace, it is essential for firms to pipeline partners (a concept known as business-to-business marketing) as well as end-use consumers known as consumer-direct or business-to-consumer marketing.

Electronic commerce, an emerging business tool, provides genuine opportunities for both marketing objectives. It is defined as the use of

telecommunications networks for the purpose of linking organizations and/or individuals who engage in some form of computer-mediated commercial trading relationship. Electronic commerce has made major break through in governmental activities through e-governance. The business community is convinced of the importance of this technology as an indispensable tool, but it is also apprehensive about the technology. It needs to better understand how the Internet will impact its market, industry and company and how it can be used as a business tool.

Electronic commerce takes place in a marketplace where all parties involved in a transaction can satisfy their needs electronically. In the past, some technically savvy organizations linked their computer systems with others through private or commercial networks and conducted business electronically. However, this would not qualify as electronic commerce since the electronic business capability was limited to a select group in the market place.

The Internet is making true electronic commerce a reality. It provides an open, ubiquitous, and affordable means to carry out business electronically for all participants in the market. For instance, the Web has embraced into the electronic marketplace many organizations and individuals with little or no technical knowledge and with very limited

resources. An increasing number of companies are establishing a presence on the Web.

Informational use of the Web is the most widely implemented Internet application. Studies indicate that over 90 percent of companies with a Web site use it to provide product and marketing information. Companies can use the Web to provide a variety of information: advertising, marketing, public relations, annual reports, stockholder information and even position announcements. Unlike traditional information media, companies can easily change the content or adjust the level of depth and brandwidth of its information at a moment's notice.

Using the Web to provide product and marketing information is only transitory and companies eventually want to sell products and services directly to customers over the network.

Business community is slowly coming out of the reluctancy of using Internet for transferring money or payment information. Recent development in cryptography and companies like Digicash Inc. and Cybercash Inc. who offer secured digital cash system are mainly responsible for this transformation.

Transactional Webs support customer-direct dealings and other activities that ultimately result in the transfer of money.

Technical concerns, such as the perceived lack of security and arduous connectivity to corporate databases, have only recently been replaced with confidence in electronic commerce proponents. Security had been considered the most troublesome issue for on-line transactions. A great deal of technical progress, such as encryption algorithms, firewalls and electronic fingerprints, has taken place to make the electronic marketplace a safe place to buy and sell.

Certain, unambiguous and well settled legal regime always act as impetus to the growth of business activities. Electronic commerce poses real threat to the existing legal regime as the age-old legal system is no way in a position to adopt electronic commerce. It is high time to realise the implication of electronic commerce on existing legal regime and give a face lift to it by amending the inconsistent laws and enacting new laws.

While rapid development time and low entry cost are the most common lure for initially going on-line, companies should expect and be prepared for changes and impacts that electronic commerce will eventually bring to the market place. The open and global nature of the

(7) To harmonise law governing electronic commerce.

(8) To facilitate cross-border recognition and enforcement of electronic transactions and signatures.

C. RECOMMENDATION

(1) A data message should satisfy any requirement for information to be in writing.

(2) Legislation should give legal effect to electronic signature subject to certain minimum standard.

(3) A provision allowing data message to satisfy requirement for an original should be enacted subject to the requirement about integrity of data message.

(4) A provision is required to deal with admissibility and evidential weight of electronic document.

(5) Record retention requirement should be same for information in paper or electronic form.

(6) Legislation should contain a provision that removes uncertainty regarding the use and validity of data message in contract formation.

(7) The time of dispatch of data message should be the time when the data message entering an information.

(8) For facilitating implementation of electronic commerce, UNCITRAL Model Law on Electronic Commerce should be implemented with immediate effect.

D. TASK AHEAD

1. Steps to transform Information Technology Bill into an Act, as it gives effect to substantial part of UNCITRAL Model Law on Electronic Commerce.

2. Information Technology Bill needs amendment as it is not applicable to negotiable instrument and thus creating obstacle for digitalisation of negotiable instrument.

3. Electronic Document/Data/Record/Data Message - information generated, sent, received, stored by electronic, optical, computer or similar means including but not limited to EDI, e-mail, telegram, telex or telecopy. This same explanation is to be inserted after Sec.63(5) and Sec.74(1)(iii) of Evidence Act and after Sec.29 of Indian Penal Code, Sec.3(18) of General Clauses Act.

4. Bankers' book includes ledgers, day books, account books and other records used in ordinary business of bank whether records

are kept in written form or in micro film, magnetic tape, any other form of mechanical or electronic data retrieval mechanism. This change is required in Sec.2 of Bankers' Book Evidence Act.

5. Any entry in Bankers' book shall be deemed to be primary evidence of such entry and such bankers' book should be regarded as document under Sec.62 of Evidence Act.

6. Sec.4 of Proposed Electronic Fund Transfer Act is required to be brought into force immediately as it prohibits organising, promoting and operating EFT system without prior authorisation of RBI.

7. Sections dealing with consumer protection of Proposed Electronic Fund Transfer Act are required to be enacted.

8. To give effect to following draft bills provided by Shere Committee.

   (a) Draft EFT Act (ANNEXURE - K)

   (b) Draft Amendment to RBI Act (ANNEXURE - L)

   (c) Draft Amendment to Bankers' Book Evidence Act (ANNEXURE - M)

   (d) Draft RBI (EFT) Regulation. (ANNEXURE - N)

9. Amend RBI Act to bring organisations issuing e-cash under control of RBI by asking them to keep an account with RBI so that RBI can keep track of their activity and to make e-cash legal tender.

10. Amend Negotiable Instrument Act to make e-cash negotiable instrument.

11. Amend Trade and Merchandise Marks Act to include service mark.

12. Trade and Merchandise Marks Act needs amendment so that Trademark holder shall get pre-emptive right over domain name.

13. Copyright Act needs overhauling reappearance to control copyright violation over Internet.

14. Indian Telegraph Act needs amendment to implement encryption system as a tool for security and confidentiality.

E. FURTHER SCOPE OF RESEARCH

Implication of Electronic Commerce on other laws like a) Insurance law, b) Data Protection law, c) Securities Transaction law, d) Tax law, specially VAT, e) Competition Law, f) Criminal Law provides further scope of research.

BIBLIOGRAPHY

BIBLIOGRAPHY

A. ARTICLES

1. A.J. Campbell, *Ten Reasons Why Your Business Should Use Electronic Commerce*, BUSINESS AMERICA, May 1998.
2. Aaron Schavey, *Publishing's Future in Electronic Commerce*, BUSINESS AMERICA January 1998.
3. Aaron Schavey, *Retailing Online: Today's Promise and Tomorrow's Opportunity*, BUSINESS AMERICA, January 1998.
4. Achamma C. Chandersekaran, *Education and Training Transformed By Internet - Enabled Electronic Commerce*, BUSINESS AMERICA, January 1998.
5. Amrit Bir Tiwana, *Freedom of Censorship*, INFORMATION TECHNOLOGY, November 1997.
6. Amy Cortese, *The Ultimate Plastic*, BUSINESS WEEK, No.3527, May 19, 1997.
7. Anand Parthasarathy, *Cyber Business: A New Model for the Millennium*, THE HINDU, March 12, 1998.
8. Anand Parthasarthy, *JAVA: Why is the Brew Turning Bitter*, THE HINDU, April 9, 1998.
9. Andrew L. Shaprio, *Privacy For Sale: Peddling Data On The Internet*, NATION, Vol.264, No.24, June 23, 1997.
10. Andy Reinhardt, *Log on, Link up, Save big*, THE ECONOMIC TIMES, Bangalore, June 26, 1998.
11. Anil Balan, *IT Cos Join E-Commerce Bandwagon*, EXPRESS COMPUTER, June 15, 1998.
12. Anil Balan, *Pioneering in Banking Services*, EXPRESS COMPUTER, March 30, 1998.
13. Anil Balan, *Technology Adoption in Banks*, EXPRESS COMPUTER, March 16, 1998.

14. Arnold Picot, *Organisation of Electronic Markets: Contribution from the New Institutional Economics*, THE INFORMATION SOCIETY, Vol.13, No.1, January-March 1997.

15. Arun Natarajan, *Information Technology Act: Spy on the Net?*, BUSINESS LINE, Thursday, January 21, 1999.

16. Atul Salgaonkar, *Profits From E-Commerce*, THE ECONOMIC TIMES, Bangalore, May 14, 1998.

17. Barbara S. Wellbery, *Privacy in the Information Age*, BUSINESS AMERICA, 1998.

18. Belinda Fehlberg, *The Husband, the Bank, the Wife and Her Signature - the Sequel*, THE MODERN LAW REVIEW, Vol.59, 1996.

19. Bharat Kumar, *There is a lot said and little Done About Web Commerce*, THE ECONOMIC TIMES, Bangalore, Tuesday, June 16, 1998.

20. Bharati Rawla, *E-vrything Ultimately Boils Down to E*, THE ECONOMIC TIMES, Bangalore, June 18, 1998.

21. Bill Gates & Michael Dertouzos, *Friction Free Capitalism and Electronic Bulldozers*, SPAN, March-April 1998.

22. Bob Ramanko, *One Must be Innovative to Make E-Commerce Happen*, EXPRESS COMPUTER, July 27, 1998.

23. Bruce D. Harsh, Direct Marketing's Future In Electronic Commerce, BUSINESS AMERICA at 29 (January 1998).

24. Bruce Elliot, *Web Sales Online Marketing and E-commerce are the Future*, EXPRESS COMPUTERS, June 1, 1998.

25. Bruce McAdam, Insurance: In Electronic Commerce a Risk?, BUSINESS AMERICA at 36 (January 1998).

26. C. Rammanohar Reddy, *E-Commerce: Next Frontier of the WTO*, THE HINDU, May 17, 1998.

27. C. William Johnson, *Maritime Transportation: Ocean Carriers Sail the Electronic Sea*, BUSINESS AMERICA, January 1998.

28. Carl R. Jacobson, *How Connecticut Companies Use Internet for Exporting*, BUSINESS AMERICA, January 1998.

29. Chandar Sundaram, *A New Chapter for Electronic Commerce in India*, THE ECONOMIC TIMES, Bangalore, March 25, 1998.

30. Chandra Agnihotri, *Cyber Shopping*, THE ASIAN AGE, July 2, 1998.

31. Chris Jones, *End to End Internet Security Still Depends on Encryption Apps*, INFO WORLD, Vol.19, No.14, April 7, 1997.

32. Connic W. Crook & Ram L. Kumar, *Electronic Data Interchange: A Multi-Industry Investigation Using Grounded Theory*, INFORMATION AND MANAGEMENT, Vol.34, 1998.

33. Correspondent, *E-Commerce Network to be Setup in City*, THE ASIAN AGE, July 28, 1998.

34. D. Linda Garcia, *Networked Commerce: Public Policy Issues in a Deregulated Communication Environment*, THE INFORMATION SOCIETY, Vol.13, No.1, January-March 1997.

35. D. Srilatha, M.K. Shankar, Gunzan Bannerjee, *E-Commerce - is it working*, COMPUTER TODAY, June 1998.

36. David O. Stephens, *Electronic Record Keeping Provisions in International Laws*, RECORD MANAGEMENT QUARTERLY, April 1997.

37. David Vinc, *I Spy*, WORLD EXECUTIVE'S DIGEST, July 1998.

38. Donna L. Hoffman & Thomas P. Novak, *A New Marketing Paradigm for Electronic Commerce*, THE INFORMATION SOCIETY, Vol.13, No.1, January-March 1997.

39. Dr. Alexander Loos, *Electronic Contracting with Suppliers under German Law.*

40. Edwin Diamond & Stephen Bates, *Law and Order Comes to Cyberspace*, TECHNOLOGY REVIEW, October 1995.

41. Eileen Hill, *Intellectual Property Protection and Electronic Commerce*, BUSINESS AMERICA, January, 1998.

42. Ernest D. Plock, *Telemedicine is Emerging as a Cost-Effective Healthcare Alternative*, BUSINESS AMERICA, January 1998

43. Eugene Alford, Air Transport and Travel on the Internet: Flying and Shipping in the Computer Age, BUSINESS AMERICA at 25 (January 1998).

44. Harold Wolbandler, *The Internet and Global Trade*, ELECTRONIC JOURNAL, November 1997.

45. Heather McCabe, *Speed - The New E-Commerce Mantra*, EXPRESS COMPUTER, June 15, 1998.

46. Ian Fletcher, *The Trouble with Bits - First Step in Internet Law*, JOURNAL OF BUSINESS LAWS, July 1996.

47. *Internet*, INFORMATION TECHNOLOGY, October 1997.

48. J. Mare Chittum, *Electronic Authentication Technologies*, BUSINESS AMERICA, January 1998.

49. J. William Gurky, *Good News and Bad News*, WORLD EXECUTIVE'S DIGEST, March 1998.

50. James P. Backhouse, *Security: The Achilles Heel of Electronic Commerce*, SOCIETY, May-June 1998.

51. Jane Merriman, *Old-World Book Shops in Britain face Net Thrust*, THE ASIAN AGE, August 5, 1998.

52. Jeffrey L. Snyder, *U.S. Expert Controls on Encryption Software*, THE JOURNAL OF WORLD INTELLECTUAL PROPERTY, Vol.1, 1998.

53. Jennifer Steinhaver, *Retailers in Cyberspace Find it Lonely Without Customers*, THE ASIAN AGE, April 27, 1998.

54. Jennifer Tallasico, *Information Services and Electronic Commerce*, BUSINESS AMERICA, January 1998.

55. Jenny C. Mccune, *Making Websites Pay*, AMERICAN MANAGEMENT ASSOCIATION INTERNATIONAL, June 1998.

56. John Ashcraft, *Keep Big Brother's Hands Off the Internet*, ELECTRONIC JOURNAL, November 1997.

57. John E. Siegmund, *Entertainment and Electronic Commerce*, BUSINESS AMERICA, January 1998.

58. John Hancock, *Technology*, US BANKER, March 1997.

59. John R. Shuman, *Banking Services: Harness Technology and Come up with a Winning Business Strategy which continues to Serve Public Interest*, BUSINESS AMERICA, January 1998.

60. Jonathan W. Palmer, *Electronic Commerce in Retailing: Differences Across Retail Formats*, THE INFORMATION SOCIETY, Vol.13, No.1, January-March 1997.

61. Joseph J. Cella & John Reed Stark, *SEC Enforcement and the Internet: Meeting The Challenge of the Next Millennium - A program for the Eagle and the Internet*, THE BUSINESS LAWYER, Vol.52, No.3, May 1997.

62. Josh Martin, *Say Goodbye To Bankers' Hours*, MANAGEMENT REVIEW, January 1998.

63. Justin Hibbard, *Utah Harnesses Web*, COMPUTER WORLD, December 23, 1996.

64. Kelvin Childs, *White House and the Internet*, EDITOR AND PUBLISHER, Vol.130, No.28, July 12, 1997.

65. L. Jean Camp & Marvin Sirbu, *Critical Issues in Internet Commerce*, IEEE COMMUNICATIONS MAGAZINE, Vol.35, No.5, May 1997.

66. Larry Irving, *The Risk and Rewards*, ELECTRONIC JOURNAL, November 1997.

67. Larry Marion, *Who's Guarding The Till At The Cybermall*, DATAMATION, Vol.41, No.3, February 15, 1995.

68. Leslie Willcocks, Valerie Graeser, Stephanic Lester, *Cybernomics and IT Productivity: Not Business as Usual*, EUROPEAN MANAGEMENT JOURNAL, Vol.16, No.3, 1998.

69. Linda Harbaugh, *Travel and Tourism Hangs Ten On the Electronic Wave*, BUSINESS AMERICA, January 1998..

70. Louis V. Gerstner, *The Internet Has Come of Age*, ELECTRONIC JOURNAL, November 1997.

71. M. Ganesh, *The Future of Business*, THE ASIAN AGE, June 2 1998.

72. Manish Sharma, *Let's Go E-Shopping*, THE ECONOMIC TIMES, July 23, 1998.

73. Mare Chittum, Professional Services: Knowledge Transfer Redefined Through Electronic Commerce, BUSINESS AMERICA at 38 (January 1998).

74. Mark D. Powell, *Electronic Commerce: An Overview of The Legal and Regulatory Issues*, INTERNATIONAL TRADE LAW AND REGULATION, Vol.3, No.3, June 1, 1997.

75. Mark Hodges, *Is Web Business Good Business?*, TECHNOLOGY REVIEW, Vol.100, No.6, August-September, 1997.

76. Martijn R. Hoogeweegen, Robert J. String, Rene W. Wagenaar, *A Comprehensive Approach to Access The Value of EDI*, INFORMATION AND MANAGEMENT, Vol.34, 1998.

77. Matt Grayson, *The Internet and the Erosion of the State Tax Bases*, SPECTRUM 1998.

78. Michael Adler, Cyberspace, *General Searches and Digital Contraband: The Fourth Amendment and the Net-wide Search*, YALE LAW JOURNAL, Vol.105, 1996.

79. Michael Bryan, *When Does A bank Receive Money?*, JOURNAL OF BUSINESS LAWS, March 1996.

80. Michael Jay Tucker, *The New Money: Transactions Pour Across The Web*, DATAMATION, Vol.43, No.4, April 1997.

81. Michael R. Ogden, *Electronic Power to the People: Who Is Technology's Keeper on the Cyberspace Frontier?*, TECHNOLOGICAL FORECASTING AND SOCIAL CHANGE, Vol.52, 1996.

82. Milton Mucller, *Telecommunications Access in The Age Electronic Commerce: Towards A Third Generation Universal Service Policy*, FEDERAL COMMUNICATIONS LAW JOURNAL, Vol.49, No.3, April 1, 1997.

83. Mohan Padmanabhan, *Electronic Data Interchange: Benefits of Speedy Implementation in Ports and Customs*, BUSINESS LINE, April 13, 1998.

84. Mumbai Bureau, *Credit Card Holders Wary of Internet Deals: Survey*, THE ECONOMIC TIMES, July 19, 1998.

85. N. Richard Werthamer & Susan U. Raymond, *Technology and Finance: The Electronic Market*, TECHNOLOGICAL FORECASTING AND SOCIAL CHANGE, Vol.55, 1997).

86. Neeraj Kaushal, *Economics of E-Commerce*, THE ECONOMIC TIMES, Bangalore, June 17, 1998.

87. New Delhi Bureau, *WTO Estimates $300 bn e-commerce by 2000*, THE ECONOMIC TIMES, Bangalore, April 11, 1998.

88. P.P. Kanthan, *Challenges to Transacting Business on the Net*, BUSINESS LINE, August 8, 1998.

89. Pat Auger & John M. Gallaugher, *Factors Affecting the Adoption of an Internet Based Sales Presence for Small Businesses*, THE INFORMATION SOCIETY, Vol.13, No.1, January-March 1997.

90. Paul Graham, Secrets to Selling on the Web, WORLD EXECUTIVE DIGEST, 43-45 (August 1998).

91. Paul J. Hart & Carol S. Saunder, *Emerging Electronic Partnerships: Antecedents and Dimensions of EDI use from the Supplier's Perspective*, JOURNAL OF MANAGEMENT INFORMATION SYSTEM, Vol.14, No.4, Spring 1998.

92. Pragya Bharati, *Can EDI Provide Solutions for E-Commerce*, EXPRESS COMPUTER, June 15, 1998.

93. Pragya Bharati, *Internet: A Powerful Information Tool*, EXPRESS COMPUTER, March 23, 1998.

94. Pragya Bharati, *Of Firewalls And Security*, EXPRESS COMPUTER, June 29, 1998.

95. Pragya Bharati, *Targeting E-commerce Security*, EXPRESS COMPUTER, May 25, 1998.

96. President Bill Clinton, *Global Partnership for E-Commerce*, ELECTRONIC JOURNAL, November 1997.

97. Probe Features, *Fire Walls - The Foundation of Internet Security*, INFORMATION TECHNOLOGY, September 1997.

98. Reuters, *China Tries E-Commerce to Boost its Exports*, EXPRESS COMPUTER, March 2, 1998.

Reuters, *E-commerce Open to Hackers, Finds Study*, EXPRESS COMPUTER, Bangalore, June 17, 1998.

99. Reuters, *Net Commerce Keeps Inflation Low in US*, THE ECONOMIC TIMES, Bangalore, April 18, 1998.

100. Reuters, *Spot Check for E-Commerce Systems*, EXPRESS COMPUTER, July 27, 1998.

101. Richard Hill, *Electronic Commerce, The World Wide Web, Minitel and EDI*, THE INFORMATION SOCIETY, Vol.13, No.1, January-March 1997.

102. Richard Lardner, *Keys to the Code*, GOVERNMENT EXECUTIVE, Vol.29, No.7, July 1997.

103. Rick Mathieson, *Do You E-Care*, WORLD EXECUTIVE'S DIGEST, July 1998.

104. Rick Mathieson, *Out of the Tornado*, WORLD EXECUTIVE'S DIGEST, May 1998.

105. Rolf T. Wigand, *Electronic Commerce: Definition, Theory and Context*, THE INFORMATION SOCIETY, Vol.13, No.1, January-March 1997.

106. Rolf Weiber & Tobias Kollmann, *Competitive Advantages in Virtual Markets - Perspectives of Information - Based Marketing in Cyberspace*, EUROPEAN JOURNAL OF MARKETING, Vol.32, No.7/8, 1998.

107. Rosham B.M., Ashok N.R., *Cyber banking: Still a Distant Dream*, EXPRESS COMPUTER, June 12, 1998.

108. Samuel O. Maduegbuna, *The Effects of Electronic Banking Techniques on the Use of Paper-based Payment Mechanisms in International Trade.*

109. Special Correspondent, *WTO Study Seen Potential For Electronic Commerce*, THE ECONOMIC TIMES, March 22, 1998.

110. Srinivasan V.S., *All That Makes The Web Tick*, THE ASIAN AGE, June 2 1998.

111. Staff Reporter, *Technology - Shaping the Future of Money*, THE ECONOMIC TIMES, Bangalore, June 11, 1998.

112. Staff Reporter, *The Way the Business Use the Internet*, EXPRESS COMPUTER, March 2, 1998.

113. Staff Reporter, *E. Business Can Change Your Business*, THE ASIAN AGE, June 2 1998.

114. Stephen J. Kobrin, *Electronic Cash and the End of National Markets*, FOREIGN POLICY, Summer, 1997.

115. *Survey: Online Commerce*, THE ECONOMIST, Vol.343, No.8016, MAY 10, 1997.

116. T.S. Subramaniyam, *Computer Fraud*, EXPRESS COMPUTER, February 16, 1998.

117. T.S. Subramaniyam, *E-Commerce Open to Hackers, Finds Study*, EXPRESS COMPUTER, June 26, 1998.

118. T.S. Subramaniyam, *Hacking the Bank*, EXPRESS COMPUTER, February 23, 1998.

119. Tanya Clark, *Asia Wobbles onto the Web*, INDUSTRY WEEK, Vol.246, No.8, April 21, 1997.

120. Terence Green, *Beyond Electronic Commerce*, EXPRESS COMPUTER, April 6, 1998.

121. Terry Brock & Chaim Yudkowsky, *Purchasing Books Online is Easy, Convenient and Fun*, DALLAS BUSINESS JOURNAL, Vol.20, May 30, 1997.

122. V. Raman Kumar, *Tele Commuting: The Future Work Force*, THE HINDU, June 6, 1998.

123. Vic Sussman & Kenan Pollack, *Gold Rush in Cyberspace*, SPAN, April-May 1996.

124. Vice President Al Gore, *A Market for Just About Anything*, ELECTRONIC JOURNAL, November 1997.

125. Vicki Allen, *US Senate Moves to Knock Gambling off the Net*, THE ECONOMIC TIMES, Bangalore, July 26, 1998.

126. Vinton Cerf, *New Products, Services Needed*, ELECTRONIC JOURNAL, November 1997.

127. Web Vision News Team, *Chennai Serves As Sterling's E-Commerce Note*, EXPRESS COMPUTER, June 1, 1998.

128. Werksmans Attorneys, *The South African Business Guide to Internet Law.*

129. William Daley, *Cooperation Needed,* ELECTRONIC JOURNAL, November 1997.

130. William M. Daley, *The Administration's Position on Electronic Commerce,* BUSINESS AMERICA, January 1998.

B. BOOKS

1. AN INTRODUCTION TO ELECTRONIC MONEY ISSUES (U.S. Department of Treasury, 1996).

2. ANU ARORA, ELECTRONIC BANKING AND THE LAW (Banking Technology, London, 1993).

3. CLIVE GRINGRAS, THE LAWS OF THE INTERNET, (Butterworths, London, 1997).

4. DANIEL C LYNCH & LESLIE LUNDQUIST, DIGITAL MONEY, (John Wiley and Sons Co. 1996).

5. DIANA FAEER, SHIPPING DOCUMENTS AND EDI (Computer and Law, Indira Carr, Katherine Williams, eds., Intellect, Oxford, England, 1994).

6. DICTIONARY OF INFORMATION TECHNOLOGY, 1989.

7. DON TAPSCOTT, THE DIGITAL ECONOMY: PROMISE AND PERIL IN THE AGE OF NETWORKED INTELLIGENCE (Mc Graw-Hill, 1995).

8. EDWARD L. RUBIN & ROBERT COOTER, THE PAYMENT SYSTEM: CASES, MATERIALS AND ISSUES (American Casebook Series, West Publishing Co., 1989).

9. GROUP OF TEN, ELECTRONIC MONEY: CONSUMER PROTECTION, LAW ENFORCEMENT, SUEPRVISORY AND CROSS BORDER ISSUES (Bank for International Settlements, 1997),
URL http://www.bis.org/publ/gent.htm

10. INDIRA CARR, KATHERINE WILLIAMS, COMPUTER AND LAW (Intellect, Oxford, England, 1994).

11. INFORMATION SECURITY AND PRIVACY IN NETWORK ENVIRONMENT, (Office of Technology Assessment, Congress of U.S. 1994).

12. LEN KEELER, CYBER MARKETING (American Management Association, 1995).

13. LILIAN EDWARDS & CHARLOTTE WAELDE, LAW AND THE INTERNET, (Hart Publishing, Oxford, 1997).

14. LOUIS W. STERN & PATRICK J. KAUFMANN, ELECTRONIC DATA INTERCHANGE IN SELECTED CONSUMER GOODS INDUSTRIES: AN INTERORGANISATIONAL PERSPECTIVE, (Marketing In An Electronic Age, Robert D. Buzzel, ed., Harward Business School, 1985).

15. MARTIN NEMOZOW, BUILDING CYBERSTORES: INSTALLATION, TRANSACTION PROCESSING AND MANAGEMENT (McGraw-Hill, 1997)

16. MICHAEL CHISSICK & ALISTAIR KELMAN, ELECTRONIC COMMERCE: LAW AND PRACTICE, (Sweet and Maxwell, London, 1999).

17. NEIL BARRETT, THE STATE OF CYBERNATION.

18. NET GENESIS CORPORATION, BUILD A WORLD WIDE WEB COMMERCE CENTER: PLAN, PROGRAM AND MANAGE INTERNET COMMERCE FOR YOUR COMPANY (John Willey, 1996).

19. P. SADANANDAN & R. CHANDRASEKAR, INFORMATION TECHNOLOGY FOR DEVELOPMENT (Tata McGraw-Hill Publishing Co. Ltd., New Delhi, 1987).

20. PARAS RAM, EXPORT-IMPORT CORRESPONDENCE AND ELECTRONIC MESSAGING (Anupam Publishers, 1998).

21. PETE LOSHIN & PAUL A. MURPHY, ELECTRONIC COMMERCE (Jaico Publishing House, 1998).

22. PETER G.W. KEEN & CRAIGG BALLANCE, ON-LINE PROFITS: A MANAGER'S GUIDE TO ELECTRONIC COMMERCE (Harvard Business School Publishing, 1997).

23. PETER GARDNER, ELECTRONIC TRADING - A PRACTICAL HANDBOOK (Butterworth Heinemann, 1994).

24. RATANLAL & DHIRAZLAL, THE LAW OF EVIDENCE (Wadhwa and Company, 19th ed., 1997).

25. RAVI KALAKOTA & ANDREW WHINSTON, ELECTRONIC COMMERCE: A MANAGER'S GUIDE (Addison-Wesley) 1997.

26. RAVI KALAKOTA & ANDREW WHINSTON, READINGS IN ELECTRONIC COMMERCE (Addison-Wesley) 1997.

27. ROBERT A. PATERSON, ELECTRONIC MARKETING AND THE CONSUMERS 12 (Sage Publication, 1997).

28. ROBERT D. BUZZEL, MARKETING IN AN ELECTRONIC AGE (Harvard Business Schools, 1985).

29. SERGEJ H. KATUS, THREE TYPES OF CONTRACT, (Computer and Law, Indira Carr & Katherine Williams, eds., Intellect, Oxford, England, 1994).

30. TED HAYNES, THE ELECTRONIC COMMERCE DICTIONARY: THE DEFINITIVE TERMS FOR DOING BUSINESS ON THE INFORMATION SUPER HIGHWAY (Robleda Company, 1995).

31. THE BLUE BOOK: A UNIFORM SYSTEM OF CITATION, (The Harvard Law Review Association, 1997).

32. THE NEW ENCYCLOPAEDIA BRITANNICA (Chicago University Press, 1991).

33. VENKATESH IYER, INDIAN CONTRACT ACT, (Asian Law Book House, Hyderabad, 1982).

34. VIJAY AHUJA, SECURE COMMERCE ON THE INTERNET (Academic Press, 1996).

35. VINCY EMERY, HOW TO GROW YOUR BUSINESS ON THE INTERNET (Coriolis Group Books, 1996).

36. WEERAMANTRY C., SLUMBERING SENTINEL - LAW IN THE WAKE OF SCIENTIFIC AND TECHNOLOGICAL DEVELOPMENT (Penguin Publication, London, 1983).

C. FOREIGN LEGISLATIONS

1. Arizona Sessions Law, 1996
2. Banking Act, 1987
3. Bill of Exchange Act, 1882
4. California Digital Signature Law, 1996
5. Civil Evidence Act, 1995
6. Commercial Documents Evidence Act, 1939
7. Companies Act, 1985
8. Copyright, Design and Patent Act, 1988
9. Florida Electronic Signature Act, 1996
10. Georgia Electronic Records and Signature Act, 1998
11. German Digital Signature Law, 1997
12. Interpretation Act, 1978
13. Law of Property (Miscellaneous Provisions) Act, 1989
14. Law of Property Act, 1925
15. Marine Insurance Act, 1906
16. New Maxico Electronic Authentication of Documents Act, 1996
17. Singapore Electronic Transaction Act, 1998
18. Sale of Goods Act, 1979
19. Supply of Goods and Services Act, 1982
20. Torts (Interphase with Goods) Act, 1939.
21. Utah Digital Signature Act, 1996
22. Verginia Trade, Commerce and Digital Signature Laws, 1996

D. INDIAN LEGISLATIONS

1. Bankers' Book Evidence act, 1891
2. Banking Regulation Act, 1949

3. Central Excise and Salt Act, 1944
4. Companies Act, 1956
5. Copyright Act, 1957
6. Customs Act, 1962
7. Foreign Exchange Regulation Act, 1973
8. General Clauses Act, 1897
9. Indian Contract Act, 1872
10. Indian Evidence Act, 1872
11. Indian Penal Code, 1860
12. Information Technology Bill, 1998
13. Negotiable Instruments Act, 1881
14. Reserve Bank of India Act, 1934
15. Sale of Goods Act, 1930
16. Telegraph Act, 1885
17. The Coinage Act, 1906
18. Trade and Merchandise Marks Act, 1958
19. Transfer of Property Act, 1882

E. INTERNATIONAL CONVENTIONS AND MODEL LAWS

1. Brussels Convention on Jurisdiction and Enforcement of Judgment in Civil and Commercial Matters, 1968
2. INCOTERM, International Chamber of Commerce, 1990
3. Rome Convention on Choice of Law, 1980
4. UN Conventions on the Carriage of Goods by Sea, 1978
5. UNCITRAL Model Law on Electronic Commerce, 1986
6. Uniform Commercial Code, 1988

F. REPORTS AND PROJECT PAPERS

1. Dinesh Singh, *Electronic Commerce - Contractual Aspects,* (unpublished MBL Project Paper, National Law School of India University).

2. Dr. N.L. Mitra, *Amendment To Banking Laws: Policy Paper 2,* National Law School of India University, 1998.

3. Dr. N.L. Mitra, *Electronic Fund Transfer: Policy Paper 1,* National Law School of India University, 1998.

4. *Electronic Commerce for Better Business,* Satyam Infoway Limited.

5. *Kickstart Your Way To Miracles With E-Commerce,* Satyam Infoway Limited.

6. M.B. Lobo, *Computer Fraud in Banks* (unpublished MBL Project Paper, National Law School of India University).

7. *Report of Conference on E-Commerce,* Confederation of Indian Industries, February 19-20, 1998.

8. *Report of Electronic Commerce Ad hoc Working Group of Compilation of List of International Organisations and Activities in Relation to Electronic Commerce,* December 5, 1997.

9. Report of Special Studies 2, *Electronic Commerce and The Role of WTO,* World Trade Organisation, 1998.

10. *Report of the Committee For Proposing Legislation on Electronic Fund Transfer And Other Electronic Payment,* Reserve Bank of India, January 1996.

11. *Report of The Legal Working Group,* TRADE/CEFACT.

12. *Report of the Working Group on Electronic Commerce,* U.N. Commission on International Trade Law, 32nd Session, Vienna, May 17-June 4, 1999, U.N. Doc.A/CN 9/457 (1999).

13. *Report on Clinton Administration's Framework for Global Electronic Commerce,* White House, July 1, 1997, URL-http://www.iift.nist.gov/ elecomm/ecomm.htm

14. Siddharth Gyaltsen, *Electronic Fund Transfer, An Agenda For Legal Regime* (unpublished Project Paper, National Law School of India University).

15. Trystan C.G. Tether, *Contracting on the Internet, IBC Conference Report*, January 28, 1998.

16. *UN/EDIFACT: A National Implementational Plan*, TRADE/CEFACT.

G. UNIFORM RESOURCE LOCATOR

1) *Asia Pacific Economic Cooperation*, http://www.apecsec.org.sg http://www..apec-wg.com (Telecommunication Working Group) http://www.apec-wg.com/busf-sg/bus-f1sg.htm (Business Facilitation Group)

2) *Canadian Information Highway Advisory Council*, http://www.strategies.is.gc.ca/ssg/iho1015 e.html

3) *Canadian Radio-television and Telecommunications Commission*, http://www.crtc.gc.ca.

4) *Computer Professionals for Social Responsibility*, http://www.snyside.sunnyside.com/home.

5) *Computer Security Resource Clearing House*, National Institute of Standards and Technology, http://www.csrc.nist.gov

6) *Cyberlaw Series*, Department of Electronics, http://www.doe.gov.in

7) *Cyberspace Law*, http://www.cli.org/x0025-LBFIN.html

8) *Data Interchange Standards Association*, http://www.disa.org

9) *Directory of Federal and State Institutions Accessible on the Internet*, http://www.iid.de/service/bundeslinks-e.html

10) *Documents Centre: Government Resources on the Web*, http://www.lib.umich.edu/libhome/Documents.center/index.html

11) *Doing business with an "e"*, http://www.ibm.com/e-business/what

12) *Electronic Commerce - An Introduction*, http://www.cordis.1u/esprit/src/ecomint.ht

13) *Electronic Commerce - Continue the Dialogue,* http://www.atp.nist.gov/hypernews/ec-collab.ht

14) *Electronic Commerce and Digital Signature Legislations,* http://www.mbc.com/legis/table 02.

15) *Electronic Commerce and EDI,* http://www.unbsj.ca/library/subject/edi.htm

16) *Electronic Commerce and the European Union,* http://www.ispo.cec.lc/Ecommerce

17) *Electronic Commerce in the National Information Infrastructure,* Corporation for National Research Initiatives, http://www.xiwt.org/XIWT/documents/Ecomm-doc/Ecomm TOC2.html

18) *Electronic Commerce Information Resource,* http://www.year-x.co.uk/ec/yxwhatis.htm

19) *Electronic Commerce Page,* http://www.ntia.doc.gov/opadhome/ecom.html

20) *Electronic Commerce Resource Centre,* http://www.ecrc.etc.com

21) *Electronic Commerce Resource Guide,* http://www.premenos.com/Resources/main.html

22) *Electronic Commerce, Law and Information Policy Strategies,* http://www.ose-edu/edips

23) *Electronic Commerce/EDI Handbook,* http://www.ntis.gov/standards/pa 834.htm

24) *Electronic Commerce/Electronic Data Interchange,* http://www.nafta.net/ecedi.htm

25) *Electronic Commerce: Has Conventional Wisdom Changed? Arthur D. Little Hosts On-Line Survey to Find Out Businesses,* http://www./NA.Get Story? story-p 0622101.000 & date = 19980623 & level 1 = 46510 & level2 = 46519 & level 3 = 76/23/98.

26) *Electronic Privacy Information Centre,* http://www.epic.org/crypto

27) *Electronic Signatures and Records: Legal, Policy and Technical Considerations*, Legislative and Policy Work Group of the Information Security Committee of the American Bar Association, http://www.abanet.org/scitech/ec/isc/stateds.html

28) *Emergence of Electronic Commerce on the Internet*, http://www.usc.edu/dept/ATRIUM/Papers/EC_on_the_Inet.html

29) *European Documentation Centre*, http://www.uni-mannheim.de/users/ddz/edz/eedz.html

30) *European Union Home Page*, http://www.s700.uminho.pt/ec.html

31) *Foreign Investment in Emerging Markets*, http://www.ipanet.net

32) *Framework for Global Electronic Commerce*, http://www.iift.nist.gov/eleccomm/ecomm.htm

33) *Free Trade Area of the America*, http://www.ftaa-alca.org

34) *G7*, http://www.diplomatic.fr/actual/g7 lyon/index.gb.html

35) *Initiative Informations gesellschaft Deutschland (Initiative Information Society, Germany)*, http://www.iid.dc.

36) *Internet Privacy Coalition*, http://www.privacy.org/ipc

37) *Internet Tax Freedom Bill*, http://www.legislate.com/xp/p-daily/i-current/a-895193212 article.view

38) *Japan Information Access Project*, http://www.nmjc.org/jiap

39) Jeffrey B. Ritter, *Facilitating Interoperability and Electronic Commerce*, http://www.atp.nist.gov/elec-com/interop/ritter.htm

40) Law and Orders - The Rise of Law in Cyberspace http://www.ssrn.com/update/lsn/cyberspace/lessons/contr01.html

41) *Lawrence H. Summers, Deputy Secretary, Department of Treasury, United States*, http://www.treas.gov/treasury/ press/ pr 052297a.html.

42) *Massachusetts Electronic Records and Signatures Act*, http://www.magnet.state.ma.us/itd/legal/mersa.htm

43) *Mid-America Payment Exchange*, http://www.mpx.org

44) *National Automated Payment Association*, http://www.napanic.org/index.html

45) *Price Waterhouse Predicts Explosive E-Commerce Growth*, http://www.internetnews.com/ec-news/1998/03/2601-pw.html

46) *Software Publishers Association*, http://www.spa.org

47) *Special Issue on Electronic Commerce*, http://www.usc.edu/dept/anninberg/vol1/issue 3/vol 1 no 3.html

48) Steward A. Baker, *International Developments Affecting Digital Signatures*, October 1997, http://www.steptoc.com/web.doc.nst/law+s+The+Net-All/All

49) *Telecom Information Resources on the Internet*, http://www.spp.umich.edu/telecom-info.html%od

50) *The American Telemedicine Association*, http://www.atmeda.org/index.html

51) *The Association for Electronic Commerce Professionals International Inc.*, http://www.acepii.com

52) *The Attention Economy and the Net*, http://www.first monday.dk/issues/issue 2-4/goldhaber/index.html

53) *The Centre for Democracy and Technology*, http://www.edt.org

54) *The Centre for Media Education*, http://www.cme.org

55) *The Coalition of Service Industries*, http://www.uscsi.org

56) *The Department of State*, http://www.state.gov

57) *The Global Internet Liberty Campaign*, http://www.gile.org

58) *The Organisation for Economic Cooperation and Development*, http://www.occd.org

59) *The President's Message to Internet Users*, http://www.Whitehouse.gov/WH/New/Commerce/message.htm

60) *The Recreational Software Advisory Council,* http://www.rsac.org

61) *The U.S. House of Representatives Internet Law Library,* http://www.law.house.gov

62) *The White House Framework for Global Electronic Commerce,* http://www.whitehouse.gov/WH/New/Commerce/read.html

63) *U.S. Department of Commerce* -
http://www.doc.gov/ecommerce
http://www.ita.doc.gov/itahome.html (International Trade Administration)
http://www.ita.doc.gov/industry/osi.html (Service Industry and Finance)
http://www.nist.gov (National Institute of Standard and Technology)
http://www.doc.gov/ecommerce (Secretariat for Electronic Commerce)
http://www.ntia.doc.gov (National Telecommunication and Information Administration)
http://www.uspto.gov (Patent and Trade Mark Office).

64) *U.S. Government Statistics,* http://www.fedstats.gov

65) *U.S. International Trade Statistics,* http://www.census.gov/foreign-trade

66) *Uniform Code Council, Inc.,* http://www.uc-council.org

67) *United Nations Commission on International Trade Law,* http://www.un.or.at/uncitral

68) *United States Trade Representative,* http://www.ustr.gov

69) *Utah Digital Signature Development Program,* http://www.commerce.state.ut.us/webcommerce/digsig/dsmain.htm

70) *Web Commerce: A Tempting Target for Tax Collectors,* http://www.house.gov/cox/Nettax/web.commerce.htm

71. *World Trade Organisation,* http://www.wto.org.

ANNEXURES

ANNEXURE- A

Table 2: Access to the Telecommunication Infrastructure, Selected Countries, 1996[1]

Country	Telephones per 100 inhabitants	Fax per 100 inhabitants	Cable TV per 100 households	Personal computers per 100 inhabitants	Internet hosts per 100 inhabitants
Industrialized countries:					
Australia	49.5	2.5	....	21.2	2.81
Canada	57.5	2.4	....	19.0	2.01
Finland	55.3	2.4	27.0	18.1	5.52
France	54.7	2.7	3.0	15.1	0.42
Germany	48.3	1.8	31.0	18.2	0.87
Italy	42.9	2.2	....	9.2	0.26
Japan	47.8	6.8	....	12.8	0.59
Netherlands	50.9	2.9	84.1	23.2	1.74
Sweden	68.3	3.4	43.0	21.3	2.61
United Kingdom	48.9	2.4	2.0	18.0	1.00
United States	59.5	7.3	59.0	36.4	3.80
Developing and transition countries:					
Argentina	14.1	0.1	....	2.4	0.04
Brazil	7.4	....	....	1.8	0.05
Chile	11.0	....	....	3.7	0.10
China	2.3	0.0	....	0.3	0.00
Hong Kong, China	54.0	4.3	....	15.1	0.78
India	1.1	0.0	....	0.2	0.00
Indonesia	1.3	0.0	....	0.5	0.01
Korea (Rep. of)	39.5	0.8	....	13.2	0.15
Mexico	9.2	....	....	2.9	0.03
Poland	13.1	0.1	....	3.6	0.14
Russia	16.2	0.0	....	2.4	0.05
Singapore	45.5	....	....	21.7	0.95
South Africa	9.1	0.2	....	3.9	0.24
Turkey	20.1		....	1.4	0.02
Selected country groups:					
EU	47.6	2.2	20.5	15.1	0.79
OECD	44.6	3.5	....	18.1	1.43
Non-OECD	....	....	....	0.8	0.02
WORLD	11.5	0.7	....	4.3	0.28

[1] Or closest year available.

Sources: ITU, "Challenges for the Network", 1997a; OECD, "Information Infrastructures: Their Impact and Regulatory Requirements", 1997a; UNDP, "UN Human Development Report", 1997.

ANNEXURE-B

Table 1.1. Technical Innovations Very Likely 1967–2000

Inexpensive design and procurement of "one of a kind" items through use of computerized analysis and automated production [mass customization!]
Extensive and intensive centralization (or automatic interconnection) of current and past personal and business information in high-speed data processors [databases/legacy systems!]
Automated universal (real time) credit, audit and banking systems [ATMs!]
Simple inexpensive home video recording and playing
Inexpensive high-capacity, worldwide, regional, and local (home and business) communication (perhaps using satellites, lasers, and light pipes) [fiber optics!]
Practical home and business use of "wired" video communication for both telephone and TV (possibly including retrieval of taped material from libraries or other sources) and rapid transmission and reception of facsimiles (possibly including news, library material, commercial announcements, instantaneous mail delivery, other printouts, and so on)
Pervasive business use of computers for the storage, processing, and retrieval of information
Shared time (public and interconnected?) computers generally available to home and business on a metered basis
Other widespread use of computers for intellectual and professional assistance (translation, teaching, literature search, medical diagnosis, traffic control, crime detection, computation, design, analysis and to some degree as intellectual collaborator generally)
Personal "pagers" (perhaps even two-way pocket phones) and other personal electronic equipment for communication, computing, and data processing [cell phones!]
Direct broadcasts from satellites to home receivers
Inexpensive (less than $20), long lasting, very small battery operated TV receivers
Home computers to "run" household and communicate with outside world
Inexpensive (less than one cent a page), rapid high-quality black and white reproduction; followed by color and high-detailed photography reproduction—perhaps for home as well as office use
Conference TV (both closed circuit and public communication system)

Source: Adapted from Kahn and Wiener (1967), *The Year 2000,* New York, NY: The Macmillan Company, pp. 52–56.

Table 1: Electronic Commerce: Features of Main Instruments

	Elements of commercial transaction		Technical Features			Ease of Access				
	Elements which can be conducted	One versus multi step transaction[1]	Type of data transmitted	"Interactive" potential	Communication potential	Start-up costs for "consumers"	Operating costs for "consumers"	Start-up costs for "producers"	Capacity (band-width) problems	User-friendly
Standard telephone	(Production), advertising, purchasing, payments, (distribution)	Multi[2]	Voice[3]	Yes	one-one[4]	Low (phone + connection charge)	Depends on phone charges	Low (phone) + connection charge)	No issue	Yes
Facsimile	Advertising, purchasing, payments, distribution	Multi	Data/text, image	No	one-one[5]	Moderate (fax machine + connection charge)	Depends on phone charges	Moderate (fax machine + connection charge)	No issue	Yes
Television	Advertising, consumption, (payments)[6]	Multi	Voice, image	No	one-many	Moderate (television + possible connection charge)	Low	High (studio, equipment, etc.)	No issue	Yes
ATM, credit + debit cards, smart cards	Payments	Multi	Data/text	No	one-one	Low (card)	Low (free or small fee)	Moderate to high (ATM machine, agio)	No issue	Yes
Electronic data interchange (EDI)[7]	Advertising, purchasing, payments	Multi	Data/text	No[8]	one-one one-many	High (equipment + various connection costs)	Depends on line charges	High (equipment + various connection costs)	Potential bottlenecks in combination with Internet	No
Internet and online services	Production, advertising, purchasing, payments,[9] distribution	One or multi	Data/text, image, voice (= multi media)	Yes	one-one one-many many-many	Moderate (PC, modem, possible connection charge)	Depends on line and service charges	Significant one-off costs for website (but typically lower than "real" shop)[10]	Potential bottlenecks	Not yet always

[1] Advertising, purchase, payment and distribution possible in one step.
[2] One-step transactions are possible, e.g. in telephone banking. More sophisticated phone applications are emerging, including telephone conferencing, video conferencing and data transmission.
[3] Telephone video conference allows image transmission.
[4] Telephone conferences and telephone video conferences allow communication from one to many people.
[5] Can also be one-many, e.g. via fax mailing lists.
[6] For example, video channels in hotels.
[7] Traditional EDI with own "hub and spoke" network.
[8] But automatic quasi-interactive transactions possible.
[9] Today mostly in combination with credit card.
[10] Technology integration, e.g., with existing payment systems, in banking, can be costly too.

ANNEXURE-C

Table 7.1. Electronic Connections between Retailers and Customers: Examples by Medium and Type of Customer Connection

ANNEXURE - D

Electronic Medium	Types of Customer Connections					
	Product and Store Information	Answer Customer Queries	Refer to Other Media	Persuasive or Image Advertising	Purchase Transactions	Feedback and Market Research
• World Wide Web (WWW)	Amazon Books, AA, Delta Airlines	Powell's Bookstore	PBS posts transcripts of TV specials; MS/NBC	Samsung on Yahoo	Best Western Hotels	*Communications Week*: on-line subscription qualif.
• On-line services	Public libraries	Compaq: user support over Compuserve		BofA cosponsors startup disk with AOL	Many vendors on AOL, Compuserve	
• Electronic kiosks; Arcade games	Ikea, Nordstrom, Barnes & Noble		Mall games refer to game reviews on WWW			
• Phone/voice-based info services	Radio stations: free cellular calls	800 numbers	AT&T links WWW and telephone	Telemarketing		Phone surveys, viewer polls
• Pagers/Beepers				Pepsi		
• CD-ROM			Bill Gates' *The Road Ahead* refers to MS s/w products			
• Television/Radio	Local video networks beamed to food court		Toyota: URL on TV ads; NPR Music Resource	Almost all retailers		
• ATM Machines		Banks			Visa, MC, Amex	
• Video Phones/ Conferencing, Whiteboards	Netframe					
• Agents	Bargainfinder					E-mail surveys
• E-mail, Usenet, Listservs		B&Bs			Idealist	
• Virtual Reality	Virtual "walk-thru" real estate properties					
• Smart Cards, Digital Signatures, Electronic Wallets				Phone cards	Phone cards, debit cards	

Continued

Electronic Medium	Types of Customer Connections					
	Increased Selection	Frequent/Preferred Buyer Clubs	Connect Customers with Each Other	Contests/ Tie-ins	Personal Shopping Services	Ameliorate Waiting Time
• World Wide Web (WWW)	Music Boulevard	Lexus	GM Saturn Division	KVO's "Where's Pierre"	Nordstrom	AA, Delta
• On-line services		Easy-SABRE				
• Electronic kiosks; Arcade games		Valley View Center Smart Shoppers Club (Dallas)				
• Phone/voice-based info services				900 numbers		
• Pagers/Beepers				Pepsi, Videoland beeper giveaways		Restaurants beep when table is ready
• CD-ROM						
• Television/Radio						Warner, Disney stores
• ATM Machines						All banks
• Video Phones/ Conferencing, Whiteboards			NetFrame			
• Agents						
• E-mail, Usenet, Listservs			Newsgroups for users of product X			
• Virtual Reality						
• Smart Cards, Digital Signatures, Electronic Wallets						Phone cards: "No fumbling for change"

ANNEXURE-E

MORE ABOUT VV

- Press Clippings
- Awards
- Accolades
- Jobs At Virtual Vineyards

SHOP SERVICES

- Sign In
- Create a New Account
- View Shopping Cart
- Site Help
- Change Shipping Destination
- About Virtual Vineyards
- Contact Us
- Shipping Information

Join the Affiliate Network

WHAT'S NEW AT VIRTUAL VINEYARDS

Busy, busy, busy! Here are recent additions to our evolving portfolio. Looking for something not so new? Take a look at the What's New archives. Remember too, that all wines get a ten percent discount on twelve or more bottles.

Pinot Noir is perhaps the most sensual of red wine grapes. This sampler includes three fine Pinots, one from Mendocino County, one from Santa Barbara County and one from, of all places, New Zealand's South Island. *2/1/99*

- Heavenly Pinot *$56.00*

Few wines are as irresistable as the fine dessert wines of the world, and few are as seductive. This sampler includes three of our current favorites, two from France and one from California. *2/1/99*

- Sweet on You *$55.00*

No wine has been as long associated with romance as Champagne. This sampler includes three fine bubblies, one from Limoux in Southern France, one from Champagne, and one from California's Sonoma County. *2/1/99*

- Bubble Your Pleasure *$52.00*

The "nose" (fancy wine geek word for smell ;>) on this lovely, crisp white wine reminded me of ripe comice or bartlett pears... *1/29/99*

- 1997 Willakenzie Estate Pinot Gris, Willamette Valley *$14.95*

Bright, red berry flavors and moderate tannins make up the signature of this dependable red. A real crowd pleaser. *1/29/99*

- 1995 Robert Mondavi "Coastal" Zinfandel, North Coast *$10.50*

Sauvignon Blancs from Marlborough are famous for their assertive, zippy personality, and this wine is a perfect exemplar of the style. *1/20/99*

- 1998 Allan Scott Sauvignon Blanc, Marlborough, New Zealand *$13.95*

A medium-bodied, juicy Chardonnay with bright pineapple/citrus fruit and a kiss of sweet oak. The quality of Marlborough grapes really shines! *1/20/99*

- 1997 Allan Scott Chardonnay, Marlborough, New Zealand *$14.95*

This charming Riesling delivers a mouthful of stone fruit and lime zest flavors with a crisp, refreshing finish. Pretty hard to resist! *1/20/99*

MORE ABOUT VV
- Press Clippings
- Awards
- Accolades
- Jobs At Virtual Vineyards

SHOP SERVICES
- Sign In
- Create a New Account
- View Shopping Cart
- Site Help
- Change Shipping Destination
- About Virtual Vineyards
- Contact Us
- Shipping Information

Join the Affiliate Network

HOW TO ORDER

This guide lets you know what to expect when you place an order and helps you streamline the process. You might want to print this page so that you can refer to it as you are ordering.

Creating a Personal Account

You can streamline ordering by creating an account with us. There are many benefits to having an account (and it's free):

- When you sign in to your account before placing an order, your billing and shipping information will automatically appear on the order form.
- You can keep credit card information securely on file with us to expedite ordering.
- You can review your purchase history and enter your own tasting notes for future reference.
- You can keep a list of friends and business associates and their addresses on file for easier gift giving.

Of course, having an account is completely optional; you can still order whether you have an account or not.

Selecting What You Want

Start by browsing through the Wine Shop, Food Shop, and Gift Shop. If there is a check box next to an item or items that you are interested in, select the boxes and click the **Put in Shopping Cart** icon. If there is no check box, just click the **Put in Shopping Cart** icon. You can browse the Wine, Food, and Gift shops as much as you like before you place your order; our software will remember all of the items that you have chosen. When you are ready to order, follow the **Shopping Cart** link at the top or bottom of any page.

Selecting Shipping Destination

When you put the first item in your shopping cart, you will be asked to choose a shipping destination. After you choose the destination, you may continue shopping or proceed with ordering by clicking Shopping Cart at the top or bottom of any page. If you continue shopping, the shipping destination will apply to any additional items you select. If you need to, you may change the destination later in the ordering process.

(E3)

Security

Once you select the Shopping Cart link, you may be asked if you would like to switch to the secure commerce server. Selecting the secure server will allow you to transmit credit card and other confidential information in an encrypted form for safety. We guarantee the security of your credit card when you make a purchase with us. See our security guarantee for details.

Ordering the Items You've Selected

After you've selected all the items you might want to buy, you complete the order by clicking the Shopping Cart link at the top or bottom of any page. On the Shopping Cart page, you enter quantities for the items you've selected, preview your total cost, and select a payment method. Subsequent pages ask for your billing and shipping information. You can also provide a gift message if your order is a gift. You also have the option to sign up for our email newsletter. These steps are described in greater detail below. If, at this point, you decide that you want additional items not listed, you may back out of the ordering process and put the additional items in your shopping cart before you continue.

Selecting Quantity

On the Shopping Cart page review the quantity for each item. If you decide that you do not want to order a specific item, simply set the quantity to zero. Note that all orders of twelve items or more, mixed or from the same producer, receive a ten percent case discount.

Selecting Delivery Method

Once you have selected a quantity for each of the items listed, select a delivery method. To select the delivery method, scroll down the list of delivery methods and select a specific method. Not all delivery methods are available to all areas.

Delivery Tips

- All orders placed after 10 A.M. Pacific time are processed the following business day. Length of delivery is based on business days. Weekends and holidays are not included.
- All deliveries require an adult signature. Someone of legal age must be at the shipping address during the day to sign for and accept the packages. Packages cannot be left without the signature of an adult.
- Deliveries may occasionally be subject to weather holds so that your selections are not damaged by extreme temperatures. Delays of up to three additional days may result.

Changing Destination

You may change the destination of your shipment anywhere on the site. To change the destination, use the link to Change Shipping Destination from the navigation bar on the left side of the page. *Please*

note: when you change the shipping destination, some of the items in your shipping cart may no longer be shippable due to state-specific restrictions on wine availability.

Previewing Cost

If you have a gift certificate or have been given a promotion code, enter the certificate number or promotion code in the labeled box. Then calculate your total by clicking **Calculate Total** on the bottom of the page. You will see the price of your order, including any tax and shipping. You may change the quantities, if you like, and recalculate until you are happy with your order.

Selecting a Payment Method

Next, select a payment method. We accept **Visa**, **MasterCard**, **American Express** and **JCB**. If you have an account with us with a credit card on file and you have signed in, you will also see **Use Card On File** as a payment option. If you have a gift certificate and there is no balance due, simply click the **Phone** option.

If you do not want to use your credit card online, select **Phone**, which allows you to phone or fax in credit card information. If you select Phone, you will not be prompted for credit card information. Be sure to call or fax us with that information after you have completed the order. Note that we do guarantee the security of your credit card when you make a purchase using the secure server. See our Security Guarantee for details.

Filling in the Billing and Shipping Information

Selecting the payment method will take you to the next page of the order process. On that page you enter your billing and shipping information. If you have an account and you signed in before placing your order, your billing and shipping information will be filled in automatically, but you can make any changes specific to the current order at this time. If you do not have an account, you'll need to provide your billing and shipping information. If your billing address and shipping address are the same, fill in only the billing information.

Signing up for Email

The order form provides you with an option to be placed on our email list. If you would like to receive our email newsletters, please enter an email address in the billing information and click **Yes**. Our email newsletters are sent out approximately twice a month and are used to announce new arrivals, wine and food industry news, etc.

Ordering a Gift

If your order is a gift, you can enter a message that will be printed on a gift card and shipped with your purchase.

Age Verification

If you are shipping wine, you must verify that both you and the person to whom you are shipping are at least twenty-one years old.

Receiving Your Confirmation Number

Once you have filled out all the appropriate information, scroll down to the end of the page and click **Here Is My Order**. You will see a new page confirming your order with a confirmation number. **Please make sure you keep this confirmation number**; it is the easiest way for us to track your order.

If you do not see the confirmation number, your order has not been placed. In place of the confirmation number you will see an error message. Please correct the problem and click **Here Is My Order** again.

Email Confirmation

You will receive confirmation by email that your order was received. After the package has been delivered, you will receive another email confirmation telling you when the package was delivered and who signed for it.

That's the entire ordering process. It may sound complicated but it's really pretty simple. If you have any questions along the way, you can always email or call us toll free.

Thank you for your business!

Peter

Table 2
Context for EDI use

Sub-category	Concepts	Textiles	Chemical	Tobacco	Bank
Organizational factors	Organization size	Large companies often had more resources to implement sophisticated EDI	• Sophisticated EDI was more likely between trading partners who were large corporations	• Sophisticated EDI more likely between large organizations	• Sophisticated EDI transactions more likely at large banks
	IT capability	• Lack of skilled IT staff	• Lack of skill sets in IS	• Skilled IT staff	• Uses diverse IS products and services
		• Relatively old technology	• Lack of stability due to recent downsizing	• Industry leader in EDI implementation	• Leading edge technology
		• Movement to outsourcing	• Outsourced specialists		• Large IT investments
					• Skilled IT staff
	Senior management commitment	• High degree of commitment on the part of senior executives since customers demand it	• Medium level of commitment with increasing awareness of the importance of EDI	• Extremely committed	• Extremely committed
				• Deadlines and help issued to suppliers to become EDI compatible	• Senior management Recognizes electronic Products as an important source of future growth
Environmental factors	Industry experience with EDI	• Major user of EDI.	• Diverse user of EDI, particularly between large organizations	• Some customer segments (retailing) are high depth users of EDI. However, not all tobacco companies are extensive EDI users.	• Many large banks use EDI extensively
		• Increasing awareness of the importance of EDI as a source of competitive advantage for the industry			• Industry groups working towards new electronic products and services
		• Big differences in EDI usage between large and small organizations			
	Nature of suppliers	• Mix of large corporations and small "mom and pop" shops, many from within the textile industry	• Variety of suppliers from different industries	• Mix of large and small suppliers from different industries	• Individual depositors, other financial institutions, and the government
	Nature of customers	• Retailers, other industrial customers	• Mainly other industrial customers	• Mainly retailers	• Individuals, commercial customers (large and small), and other financial institutions

ANNEXURE-F

ANNEXURE-4

Table 6
Consequences of EDI use

Sub-categories	Concepts	Textiles	Chemical	Tobacco	Bank
Industry consequences	Competitive advantage	• Industry standards • Involvement in projects w/associations and universities	• Industry standards	• Industry standards	• Industry standards • Financial services consortium
	Conflicts	• Standards • Between small versus large suppliers	• Standards – different requirements from different industries they supply	• Between small versus large suppliers	• Banks and other financial services providers
Organizational consequences	Financial performance	• Market share improvement • Cost savings (some companies)	• Market share improvement • Cost savings(inventory, paperwork)	• Sustaining market share • Cost savings (inventory, paperwork, people)	• Market share improvement • Reduce cost for customer • New products/services
	Improved customer service	• Better information availability • Quick response to changing customer needs	• Better information availability • Just-in-time for its customers	• Better information availability	• Better information availability • Innovative services
	New products/services	• Vendor managed replenishment	• Just-in-time with ASN	• Vendor managed replenishment	• Cash management • Comprehensive payables
Individual consequences	IS personnel	• Learn new technology and business integration • Direct interaction with customers (especially if problem) • Problems highly visible to management	• Learn new technology and business integration • Direct interaction with customers (especially with problems • Problems highly visible to management • Accompany salespersons on customer calls	• Learn new technology and business integration • Direct interaction with customers (especially with problems)	• Learn new technology and business integration • Direct interaction with customers • Accompany salespersons on customer calls
	Non-IS personnel	• Learn new technology • Auditing concerns • Understand changes in business processes	• Learn new technology • More interaction with IS (salesforce) • Security and auditing concerns • Legal concerns with electronic transactions	• Learn new technology • More interaction with IS (salesforce) • Security and auditing concerns • Legal concerns with electronic transactions • Impact on jobs	• Learn new technology and business uses • More interaction with customers and IS • Security and auditing concerns • Legal concerns with electronic transactions

MODEL

ELECTRONIC DATA INTERCHANGE

TRADING PARTNER AGREEMENT

AND

COMMENTARY

Prepared by
the

Electronic Messaging Services Task Force

Subcommittee on
Electronic Commercial Practices
Uniform Commercial Code Committee
Section of Business Law

American Bar Association

ANNEXURE-H (H1)

1717

FOREWARD

This Model Electronic Data Interchange Trading Partner Agreement and Commentary were prepared by the Electronic Messaging Services Task Force under the auspices of the Subcommittee on Electronic Commercial Practices of the Uniform Commercial Code Committee, Section of Business Law, of the American Bar Association.

The Model Agreement and Commentary are to be used by attorneys in advising clients who are establishing commercial trading practices which implement electronic data interchange ("EDI"). The format of the Model Agreement and Commentary is considered an appropriate manner in which to identify the issues arising in EDI and to suggest uniform approaches in response. However, it is not intended that the Model Agreement represent the only form in which those issues may be addressed by counsel considering the underlying business relationships. Those reviewing the Model Agreement and Commentary are strongly encouraged to consider and study their provisions and to use independent judgment as to the effectiveness of the provisions of the Model Agreement and the advisability of their use in particular transactions.

The Model Agreement and Commentary reflect the views of those involved in their preparation; neither the contents of the Model Agreement and Commentary, nor the opinions expressed therein, represent the views, in whole or in part, of the American Bar Association or any part thereof.

Background

Beginning in the early 1970's, EDI was introduced as a method by which business data could be communicated electronically between computers in standardized formats in substitution for conventional paper-based documents. The commercial implementation of EDI to effect the purchase and sale of goods has experienced exponential growth, and has begun to change the manner in which contracts are negotiated and created.

In April 1987, the Subcommittee on the Scope of the Uniform Commercial Code, of the Uniform Commercial Code Committee, Section of Business Law, of the American Bar Association, through the Electronic Messaging Services Task Force, initiated a study to examine the effects of electronic commerce upon fundamental principles of contract law and related legal issues. In 1988, that Subcommittee issued a responsive report, entitled *Electronic Messaging* (ABA Publication No. 507-0210, 1988) and authorized a further examination of EDI and other electronic messaging systems (a) to determine how contract formation and related issues were being addressed by existing agreements, (b) to identify possible uniform approaches to those issues, and (c) to develop a means of communicating to practicing attorneys the issues which should be considered when drafting agreements for parties conducting business through the use of EDI.

In July 1989, in recognition of the continued expansion of electronic commerce and the legal issues which arise as a result, a new Subcommittee on Electronic Commercial Practices was organized. In October 1989, the Electronic Messaging Services Task Force issued to the Subcommittee on Electronic Commercial Practices and to the Subcommittee on the Scope of the Uniform Commercial Code a report entitled *The Commercial Use of Electronic Data Interchange--A Report*, 44 Bus. Law. ____ (June 1990). Counsel is encouraged to review the report in connection with the use of the Model Agreement.

Members of the Task Force responsible for the preparation of the Model Agreement and Commentary were: Michael S. Baum (Cambridge, Massachusetts), Philip V. Otero (Rockville, Maryland), Jeffrey B. Ritter (Columbus, Ohio), Thomas J. McCarthy (Wilmington, Delaware) and Amelia H. Boss (Philadelphia, Pennsylvania). The Task Force also wishes to recognize the invaluable comments and support provided by Patricia B. Fry (Grand Forks, North Dakota), Chair of the Subcommittee on Electronic Commercial Practices.

(H2)

USE OF THE MODEL AGREEMENT AND COMMENTARY

The following should be considered by counsel in reviewing and implementing the Model Agreement and Commentary:

1. Provisions of the Model Agreement contained in brackets ([ ]) identify options for counsel to consider; in several cases, the bracketed language represents alternatives presented within the Model Agreement, while in other instances the provisions are themselves presented as optional.

2. The Commentary has the following purposes:

   - To explain how the Model Agreement works, the purposes of each section and the intended effect of certain provisions in the context of existing commercial law.

   - To provide background technical information relating to certain aspects of EDI and prevailing general industry practices.

   - To provide specific drafting considerations on the manner in which provisions of the Model Agreement may be utilized or modified in preparing a definitive agreement.

3. The Appendix is an essential component of the Model Agreement. The parties should use the Appendix to set forth information essential to the proposed trading relationship as well as additional terms and conditions. Counsel should not consider the Appendix merely a "technical" item; rather, it is the field upon which mutual business decisions which affect the substance of the relationship of the parties, as well as the validity and enforceability of the underlying transactions, are to be specified. For that reason, the format of the Appendix is a suggested format, but does not represent a required structure. Counsel is encouraged to adapt the form and content of the Appendix to meet the requirements of any particular business relationship.

MODEL ELECTRONIC DATA INTERCHANGE TRADING PARTNER AGREEMENT

THIS ELECTRONIC DATA INTERCHANGE TRADING PARTNER AGREEMENT (the "Agreement") is made as of _____, 19_, by and between _____ ("ABC"), a _____ corporation, with offices at _____ and _____ ("XYZ"), a _____ corporation, with offices at _____.

RECITALS

ABC and XYZ desire to facilitate purchase and sale transactions ("Transactions") by electronically transmitting and receiving data in agreed formats in substitution for conventional paper-based documents and to assure that such Transactions are not legally invalid or unenforceable as a result of the use of available electronic technologies for the mutual benefit of the parties.

NOW THEREFORE, the parties, intending to be legally bound, agree as follows:

Comment

1. The scope and purposes of the Agreement are as follows:

   - The Agreement is to be used between commercial trading partners; the Agreement is not intended for use in consumer transactions.

   - The Agreement is to be used only in connection with domestic purchase and sale transactions involving goods, as contemplated by Article 2 of the Uniform Commercial Code (the "Code"). Counsel may wish to consider the Agreement in developing suitable provisions for use in other types of EDI relationships, such as those which are international in scope, or which involve the performance of services (including transportation and shipping activities).

   - The Agreement is intended to facilitate the commercial relationship of the trading parties. The Agreement does not generally advocate particular

H3

solutions to what are essentially business issues; freedom of contract is encouraged.

- The Agreement does not attempt to resolve all aspects of commercial trading relationships which are within the scope of Article 2 of the Code. Counsel is cautioned to consider the additional issues which arise from the underlying Transactions (issues which are not unique to the use of EDI) and to develop appropriate responses.

2. Certain provisions of the Agreement have the effect of varying the application of provisions of Article 2. In this respect, the Agreement implements two of the fundamental purposes of the Code, namely (a) to simplify, clarify and modernize the law governing commercial transactions, and (b) to permit the continued expansion of commercial practices through custom, usage and agreement of the parties. See UCC § 1-102(2). In order to accomplish these purposes, the Code is to be liberally construed and applied. See UCC § 1-102(1). This flexibility is intended to allow the underlying principles to be developed in light of unforeseen and new circumstances and practices. See UCC § 1-102, comment 1. Freedom of contract is also an important principle of the Code. See UCC § 1-102(3) and § 1-102, comment 2. Thus, parties are free to vary by agreement the effect of all provisions of the Code, except to the extent the general obligations of good faith, diligence, reasonableness and care may not be displaced. See UCC § 1-102(3) and § 1-102, comment 3.

3. The Recitals set forth the mutual intention of the parties for valid and enforceable obligations to result from the electronic communication of data in substitution for conventional paper-based documents. See also Sections 1.1, 2.1 and 3.3, and the Comments thereto. The execution and delivery of the Agreement and the performance of Transactions, together with the conduct of the parties in accordance with its terms, should be considered sufficient to show the existence of contracts for the sale of goods. See UCC § 2-204.

Drafting Considerations

1. The Agreement does not designate either party as buyer or seller. Either party may, therefore, purchase or sell goods in accordance with its provisions, unless appropriate modifications are made. For example, counsel may wish to add to the Appendix, as to each Document (as defined in Section 1.1), which party may be the "Sender" of that Document. See Sections 1.1 and 3.1, and the Comments and Drafting Considerations thereto.

2. Consider whether either or both of the parties are merchants, and the implications under the Code of that classification on the underlying commercial relationship and the rules of conduct which are defined by the Agreement. See UCC §§ 2-104(1) and 2-104(3). Note that if the parties are not corporations, appropriate changes should be made.

Section 1. Prerequisites.

1.1. Documents; Standards. Each party may electronically transmit to or receive from the other party any of the transaction sets listed in the Appendix, [transaction sets which the parties regularly transmit] and transaction sets which the parties by written agreement add to the Appendix (collectively "Documents"). Any transmission of data which is not a Document shall have no force or effect between the parties unless justifiably relied upon by the receiving party. All Documents shall be transmitted in accordance with the standards [and the published industry guidelines] set forth in the Appendix.

Comment

General:

1. Establishing an EDI trading relationship, by necessity, involves a series of decisions, primarily technical in nature, by both parties regarding: (a) the formats in which the data will be transmitted, and the standards and possible implementation guidelines to be adopted in connection with such formats; (b) the possible selection of third-party service providers (as well as the various business decisions required in connection with establishing such relationship); and (c) the development and maintenance of appropriate computer and communication systems and security procedures. Section 1 and the Appendix provide a framework for the parties to mutually structure these decisions. Compliance with the provisions of Section 1 will confirm their intent to give legal significance to the transmissions. See Sections 2.1, 2.3 and 3.3.3, and the Comments thereto.

2. Implementing EDI should also involve careful evaluation of existing internal business procedures and controls of the parties relating to paper-based commercial practices, and consideration of the extent to which such procedures and controls should be strengthened and/or modified in connection with the establishment of an electronic communication and trading environment. For example, authorizations to release purchase orders or approve payments, as well as rules regarding security and confidentiality, should be reviewed. See also Sections 2.1 and 3, and the Comments thereto.

3. This Section contains the first use of "by written agreement" or "in writing" in the Agreement. The Agreement provides the flexibility to allow notices, modifications, amendments or other communications required or permitted by the Agreement to be "in writing" to consist of electronic transmissions, but only if the transmissions satisfy the criteria of the Agreement for "Signed Documents" (as defined in

(H4)

Section 3.3.2). Alternatively, the Agreement could specify paper-based writings are required, if the parties consider it appropriate.

Documents:

4. "Transaction sets" define the types of data which the specified transmission must contain and the format in which the data must appear. Transaction sets function like conventional paper document forms, and include purchase orders, requests for quotation, purchase order acknowledgements, invoices, remittance advices and purchase order change requests. In addition, transaction sets exist in which "free text" may be communicated as a segment; this type of transaction set would be appropriate for notices, modifications or amendments (such as those described in Comment 3 above).

5. The Agreement generally applies only to those transmissions of data classified as "Documents" under Section 1.1. At a minimum, transaction sets listed in the Appendix (including subsequent additions) are Documents.

6. The Agreement provides, as an option, for transaction sets which are not listed in the Appendix but which are regularly transmitted to be considered as Documents. No attempt to define "regularly transmit" has been made. However, see Section 3.3.3 (and UCC § 2-208).

7. The "regularly transmit" option should be considered when both parties wish to give effect to new transaction sets without express prior agreement. Parties who wish to retain tight control over which transmissions qualify as Documents under Section 1.1 will eliminate the "regularly transmit" option from the Agreement. Note that, if the "regularly transmit" option is not included, regularly transmitted transaction sets may still be given effect, though inconsistent with the terms of this Agreement. See UCC §§ 1-103, 2-208 and 2-209. In addition, such parties may wish to eliminate from the second sentence of Section 1.1 the phrase " . . . unless justifiably relied upon by the receiving party" or make other modifications to, or entirely delete, that sentence. Note, however, that such changes may not effectively prevent a transmission which is not a Document from having legal effect, where the receiving party has under the circumstances, including the language in the Agreement, justifiably relied on that transmission. See Comment 6 above and Comment 8 below.

8. The second sentence of Section 1.1 is not intended to alter the law of reliance; the provision simply prevents a party which has transmitted data from avoiding the legal effect of the receiving party's justifiable reliance merely because the format had not been previously classified as a Document. However, note that the remaining provisions of the Agreement relating to Documents are not applicable in those circumstances. See, for example, Sections 1.2.3, 2.1, 3.3, and 4.6.

Standards:

9. "Standards" are the uniform specifications for the electronic interchange of business data and include provisions of the structure and format of data as well as the transmission of the formatted data. There are also standards, among other things, for certain security and communication procedures.

10. The selection of applicable standards is a matter of some flexibility. The parties may mutually select and utilize one or more sets of recognized standards, or, within certain technical limits, customize those standards to their mutual benefit. Existing technology also permits each party to adopt a different standard for transmission of a Document, with Providers (as defined in Section 1.2.1) subsequently conforming the different formats to each party's adopted standard.

11. Virtually all standards for EDI include detailed technical requirements to facilitate EDI, including transaction sets, data dictionaries, segment dictionaries and other uniform controls. Pursuant to the provisions of the Appendix, the selection by the parties of applicable standards acts to incorporate by reference these additional requirements. Should the parties desire to exclude or modify any of such requirements, such changes may be made in the Appendix.

Guidelines:

12. "Published industry guidelines" contain recommended procedures and implementation guidelines for the use of EDI within particular industry groups (recent examples include guidelines of the automotive, chemical and pharmaceutical industries). In contrast to standards, which require compliance for the effective interchange of data, guidelines generally are intended to aid implementation among trading partners. The Agreement, as an option, provides the parties the ability to require compliance with any guidelines which they mutually adopt and specify.

13. Counsel should carefully evaluate any available guidelines to assure that any conflicts between the guidelines and the standards, or between different guidelines, are understood and resolved. The adoption of certain guidelines, for example, may affect the process of contract formation in an unintended manner, since several current guidelines suggest certain procedures (e.g., which Documents are acceptable responses to other specified Documents) which may be in conflict with what the parties mutually negotiate and specify in the Appendix. Language in the Appendix has been included to avoid this result by subordinating the content of any selected guidelines to the provisions of the Agreement.

14. Counsel should evaluate whether any existing guidelines, whether or not adopted, may be considered, in any interpretation of the Agreement, as a usage of trade to be considered with respect to any Transaction. See UCC § 1-205(2).

Drafting Considerations

1. The parties should identify and list the transaction sets which may be transmitted between them

H5

as Documents. The Appendix is structured in accordance with most common methods of identifying Documents. However, proprietary Documents, not based upon any particular standard, may also be utilized and listed.

2. In specifying Documents in the Appendix, it is recommended that the parties agree that any selected Document be communicated only in the then current release version or the release version immediately preceding the then current release version. Consistent with the provisions of Section 1.3, this will require the parties to periodically install new release versions of software corresponding to new revisions of the applicable standards. See Section 1.3, and the Comments thereto. Counsel may wish to consider establishing a time frame in which any such releases must be installed.

3. In completing the Appendix, any transaction set listed as an Acceptance Document (pursuant to Section 2.3) should also be listed as a Document. See Section 2.3, and the Comments thereto.

4. The Agreement permits any Document specified in the Appendix to be transmitted by either party. If this result is not desired, appropriate restrictions should be specified in the Appendix. See Recitals, Drafting Consideration 1.

5. If the parties do not wish transmissions which are not Documents to be given any force or effect, appropriate changes may be made. See Comments 7 and 8 above.

1.2. Third Party Service Providers.

1.2.1. Documents will be transmitted electronically to each party either, as specified in the Appendix, directly or through any third party service provider ("Provider") with which either party may contract. Either party may modify its election to use, not use or change a Provider upon 30 days prior written notice.

Comment

1. Section 1.2 provides the structure to specify the channel(s) of communication to be used in transmitting Documents between the parties. Transmissions may be made directly between the parties or through Providers. To the extent Providers are selected, Section 1.2 provides a framework for considering those aspects of the trading partners' relationship under the Agreement which are related to the use of Providers.

2. Among other things, Providers function as electronic mail processing systems and may (a) maintain electronic "mailboxes" into which communications can be placed for trading partners, and (b) interconnect with other Providers to permit communication between their respective customers. Providers have become an important aspect of general industry practice relating to EDI.

3. Section 1.2.1 provides maximum flexibility for each party to choose and maintain the desired channel of communication. Decisions to communicate directly or through Providers will be affected by factors such as cost, the nature of available services, the volume of transmissions, the bargaining power of the respective parties and continued evolutions in technology.

4. Counsel should note that Section 1.2.1 requires the parties to have contracted with any Provider specified for them in the Appendix. This assures that each party has obtained the availability of each such Provider.

5. Notice of any modification of a party's election provides a reasonable opportunity for the other party to make corresponding adjustments in operations. Generally, 30 days is considered, consistent with general industry practice, as a reasonable notice period; however, that period may be adjusted, based on what may be reasonable for a particular relationship.

Drafting Considerations

1. If the parties elect to communicate directly, counsel may wish to consider specifying in the Appendix appropriate technical information.

2. If either party uses one or more Providers, the names and related information of such Providers are to be set forth in the Appendix. If Providers are to be used for particular services or transactions, such indications would be appropriate in the Appendix.

1.2.2. Each party shall be responsible for the costs of any Provider with which it contracts, unless otherwise set forth in the Appendix.

Comment

1. Section 1.2.2 permits the parties to allocate between them the various expenses incurred in the use of Providers. Such expenses relate to the basic services of transmission, receipt, data storage, and data translation as well as additional services which may be offered. Counsel should consider the effect of this Section 1.2.2 when Providers offer a service permitting the parties to automatically agree on-line as to the allocation of these types of expenses.

2. The Agreement is consistent with the general industry practice within a paper-based environment that each party absorb its respective communication costs (i.e., postage, courier costs, and printing expenses).

Drafting Considerations

To the extent the parties allocate costs in a manner other than as provided in Section 1.2.2, such allocation may be added in the Appendix; no change in the Agreement is required.

[1.2.3. Each party shall be liable for the acts or omissions of its Provider while transmitting, receiving, storing or handling Documents, or performing related activities, for such party; provided, that if both the parties use the same Provider to effect the transmission and receipt of a Document, the originating party shall be liable for the acts or omissions of such Provider as to such Document.]

Comment

1. This optional Section permits the parties to establish contractual responsibility between them for the conduct of their respective Providers. This Section, if used, has the effect of providing a clear rule within the Agreement for allocating the risk of loss between the parties arising from the Provider's conduct. If this Section is omitted, the parties will have no contractual liability to each other under the Agreement for the conduct of their respective Providers, except where such conduct is attributable to either party and causes such party to breach the provisions of the Agreement.

2. The originating party is responsible for the acts of a shared Provider on the basis that such party initiates the final action, with respect to any Document, to use the Provider.

3. The Agreement does not address the respective right of either party to assert claims against any Provider under any applicable service contract, nor does the Agreement alter the liability of the parties to each other, if any, pursuant to any applicable legal principles.

Drafting Considerations

1. Liability arising under Section 1.2.3 is subject to the exclusion of damages contained in Section 4.6; counsel should consider whether this result is appropriate. The possible effect of Section 4.5 (Force Majeure) to relieve a party of liability under Section 1.2.3 should also be evaluated.

2. Note that Section 1.2.3 does not act to allocate liability between the parties where a Provider is not used. See Section 1.2.1.

3. This Section, if used, may be modified to allocate liability in any other manner upon which the parties agree.

1.3. System Operations. Each party, at its own expense, shall provide and maintain the equipment, software, services and testing necessary to effectively and reliably transmit and receive Documents.

Comment

1. This Section imposes a reciprocal obligation upon the parties to support effective and reliable communications, and allocates the related costs.

2. Consistent with general industry practice, the obligation to "maintain" is intended to require the parties to update the specified items as necessary to assure that effective and reliable communications are maintained in accordance with prevailing commercial practices and technology. See Section 1.1, and the Comments thereto. Section 1.3 may require, therefore, additional hardware or software acquisitions by the parties as well as the possible adoption of new security procedures satisfying the requirements of Section 1.4.

3. The conduct of the parties in establishing and maintaining effective and reliable communication enhances the reliability of Documents (including their content). See Sections 2.1, 3.3, and the Comments thereto.

Drafting Considerations

To the extent the parties agree upon a different allocation of expenses, appropriate changes may be made.

1.4. Security Procedures. Each party shall properly use those security procedures, including those specified in the Appendix, if any, which are reasonably sufficient to ensure that all transmissions of Documents are authorized and to protect its business records and data from improper access.

Comment

1. Adequate security procedures are recognized by general industry practice as critical to the efficacy of electronic communication. This Section imposes affirmative duties to use security procedures to ensure the reliability of the communication systems and resulting business records. The use of adequate security enhances the reliability of those records and enhances the ability to prove the substantive terms of any underlying commercial transaction. See Section 3.3.4, and the Comments thereto.

2. This Section imposes two obligations. First, each party must use security procedures sufficient to "reasonably" ensure proper authorization of transmissions. If a party fails to adequately secure its transmission activities, it may be liable for any unauthorized transmissions, and the consequences thereof. Second, each party must use security procedures sufficient to "reasonably" protect business records and data from improper access. In this case a failure to comply may again result in liability. This second obligation, when properly performed, also gives one party some measure of assurance that its own operations will not be subject to improper access through the systems and operations of the other party. A party failing to meet this second duty would, in addition, likely be estopped from submitting its records as superior to those of the other party, where the other party has properly met its own duty under Section 1.4.

3. Security procedures may be far-ranging in both sophistication and detail. Examples include the confidential exchange of Signatures (see Section 1.5) to authenticate the parties and the content of Documents which are transmitted or received, the exchange of encryption keys (by which the content of communications may be scrambled and unscrambled only pursuant to the exchanged keys), physical control of access to equipment and facilities, and the exchange of identifying information regarding the terminals from which authorized EDI transmissions may originate (which identifying information may be contained as part of the electronic "envelope" in which transmissions are exchanged).

4. Whether in any circumstance procedures which have been adopted or implemented will be considered as "reasonable" will vary based on the size and relative sophistication of the parties, the complexity of the operations of the parties, the nature of the communications and the underlying commercial transactions and additional factors. This Section provides an objective but flexible test by which to measure the conduct of the parties. See UCC § 1-204(2).

5. Under this Section, the parties may specify in the Appendix additional security procedures in connection with either or both of the requirements described in the above comments. This provision provides flexibility; as EDI and related technologies continue to advance, increasingly sophisticated security procedures will likely emerge which may be appropriate for one or both parties to implement. Parties should consider specifying in the Appendix any existing, generally accepted security procedures, special industry standards and any proprietary or unique security procedures required by the underlying commercial relationship.

6. This Section encourages the parties to negotiate the level of security required to induce them to enter Transactions. See Section 3.3, Comment 5. However, to the extent any duty of care may exist between the parties, liability may also arise at common law. See UCC § 1-103.

7. This Section relates to obtaining access to business records and data; the use of such records and data is covered by Section 3.2. Counsel should consider the relationship between security procedures required by Section 1.4 and the treatment of confidentiality in Section 3.2.

Drafting Considerations

Counsel should note that the provisions of Section 4.6 (Exclusion of Damages) do not apply to any breach of the obligations arising under Section 1.4.

1.5. Signatures. Each party shall adopt as its signature an electronic identification consisting of symbol(s) or code(s) which are to be affixed to or contained in each Document transmitted by such party ("Signatures"). Each party agrees that any Signature of such party affixed to or contained in any transmitted Document shall be sufficient to verify such party originated such Document. Neither party shall disclose to any unauthorized person the Signatures of the other party.

Comment

1. This Section establishes a mechanism for the adoption by each party of an electronic signature by which each Document may be signed. UCC § 1-201(39) defines "signed" to include ". . . any symbol executed or adopted by a party with present intention to authenticate a writing (emphasis added)." Use of a Signature is important to establishing the validity of any EDI communication. See Section 3.3, and the Comments thereto.

2. This Section requires each party to adopt a Signature, but retains considerable flexibility as to what symbols or codes shall be adopted. The decision of each party will be made in light of existing technology, the relative sophistication of the parties, the requirements of applicable standards and any security procedures which are in use. A party may select as its Signature the use of its name on a Document (similar to a form of purchase order imprinted with the buyer's name and containing no other authorized signature). What is important is that the use of the adopted symbol or code reflect the intent to authenticate required by the Code. Regulating the use of any Signature may also be part of security procedures required by the Agreement; counsel should evaluate any such procedures to assure that the required intent to authenticate is preserved.

(Hg)

3. The electronic signature of any party may change from time to time, in order to protect its confidential character. Accordingly, the Appendix does not provide for disclosure of any Signature, but relies on general industry practice for the exchange of Signatures by other means of communication. If any Signature is used by a party as part of adopted security procedures the practice of periodically changing the Signature could be considered as consistent with the obligations of such party under Section 1.4 to use reasonable security procedures.

4. The last sentence of Section 1.5 prohibits only disclosure of the Signatures of the other party. If security procedures required by the Agreement relate to non-disclosure of Signatures, a party which discloses its own Signature to an unauthorized person may breach the provisions of Section 1.4.

Section 2. Transmissions.

2.1. Proper Receipt. Documents shall not be deemed to have been properly received, and no Document shall give rise to any obligation, until accessible to the receiving party at such party's Receipt Computer designated in the Appendix.

Comment

1. The increased speed and accuracy of electronic commerce fundamentally differ when compared to contract formation practices in a paper-based environment. Parties engaging in electronic commerce have the ability to efficiently determine whether a particular transmission has been received by the other party, whether any transmission is inconsistent with prior business arrangements, or whether any transmission may be outside negotiated contractual limits. Consequently, the procedures of electronic commerce, when effectively implemented, offer the opportunity to achieve greater certainty in the contracting process. Section 2 provides a framework for the effective implementation of those procedures for the mutual benefit of both parties. The provisions set forth rules pertaining to the timing of receipt (Section 2.1), the obligation of the receiving party to verify receipt (Section 2.2), the manner in which acceptance occurs within an EDI environment (Section 2.3), and the disposition of unintelligible or garbled transmissions (Section 2.4).

2. Section 2.1 provides that no Document may create any legal obligation until properly received. This Section, therefore, represents a departure from the "mailbox rule" and parallel legal doctrines. Since the technology exists by which the party originating the transmission of any Document can effectively confirm receipt has occurred, it is inappropriate that the mere dispatch of any Document should be sufficient for any legal purpose.

3. "Properly received" requires that the transmitted Document be accessible at a computer designated by the receiving party. This permits each party to determine the appropriate system location. A Receipt Computer may be the computer of the third party service provider, the computer of either party or a specific terminal within a party's internal network (for example, a billing supervisor's desk). The Receipt Computer should be situated to enable the receiving party to promptly and properly transmit a functional acknowledgement upon proper receipt of any Document, as required by Section 2.2. Such acknowledgement may be sent by the Receipt Computer or by a computer with which the Receipt Computer communicates. Counsel should review the applicable operations to ensure that a functional acknowledgement cannot be transmitted before a Document reaches the Receipt Computer. Counsel should carefully consider the effects under remaining provisions of the Agreement of selecting as the Receipt Computer a computer which is not under the respective control of each party. Note that receipt does not require that any Document actually be examined, only that the Document be accessible. In a paper-based environment, this is similar to when a letter is delivered, but the envelope remains unopened. Each party thereby defers "receipt" until the "right" person or machine has an opportunity to have access to the transmitted data.

4. Note that Section 2.1 operates to relieve both parties from any obligation until the Document has been properly received.

5. Except as described in Comment 2 above, the provisions of Section 2 are not intended to displace other applicable laws relating to contract formation or the underlying commercial relationship of the parties.

6. Several examples which illustrate the operation of the provisions of Section 2 appear at Section 2.4, Comment 6.

Drafting Considerations

1. In identifying the proper Receipt Computer, counsel may wish to consider, by example, current internal practices of the parties for giving notice under existing agreements and identify the person designated for such purposes (see Section 1.1, Comment 2). Since virtually any Document may be sent without direct human involvement, care should be taken that adequate controls have been established regulating the level of approval (and human authorization) required to properly receive any Document.

2. Counsel should consider whether any modification by either party under Section 1.2.1 will require conforming changes in the designation of the Receipt Computer for such party.

(Hq)

2.2. Verification. Upon proper receipt of any Document, the receiving party shall promptly and properly transmit a functional acknowledgement in return, unless otherwise specified in the Appendix. A functional acknowledgement shall constitute conclusive evidence a Document has been properly received.

Comments

1. In light of the capability of technology to facilitate nearly immediate verification of receipt, and also to verify that no defect in receipt has occurred, Section 2.2 imposes an affirmative obligation to provide verification of receipt. Effective verification practices increase the opportunity for the early detection and resolution of transmission errors, thereby reducing the exposure of both parties to possibly significant damages.

2. A "functional acknowledgement" is a transaction set which confirms that receipt of a Document (in the format specified by such functional acknowledgement) has occurred and that all required portions of the Document have been received and are syntactically correct, but otherwise does not confirm the substantive content of the related Document. A functional acknowledgement can verify receipt, but is also designed to identify whether, in fact, omissions or errors in format or syntax have occurred. To the extent a party transmitting a functional acknowledgement identifies any errors or omissions, such notice would satisfy the notice requirements of Section 2.4. See Section 2.4, and the Comments thereto.

3. A party will "properly transmit" a functional acknowledgement or Document if it has been transmitted in a manner which complies with the provisions of Section 1.

4. Whether or not verification is provided will not alter the legal significance of the initial Document; Section 2.1 controls in that respect.

5. Counsel may wish to evaluate whether any circumstances exist where the affirmative obligation to verify receipt should not be imposed and make appropriate exceptions in the Appendix. For example, a party's system may not include functional acknowledgements or the parties may elect to verify in another manner, such as transaction sequence checking.

6. A party initially transmitting a Document may have an obligation to make reasonable inquiries or take other actions to discharge any duty which may exist to mitigate damages arising from a breach of the provisions of Section 2.2 by the receiving party.

7. The conclusive quality of a functional acknowledgement established by this Section assures that subsequent reliance thereon is reasonable.

2.3. Acceptance. If acceptance of a Document is required by the Appendix, any such Document which has been properly received shall not give rise to any obligation unless and until the party initially transmitting such Document has properly received in return an Acceptance Document (as specified in the Appendix).

Comment

1. Section 2.3 unambiguously indicates, with respect to the offer and acceptance of any contract, that no obligation will arise except upon satisfaction of the provisions of the Agreement. See UCC § 2-206(1). The parties, by designating appropriate Acceptance Documents, have the opportunity to define what will constitute acceptance and can assure that no contract arises from any Document until there has been mutual and certain agreement upon the terms contained in such Document.

2. This Section permits the parties to designate Acceptance Documents for Documents not specifically included in the contract formation process.

3. An Acceptance Document might be a computer generated response or a more significant communication, possibly requiring human evaluation at the receiving end. Selection of the appropriate Acceptance Document in a particular context may also be influenced by the manner in which either party interacts with its Provider and by the commercial relationship of the parties. Note that Section 2.3 operates to relieve both parties from any obligation until an Acceptance Document has been properly received in return.

4. Note that the party receiving a Document also controls whether the Acceptance Document is to be sent. If the proposed terms or content of an initial Document is objectionable, neither party has any obligation if the Acceptance Document is not properly received in return.

Drafting Considerations

1. In identifying possible Acceptance Documents, counsel may wish to consider, by example, current internal practices of the parties for giving notice under existing agreements and identify the person designated for such purposes (see Section 1.1, Comment 2). Since virtually any Document may be sent without direct human involvement, care should be taken that adequate controls have been established regulating the level of approval (and human authorization) required to transmit any Document.

2. Counsel is strongly encouraged to review the substantive content of possible Acceptance Documents in selecting the appropriate confirmation of any Document. For example, in response to a purchase order, the Acceptance Document may be:

- a purchase order acknowledgement (which substantively confirms the terms of the purchase order); or

- a shipping notice (specifying that the goods have been or will be shipped; see UCC § 2-206(1)(b)).

3. For certain Documents (for example, a notice of rejection of goods from the buyer), no Acceptance Document will be appropriate. Note, however, if the buyer, having sent such notice does not receive a functional acknowledgement in return, the buyer is on notice that its notice of rejection may not have been received, and should consider either re-sending the notice, or providing such notice by means other than EDI. See UCC § 1-201(26).

4. Counsel may wish to consider applicable industry implementation guidelines in selecting appropriate Acceptance Documents. See Section 1.1, Comments 2 and 13.

5. Counsel should also consider what effects, if any, the selection and use of Acceptance Documents may have upon the additional terms and conditions of the underlying commercial relationship, which may more specifically address contract formation issues (such as the time period in which offers must be accepted or rejected, and the manner of communicating rejection, if at all), rights of rejection and other matters. In addition, notwithstanding the last sentence of Section 3.1, counsel should endeavor to assure that the contract formation practices developed under the Agreement are consistent with any commercial relationship established by any other agreement described in Section 3.1. See Section 3.1, and the Comments thereto.

2.4. Garbled Transmissions. If any transmitted Document is received in an unintelligible or garbled form, the receiving party shall promptly notify the originating party (if identifiable from the received Document) in a reasonable manner. In the absence of such a notice, the originating party's records of the contents of such Document shall control.

Comment

1. Section 2.4 is intended to apply only to unintelligible or garbled messages, incapable of having effective meaning or missing material data components, for which the originating party may be identified within the context of the relevant Document. In those cases, the originating party's records control unless the receiving party gives prompt notification in a reasonable manner. See UCC § 1-204. Such notice may be given by other than electronic means. The obligation to provide notice under this Section is not burdensome in an electronic environment, and has the advantage of assisting the transmitting party to correct promptly a miscommunication.

2. The phrase "unintelligible or garbled" is not intended to include Documents which are, in human readable form, capable of being read but which contain information which the receiving party knows, or has reason to know, may be incorrect. For example, if ABC has always ordered no more than 200 pencils, its purchase order for 200,000 pencils should not be considered unintelligible or garbled, since pursuant to Section 2.1, the parties can adopt a procedure where XYZ can always review, confirm or reject the substantive terms contained in any Document.

3. Section 2.4 is not intended to displace the applicable principles of the law of mistake. See UCC § 1-103.

4. If, pursuant to Section 2.3, no obligation arises with respect to a Document otherwise subject to this Section because the required Acceptance Document has not been properly received in return, then the fact that such Document is unintelligible or garbled should have no consequences under this Section.

5. Section 4.6 (Exclusion of Damages) clearly applies to liabilities which may arise in connection with any unintelligible or garbled transmission; if the parties wish a different result, appropriate changes may be made.

6. The following examples illustrate the operation of the provisions of Section taken as a whole:

Example 1. XYZ has specified its mainframe computer as its Receipt Computer. ABC sends a Document to XYZ's Provider, but the Document is never made accessible to XYZ's Receipt Computer. ABC's transmission of the Document has no legal effect.

Example 2. XYZ properly receives a purchase order from ABC but never transmits in return either a functional acknowledgement or an Acceptance Document. No contract has been formed but XYZ is liable for any damages suffered by ABC, if any, from XYZ's failure to provide verification as required.

Example 3. XYZ properly receives a purchase order from ABC which by its terms is open for 10 days. XYZ properly transmits an Acceptance Document within the 10 day period, but the Acceptance Document is not "properly received" until the 11th day. No contract is formed.

Example 4. The Appendix requires, as to a purchase order, that a purchase order acknowledgement be sent as an Acceptance Document. ABC, as buyer, sends a purchase order, receipt of which is verified by XYZ, as seller, by sending a functional acknowledgement. However, XYZ never sends an Acceptance Document. No contract for sale has been formed.

Example 5. XYZ properly transmits an Acceptance Document,

which is received by XYZ's Provider and stored. Meanwhile, ABC properly transmits a revocation of its offer, which revocation is properly received by XYZ's Receipt Computer before the Acceptance Document is forwarded to ABC's Receipt Computer by XYZ's Provider. No contract is formed; the revocation is effective.

Example 6. The Appendix requires, as to a purchase order, that a purchase order acknowledgement be sent as an Acceptance Document. XYZ, as seller, properly receives a purchase order from ABC, as buyer, but the price data is missing. XYZ sends a functional acknowledgement which identifies the omitted data. Under Section 2.4, XYZ has met its obligations. If XYZ, without the price data, then sends an Acceptance Document, a contract is formed, with the price to be determined pursuant to applicable law. See UCC § 2-305.

Section 3. Transaction Terms.

3.1. Terms and Conditions. This Agreement is to be considered part of any other written agreement referencing it or referenced in the Appendix. In the absence of any other written agreement applicable to any Transaction made pursuant to this Agreement, such Transaction (and any related communication) also shall be subject to [CHOOSE ONE]:

[A] those terms and conditions, including any terms for payment, included in the Appendix.

[B] the terms and conditions included on each party's standard printed applicable forms attached to or identified in the Appendix [as the same may be amended from time to time by either party upon written notice to the other]. The parties acknowledge that the terms and conditions set forth on such forms may be inconsistent, or in conflict, but agree that any conflict or dispute that arises between the parties in connection with any such Transaction will be resolved as if such Transaction had been effected through the use of such forms.

[C] such additional terms and conditions as may be determined in accordance with applicable law.

The terms of this Agreement shall prevail in the event of any conflict with any other terms and conditions applicable to any Transaction.

Comment

1. Section 3 recognizes that the exchange of Documents furthers the commercial relationship of the parties, and that the use of available technology pursuant to its terms should not create any conflict with other written agreements between the parties, or fail to properly accommodate the terms and conditions which define the dimensions of the commercial transactions.

2. Section 3.1 responds to three situations:

- The parties have previously or concurrently executed a separate contract for the sale of goods, which may, by example, be in the form of a master purchase, requirements or outputs agreement. See UCC § 2-306.

- The parties execute such an agreement after the Agreement is signed.

- The parties conduct business in the absence of, or outside the scope of, any such agreements, relying solely upon the Documents and the conduct of the parties pursuant to the Agreement to establish any contract.

In either the first or second case, the other agreement is assumed to be the instrument by which the parties have had the opportunity to negotiate and agree upon terms and conditions applicable to any Transaction which are not defined by the content of any Document. However, in the final case, Section 3.1 requires the parties to elect from among three alternatives the manner for providing the additional terms and conditions not anticipated by the standard formats of applicable transaction sets.

3. Option [A] requires negotiation and agreement upon the additional terms and conditions. Such option, as compared to the remaining options, achieves the highest level of certainty in establishing the terms of any contract of sale. Essential terms and conditions to be negotiated, by way of example, may include warranty, delivery, rejection, liability for non-conforming goods and attorney's fees. The negotiated terms would be included in the Appendix.

4. Option [B] permits incorporation into the electronic environment of existing paper-based methods of conducting business. Option [B] has the objective of clearly defining, for each party, the terms and conditions upon which it wishes to conduct business, and, to the extent amendments may be accommodated, the terms and conditions applicable at any time during the commercial relationship. If selected, however, Option [B], in anticipating, but not resolving, inconsistencies or conflicts in the respective forms of the parties, will not achieve the highest level of certainty as to the terms of any contract of sale.

5. Option [B] requires each party's standard printed forms to be incorporated as a part of the Agreement. The parties may attach

such forms to the Appendix or may identify the appropriate forms which are to be incorporated by reference. Any identification provided should be sufficiently specific to identify only one form. However, selecting the option of attaching such forms to the Appendix assures that the terms and conditions of such forms are explicitly known and disclosed.

6. In response to general industry practice, Option [B] includes, as a further option, language permitting the terms and conditions of any form attached to or identified in the Appendix to be amended by subsequent written notice (which notice must be sufficient to adequately identify the new form or changes). If this option is elected, either party may incorporate into EDI trading the changes in terms and conditions which may occur in its paper-based trading practices. Parties wishing to retain greater control over subsequent amendments would not elect the optional language. In that case, subsequent forms would require mutual agreement for subsequent attachment or identification.

7. In the event of any inconsistency or conflict between the respective forms of the parties, Option [B] incorporates the method of resolution set forth in UCC § 2-207 and other applicable law. Since the attached or identified forms will correspond to Documents which have been transmitted, the terms and conditions contained in such forms should be considered in the same sequence in which the related Documents are transmitted and received between the parties.

8. Option [C], if elected, incorporates into each contract for sale of goods the manner by which applicable law determines additional terms and conditions (other than quantity) which have not been agreed upon by the parties. See, e.g., UCC § 2-305 (Open Price Term), § 2-307 (Delivery and Single Lot), § 2-308 (Place for Delivery) and § 2-309 (Time for Shipment or Delivery). Under the circumstances contemplated by the Agreement, any contract for sale should not fail for indefiniteness. See UCC § 2-204(3).

9. The last sentence of Section 3.1 confirms that the intent of the parties to give effect to the provisions of the Agreement is not contradicted by other terms and conditions applicable to any Transaction, whether set forth in any agreement described in Section 3.1 or by applicable law. For example, a separate contract for the sale of goods may provide for acceptance, in a paper-based environment, to occur upon the receipt of a signed purchase order acknowledgement at the offices of buyer by certified mail. The last sentence of Section 3.1 provides for the acceptance mechanism established pursuant to the Agreement to control with respect to EDI transmissions. Thus, the commercial intent of the parties, taken as a whole, is given effect.

Drafting Considerations

1. If the parties clearly intend that the Agreement is to be used solely and exclusively in connection with other written agreements, and that no other EDI transactions should be authorized, the second sentence of this Section may be deleted. However, such sentence serves as a "safety basket" for future transactions not otherwise contemplated and should be deleted only after careful analysis.

2. If the parties elect Option [A], counsel is encouraged to carefully consider whether additional terms and conditions should be included to fully implement the commercial intentions of the parties expressed in other provisions of the Agreement. See Section 1.1, Comment 2, and Section 2.3, Drafting Consideration 5.

3. If the parties elect Option [B], counsel may wish to consider specifying the method of providing notice of any amendments to the printed forms adopted by either party, as well as any minimum period before such notices take effect.

3.2. Confidentiality. No information contained in any Document or otherwise exchanged between the parties shall be considered confidential, except to the extent provided in Section 1.5, by written agreement between the parties, or by applicable law.

Comment

1. Section 3.2 focuses on whether the information transmitted in any Document requires confidential treatment by the parties. This Section provides for no confidential treatment except for Signatures (as provided in Section 1.5), and as required by other written agreements (see Section 1.1, Comment 3) or by applicable law. Examples of applicable law would include common law relating to trade secrets, any court order imposing confidentiality obligations as to any relevant information or 47 USC 605.

2. If confidential treatment is to be provided, counsel, in substitution for the provisions of Section 3.2, should prepare appropriate provisions as to the scope and duration of any obligations, as well as appropriate remedies. Counsel may wish to give special emphasis, if only certain information is to be considered as confidential, on the manner in which, in an electronic environment, information is to be designated as confidential by the parties. Information may be designated as confidential on a transaction-by-transaction basis by including an appropriate designation (by the use of special codes) within the related electronic transmissions. Such a technique would satisfy the requirement of this Section 3.2 for "written agreement" if the parties intend for that effect. See Section 1.1, Comment 3.

H13

3.3. Validity; Enforceability.

3.3.1. This Agreement has been executed by the parties to evidence their mutual intent to create binding purchase and sale obligations pursuant to the electronic transmission and receipt of Documents specifying certain of the applicable terms.

3.3.2. Any Document properly transmitted pursuant to this Agreement shall be considered, in connection with any Transaction, any other written agreement described in Section 3.1, or this Agreement, to be a "writing" or "in writing"; and any such Document when containing, or to which there is affixed, a Signature ("Signed Documents") shall be deemed for all purposes (a) to have been "signed" and (b) to constitute an "original" when printed from electronic files or records established and maintained in the normal course of business.

3.3.3. The conduct of the parties pursuant to this Agreement, including the use of Signed Documents properly transmitted pursuant to this Agreement, shall, for all legal purposes, evidence a course of dealing and a course of performance accepted by the parties in furtherance of this Agreement, any Transaction and any other written agreement described in Section 3.1.

3.3.4. The parties agree not to contest the validity or enforceability of Signed Documents under the provisions of any applicable law relating to whether certain agreements are to be in writing or signed by the party to be bound thereby. Signed Documents, if introduced as evidence on paper in any judicial, arbitration, mediation or administrative proceedings, will be admissible as between the parties to the same extent and under the same conditions as other business records originated and maintained in documentary form. Neither party shall contest the admissibility of copies of Signed Documents under either the business records exception to the hearsay rule or the best evidence rule on the basis that the Signed Documents were not originated or maintained in documentary form.

Comment

1. This Section confirms the validity and enforceability of the underlying contracts formed by the electronic transmission and receipt of Documents. See Recitals, Comment 3.

2. The intent of any party to a contract that the contract be legally binding is an essential predicate for the underlying transaction. The Recitals of the Agreement initially stated the parties' intentions that Transactions arising under the Agreement be legally valid and enforceable; Section 3.3.1 implements such intent.

3. Section 3.3.2 establishes any properly transmitted Document as a "writing". This provision expands upon the existing definition contained in UCC § 1-201(46) (defining "writing" to include "printing, typewriting or any other intentional reduction to tangible form."). This modification is of the type contemplated by the Code. See UCC § 1-102(3) and Recitals, Comment 2.

4. Section 3.3.2 (taken with the provisions of Section 1.5) also establishes Signed Documents as sufficient to satisfy the formal requirements of UCC § 2-201 (the Statute of Frauds) when the Documents relate to the formation of any contract for the sale of goods for the price of $500 or more. See UCC § 2-201 and comments thereto. Finally, Section 3.3.2 also establishes that Signed Documents shall be deemed to constitute "original" business records under certain circumstances. See Comment 7 below; see also Section 1.4, Comment 1.

5. Under Section 3.3.3, the conduct of the parties pursuant to the Agreement constitutes a course of dealing and a course of performance upon which they may rely in structuring their business relationship. This conduct includes the identification of the Documents to be transmitted, the establishment of channels of communication and the adoption of mutually acceptable security procedures, all pursuant to the provisions of Section 1. UCC § 2-208 contemplates that such conduct be considered in determining the meaning of this Agreement and any underlying contract for the sale of goods. See UCC §§ 1-205 and 2-208. This conduct, either as a course of dealing or as a course of performance, should be given effect with respect to both the Agreement and other applicable purchase contracts, independent of the status of Signed Documents as signed writings under applicable law. See also UCC §§ 2-202(a) and 2-207(3).

6. Nothing in the Agreement, other than the prohibition on oral waivers contained in Section 4.3, operates to prevent either party from contending that the terms and conditions applicable to any Transaction, or those set forth in the Agreement, may be modified or waived as contemplated by UCC § 2-209.

7. Section 3.3.4 establishes rules of conduct for the parties in connection with the use of Signed Documents as evidence in any proceeding between the parties. By way of example, see Federal Rules of Evidence 802, 803(6) and 1002. However, Section 3.3.4 (together with Section 3.3.2) does not waive the need for a proper foundation to be established for the admissibility of the evidence. In this regard, the effectiveness and reliability of each party's security procedures, record retention policies, confidentiality

(H14)

obligations and their conduct under the provisions of the Agreement may be relevant in individual cases to the ultimate admissibility of any Signed Documents.

Section 4. Miscellaneous.

4.1. Termination. This Agreement shall remain in effect until terminated by either party with not less than 30 days prior written notice, which notice shall specify the effective date of termination; provided, however, that any termination shall not affect the respective obligations or rights of the parties arising under any Documents or otherwise under this Agreement prior to the effective date of termination.

Comment

1. The provisions of Section 4 include provisions often found in many types of agreements. These provisions are not exclusive, and counsel may wish to consider other similar customary provisions which, for the most part, are not effected by the use of electronic communications. However, as discussed in these Comments, these provisions focus upon some significant legal factors relating to the use of electronic communication under the Agreement.

2. Section 4.1 assures freedom of contract, but also assures the non-terminating party an appropriate opportunity to establish (or re-institute) alternative procedures of communication.

3. A 30-day notice period is considered reasonable by general industry practice. However, see Section 1.2.1, Comment 5.

4. Any notice of termination under Section 4.1 does not affect obligations under the underlying commercial relationship; any notices relating to such obligations would be separately required.

5. With respect to the requirement that notice under this Section be "written", see Section 1.1, Comment 3.

4.2. Severability. Any provision of this Agreement which is determined to be invalid or unenforceable will be ineffective to the extent of such determination without invalidating the remaining provisions of this Agreement or affecting the validity or enforceability of such remaining provisions.

Comment

The Agreement has been prepared for implementation in a variety of situations; Section 4.2 has been included to assure that the entire contract does not fail in the event any specific provision is determined to be unenforceable under any particular circumstances.

4.3. Entire Agreement. This Agreement and the Appendix constitute the complete agreement of the parties relating to the matters specified in this Agreement and supersede all prior representations or agreements, whether oral or written, with respect to such matters. No oral modification or waiver of any of the provisions of this Agreement shall be binding on either party. No obligation to enter into any Transaction is to be implied from the execution or delivery of this Agreement. This Agreement is for the benefit of, and shall be binding upon, the parties and their respective successors and assigns.

Comment

1. Section 4.3 integrates the Appendix with the Agreement into a complete agreement. The provisions of Section 3.1 are effective to integrate the Agreement (with the Appendix) into any other specified purchasing contract.

2. Section 4.3 permits modifications and waivers of the Agreement by Signed Documents (but the parties must include "free-text" Documents to have this result). See Section 1.1, Comments 3 and 4. If the parties wish to require paper-based writing for modifications or waivers, appropriate changes should be made.

3. This Section confirms that the Agreement itself creates no obligations relating to the purchase and sale of goods; such obligations arise only from the Documents and the conduct of the parties.

4.4. Governing Law. This Agreement shall be governed by and interpreted in accordance with the laws of the State of _____.

Comment

In addition to customary factors considered in selecting applicable law, counsel may wish to evaluate various state laws which may be in effect relating to criminal use of computers, computer privacy and similar issues relating to technology.

H15

4.5. Force Majeure. No party shall be liable for any failure to perform its obligations in connection with any Transaction or any Document, where such failure results from any act of God or other cause beyond such party's reasonable control (including, without limitation, any mechanical, electronic or communications failure) which prevents such party from transmitting or receiving any Documents.

Comment

1. The scope of this Section is limited to events which prevent the transmission or receipt of Documents and does not extend to the impact of those events on any other obligations of the parties, whether under the Agreement or in connection with any underlying Transaction.

2. Among other things, this Section is specifically intended to excuse performance resulting from such events as a general power outage in the community or unscheduled "down-time" events outside the reasonable control of one of the parties.

3. Counsel should carefully consider the effect of this Section upon the obligations arising under Section 1.2.3, if such Section is included. To the extent Section 1.2.3 imposes liability, counsel should evaluate whether Section 4.5 reduces or eliminates liability to the extent the actions of a Provider may be considered beyond the reasonable control of either party.

4.6. Limitation of Damages. Neither party shall be liable to the other for any special, incidental, exemplary or consequential damages arising from or as a result of any delay, omission or error in the electronic transmission or receipt of any Documents pursuant to this Agreement, even if either party has been advised of the possibility of such damages.

Comment

Since the benefits of conducting electronic commerce are substantial and far-reaching, an exclusion of damages is appropriate and consistent with general industry practice to encourage recognition of those benefits. However, the scope of this Section is also limited, as provided in Section 4.5, solely to damages arising from or as a result of any delay, omission or error in the transmission or receipt of Documents pursuant to the Agreement. See Section 2.4, Comment 5. Section 4.6 does not limit any damages resulting from a breach of Section 1.4 (Security Procedures) or Section 1.5 (Confidentiality) and does not apply to damages resulting from a breach of any related Transaction. If different results are desired, appropriate changes should be made.

[4.7. Arbitration. Any controversy or claim arising out of or relating to this Agreement, or the breach thereof, shall be settled in accordance with the Commercial Arbitration Rules of the American Arbitration Association, and judgment on the award rendered by the arbitrator(s) may be entered in any court having jurisdiction thereof.]

Comment

1. Section 4.7 sets forth, as an option, the recommended arbitration clause of the American Arbitration Association.

2. Counsel is encouraged to consider the advisability of arbitration and other forms of alternative dispute resolution in connection with the Agreement and Transactions conducted pursuant to the Agreement. Of course, to the extent arbitration or other similar methods are considered appropriate, the parties may modify or amend the suggested language.

Each party has caused this Agreement to be properly executed on its behalf as of the date first above written.

ABC	XYZ
By_____	By_____
Name:_____	Name:_____
Title:_____	Title:_____

APPENDIX

STANDARDS

Specify ALL applicable standards (and the issuing organizations):

_____ _____

Selected standards include, as applicable, all data dictionaries, segment dictionaries and transmission controls referenced in those standards, but include only the Transaction Sets listed in the DOCUMENTS section of this Appendix below.

DOCUMENTS

Transaction Set No.	Document Name or Description	Version Release	Verification Required (Yes or No)	Acceptance Required (Yes or No)	Acceptance Document: Transaction Set No.	Acceptance Document: Document Name or Description
		Then current and one prior version				

GUIDELINES

Specify ALL applicable published industry guidelines: _____

The provisions of the Agreement (including this Appendix) shall control in the event of any conflict with any listed guidelines.

THIRD PARTY SERVICE PROVIDERS

(If the parties will be transmitting Documents directly, insert "NONE")

	Name	Address	Telephone Number
ABC -			
XYZ -			

RECEIPT COMPUTER

ABC -

XYZ -

ALLOCATION OF PROVIDER COSTS

(If no special allocation has been agreed upon, enter "NONE"): _____

SECURITY PROCEDURES

(If no security procedures have been agreed upon, enter "NONE"): _____

EXISTING AGREEMENTS

(If the Agreement is not to be considered a part of any existing written agreement, enter "NONE"): _____

[TERMS AND CONDITIONS

If the parties select Section 3.1[A], specify terms and conditions: _____

If the parties select Section 3.1[B], attach applicable forms or provide sufficient identification of each form being incorporated: _____]

UNCITRAL Model Law on Electronic Commerce

[Original: Arabic, Chinese, English, French, Russian, Spanish]

Part one. Electronic commerce in general

CHAPTER I. GENERAL PROVISIONS

*Article 1. Sphere of application**

This Law** applies to any kind of information in the form of a data message used in the context*** of commercial**** activities.

---

*The Commission suggests the following text for States that might wish to limit the applicability of this Law to international data messages:

"This Law applies to a data message as defined in paragraph (1) of article 2 where the data message relates to international commerce."

**This Law does not override any rule of law intended for the protection of consumers.

***The Commission suggests the following text for States that might wish to extend the applicability of this Law:

"This Law applies to any kind of information in the form of a data message, except in the following situations: [...]."

****The term "commercial" should be given a wide interpretation so as to cover matters arising from all relationships of a commercial nature, whether contractual or not. [Relationships of a commercial nature include, but are not limited to, the following transactions: any trade transaction for the supply or exchange of goods or services; distribution agreement; commercial representation or agency; factoring; leasing; construction of works; consulting; engineering; licensing; investment; financing; banking; insurance; exploitation agreement or concession; joint venture and other forms of industrial or business cooperation; carriage of goods or passengers by air, sea, rail or road.]

ANNEXURE - I

Article 2. Definitions

For the purposes of this Law:

(a) "Data message" means information generated, sent, received or stored by [electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy;]

(b) "Electronic data interchange (EDI)" means the electronic transfer from computer to computer of information using an agreed standard to structure the information;

(c) "Originator" of a data message means a person by whom, or on whose behalf, the data message purports to have been sent or generated prior to storage, if any, but it does not include a person acting as an intermediary with respect to that data message;

(d) "Addressee" of a data message means a person who is intended by the originator to receive the data message, but does not include a person acting as an intermediary with respect to that data message;

(e) "Intermediary", with respect to a particular data message, means a person who, on behalf of another person, sends, receives or stores that data message or provides other services with respect to that data message;

(f) "Information system" means a system for generating, sending, receiving, storing or otherwise processing data messages.

Article 3. Interpretation

(1) In the interpretation of this Law, regard is to be had to its international origin and to the need to promote uniformity in its application and the observance of good faith.

(2) Questions concerning matters governed by this Law which are not expressly settled in it are to be settled in conformity with the general principles on which this Law is based.

Article 4. Variation by agreement

(1) As between parties involved in generating, sending, receiving, storing or otherwise processing data messages, and except as otherwise provided, the provisions of chapter III may be varied by agreement.

(2) Paragraph (1) does not affect any right that may exist to modify by agreement any rule of law referred to in chapter II.

CHAPTER II. APPLICATION OF LEGAL REQUIREMENTS TO DATA MESSAGES

Article 5. Legal recognition of data messages

Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message.

Article 6. Writing

(1) Where the law requires information to be in writing, that requirement is met by a data message if the information contained therein is accessible so as to be usable for subsequent reference.

(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being in writing.

(3) The provisions of this article do not apply to the following: [...].

Article 7. Signature

(1) Where the law requires a signature of a person, that requirement is met in relation to a data message if:

(a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and

(b) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

(3) The provisions of this article do not apply to the following: [...].

I2

Article 8. Original

(1) Where the law requires information to be presented or retained in its original form, that requirement is met by a data message if:

(a) there exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form, as a data message or otherwise; and

(b) where it is required that information be presented, that information is capable of being displayed to the person to whom it is to be presented.

(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being presented or retained in its original form.

(3) For the purposes of subparagraph *(a)* of paragraph (1):

(a) the criteria for assessing integrity shall be whether the information has remained complete and unaltered, apart from the addition of any endorsement and any change which arises in the normal course of communication, storage and display; and

(b) the standard of reliability required shall be assessed in the light of the purpose for which the information was generated and in the light of all the relevant circumstances.

(4) The provisions of this article do not apply to the following: [...].

Article 9. Admissibility and evidential weight of data messages

(1) In any legal proceedings, nothing in the application of the rules of evidence shall apply so as to deny the admissibility of a data message in evidence:

(a) on the sole ground that it is a data message; or,

(b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.

(2) Information in the form of a data message shall be given due evidential weight. In assessing the evidential weight of a data message, regard shall be had to the reliability of the manner in which the data

message was generated, stored or communicated, to the reliability of the manner in which the integrity of the information was maintained, to the manner in which its originator was identified, and to any other relevant factor.

Article 10. Retention of data messages

(1) Where the law requires that certain documents, records or information be retained, that requirement is met by retaining data messages, provided that the following conditions are satisfied:

(a) the information contained therein is accessible so as to be usable for subsequent reference; and

(b) the data message is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and

(c) such information, if any, is retained as enables the identification of the origin and destination of a data message and the date and time when it was sent or received.

(2) An obligation to retain documents, records or information in accordance with paragraph (1) does not extend to any information the sole purpose of which is to enable the message to be sent or received.

(3) A person may satisfy the requirement referred to in paragraph (1) by using the services of any other person, provided that the conditions set forth in subparagraphs *(a)*, *(b)* and *(c)* of paragraph (1) are met.

CHAPTER III. COMMUNICATION OF DATA MESSAGES

Article 11. Formation and validity of contracts

(1) In the context of contract formation, unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by means of data messages. Where a data message is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole ground that a data message was used for that purpose.

(2) The provisions of this article do not apply to the following: [...].

I3

Article 12. Recognition by parties of data messages

(1) As between the originator and the addressee of a data message, a declaration of will or other statement shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message.

(2) The provisions of this article do not apply to the following: [...].

Article 13. Attribution of data messages

(1) A data message is that of the originator if it was sent by the originator itself.

(2) As between the originator and the addressee, a data message is deemed to be that of the originator if it was sent:

(a) by a person who had the authority to act on behalf of the originator in respect of that data message; or

(b) by an information system programmed by, or on behalf of, the originator to operate automatically.

(3) As between the originator and the addressee, an addressee is entitled to regard a data message as being that of the originator, and to act on that assumption, if:

(a) in order to ascertain whether the data message was that of the originator, the addressee properly applied a procedure previously agreed to by the originator for that purpose; or

(b) the data message as received by the addressee resulted from the actions of a person whose relationship with the originator or with any agent of the originator enabled that person to gain access to a method used by the originator to identify data messages as its own.

(4) Paragraph (3) does not apply:

(a) as of the time when the addressee has both received notice from the originator that the data message is not that of the originator, and had reasonable time to act accordingly; or

(b) in a case within paragraph (3)*(b)*, at any time when the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the data message was not that of the originator.

(5) Where a data message is that of the originator or is deemed to be that of the originator, or the addressee is entitled to act on that assumption, then, as between the originator and the addressee, the addressee is entitled to regard the data message as received as being what the originator intended to send, and to act on that assumption. The addressee is not so entitled when it knew or should have known, had it exercised reasonable care or used any agreed procedure, that the transmission resulted in any error in the data message as received.

(6) The addressee is entitled to regard each data message received as a separate data message and to act on that assumption, except to the extent that it duplicates another data message and the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the data message was a duplicate.

Article 14. Acknowledgement of receipt

(1) Paragraphs (2) to (4) of this article apply where, on or before sending a data message, or by means of that data message, the originator has requested or has agreed with the addressee that receipt of the data message be acknowledged.

(2) Where the originator has not agreed with the addressee that the acknowledgement be given in a particular form or by a particular method, an acknowledgement may be given by

(a) any communication by the addressee, automated or otherwise, or

(b) any conduct of the addressee, sufficient to indicate to the originator that the data message has been received.

(3) Where the originator has stated that the data message is conditional on receipt of the acknowledgement, the data message is treated as though it has never been sent, until the acknowledgement is received.

(4) Where the originator has not stated that the data message is conditional on receipt of the acknowledgement, and the acknowledgement has not been received by the originator within the time specified or

I4

agreed or, if no time has been specified or agreed, within a reasonable time, the originator:

(a) may give notice to the addressee stating that no acknowledgement has been received and specifying a reasonable time by which the acknowledgement must be received; and

(b) if the acknowledgement is not received within the time specified in subparagraph *(a)*, may, upon notice to the addressee, treat the data message as though it had never been sent, or exercise any other rights it may have.

(5) Where the originator receives the addressee's acknowledgement of receipt, it is presumed that the related data message was received by the addressee. That presumption does not imply that the data message corresponds to the message received.

(6) Where the received acknowledgement states that the related data message met technical requirements, either agreed upon or set forth in applicable standards, it is presumed that those requirements have been met.

(7) Except in so far as it relates to the sending or receipt of the data message, this article is not intended to deal with the legal consequences that may flow either from that data message or from the acknowledgement of its receipt.

Article 15. Time and place of dispatch and receipt of data messages

(1) Unless otherwise agreed between the originator and the addressee, the dispatch of a data message occurs when it enters an information system outside the control of the originator or of the person who sent the data message on behalf of the originator.

(2) Unless otherwise agreed between the originator and the addressee, the time of receipt of a data message is determined as follows:

(a) if the addressee has designated an information system for the purpose of receiving data messages, receipt occurs:

(i) at the time when the data message enters the designated information system; or

(ii) if the data message is sent to an information system of the addressee that is not the designated information system, at the time when the data message is retrieved by the addressee;

(b) if the addressee has not designated an information system, receipt occurs when the data message enters an information system of the addressee.

(3) Paragraph (2) applies notwithstanding that the place where the information system is located may be different from the place where the data message is deemed to be received under paragraph (4).

(4) Unless otherwise agreed between the originator and the addressee, a data message is deemed to be dispatched at the place where the originator has its place of business, and is deemed to be received at the place where the addressee has its place of business. For the purposes of this paragraph:

(a) if the originator or the addressee has more than one place of business, the place of business is that which has the closest relationship to the underlying transaction or, where there is no underlying transaction, the principal place of business;

(b) if the originator or the addressee does not have a place of business, reference is to be made to its habitual residence.

(5) The provisions of this article do not apply to the following: [...].

Part two. Electronic commerce in specific areas

CHAPTER I. CARRIAGE OF GOODS

Article 16. Actions related to contracts of carriage of goods

Without derogating from the provisions of part one of this Law, this chapter applies to any action in connection with, or in pursuance of, a contract of carriage of goods, including but not limited to:

(a) (i) furnishing the marks, number, quantity or weight of goods;

I5

(ii) stating or declaring the nature or value of goods;

(iii) issuing a receipt for goods;

(iv) confirming that goods have been loaded;

(b) (i) notifying a person of terms and conditions of the contract;

(ii) giving instructions to a carrier;

(c) (i) claiming delivery of goods;

(ii) authorizing release of goods;

(iii) giving notice of loss of, or damage to, goods;

(d) giving any other notice or statement in connection with the performance of the contract;

(e) undertaking to deliver goods to a named person or a person authorized to claim delivery;

(f) granting, acquiring, renouncing, surrendering, transferring or negotiating rights in goods;

(g) acquiring or transferring rights and obligations under the contract.

Article 17. Transport documents

(1) Subject to paragraph (3), where the law requires that any action referred to in article 16 be carried out in writing or by using a paper document, that requirement is met if the action is carried out by using one or more data messages.

(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for failing either to carry out the action in writing or to use a paper document.

(3) If a right is to be granted to, or an obligation is to be acquired by, one person and no other person, and if the law requires that, in order to effect this, the right or obligation must be conveyed to that person by the transfer, or use of, a paper document, that requirement is met if the right or obligation is conveyed by using one or more data messages, provided that a reliable method is used to render such data message or messages unique.

(4) For the purposes of paragraph (3), the standard of reliability required shall be assessed in the light of the purpose for which the right or obligation was conveyed and in the light of all the circumstances, including any relevant agreement.

(5) Where one or more data messages are used to effect any action in subparagraphs *(f)* and *(g)* of article 16, no paper document used to effect any such action is valid unless the use of data messages has been terminated and replaced by the use of paper documents. A paper document issued in these circumstances shall contain a statement of such termination. The replacement of data messages by paper documents shall not affect the rights or obligations of the parties involved.

(6) If a rule of law is compulsorily applicable to a contract of carriage of goods which is in, or is evidenced by, a paper document, that rule shall not be inapplicable to such a contract of carriage of goods which is evidenced by one or more data messages by reason of the fact that the contract is evidenced by such data message or messages instead of by a paper document.

(7) The provisions of this article do not apply to the following: [...].

INFORMATION TECHNOLOGY ACT, 1998
(No. of 1998)

ARRANGEMENT OF SECTIONS

ANNEXURE

Intituled
An Act to make provisions for the security and use of electronic transactions and for matters connected therewith.

PART I
PIRELIMINARY
Short title and commencement
1.-(1) This Act may be cited as the Information Technology Act, 1998.
Definitions
2. In this Act, unless the context otherwise requires –
"data" means a representation of information, knowledge, facts, concepts, or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed, or has been processed in a computer system or computer

network, and should be classified as intellectual property, and may be in any form, including computer printouts, magnetic storage media, punched cards, punched tapes, or stored internally in the memory of the computer;
"computer" means an electronic magnetic, optical or other high speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network;
"computer system" means a device or collection of devices, including support devices and excluding calculators which are not programmemable and capable of being used in conjunction with external files, or more of which contain computer programmes, electronic instructions, input data, and output data, that performs functions including, but not limited to, logic, arithmetic, data storage and retrieval, communication, and control;
"IT products" include computer, digital/data communication and digital/data broadcasting products, by recognising the progressive technological convergence of these three categories.
"IT software" means any representation of instructions, data, sound or image, including source code and object code, recorded in a machine readable form, and capable of being manipulated or providing interactivity to a user; by means of an automatic data processing machine falling under heading IT products; but does not include 'non-IT products';
"Computer Network" means the interconnection of one or more computers through :
(i) The use of satellite, microwave, line, or other communication media; and
(ii) Terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained.
"IT services" include, but is not limited to, computer time, data processing, or storage functions, or other uses of a computer, computer system, or computer network;
"computer system services" means utilisation of a computer, computer system, or computer network to assist an individual or entity with the performance of a particular lawful function which that individual or entity has been given the right, duty, and power, together with the responsibility, to perform;
"computer programme" means a set of instructions or statements, and related data, that when executed in actual or modified form, cause a computer, computer system, or computer network to perform specified functions;
"Computer data base" means a representation of information, knowledge, facts, concepts, or instructions that :
(i) Are being prepared or have been prepared in a formalised manner or are or have been produced by a computer, computer system, or computer network; and
(ii) Are intended for use in a computer, computer system, or computer network.
"Computer security system" means a software programme or computer device that :
(1) is intended to protect the confidentiality and secrecy of data and information stored in or accessible through the computer system; and
(2) displays a conspicuous warning to a user that the user is entering a secure system or requires a person seeking access to knowingly respond by use of an authorised code to the programme or device in order to gain access.
"electronic document" means electronic document/data/record/data message – information generated, sent, received or stored by electronic, optical, computer or similar means including, but not limited to, Electronic Data Interchange (EDI), electronic mail, telegram, telex or telephony;
"electronic signature" means any letters, characters, numbers or other symbols in digital form attached to or logically associated with an electronic record, and executed or adopted with the intention of authenticating or approving the electronic record;
"information" includes data, text, images, sound, codes, computer programmes, software and databases;
"computer output" or "output" means a statement or a representation whether in written, printed, pictorial, film, graphical, acoustic or other form-
(a) produced by a computer;
(b) displayed on the screen of a computer; or
(c) accurately translated from a statement or representation so produced;
"function" includes logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within a computer;
"Computer virus" means any computer instruction, information, data or programme that degrades the performance of a computer resource; disables; damages or destroys a computer resource; or attaches itself to another computer resource and executes when the host computer programme, data or instruction is executed or when some other event takes place in the host computer resource, data or instruction.
"computer contaminant" means any set of computer instructions that are designed to modify, damage, destroy, record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information. They include, but are not limited to, a group of computer instructions commonly called viruses or worms, which are self-replicating or self-propagating and are designed to contaminate other computer programmes or computer data, consume computer resources, modify, destroy, record, or transmit data, or in some other fashion usurp the normal operation of the computer, computer system, or computer network;
"Damage" means to destroy, alter, disrupt, delete, add, modify or rearrange any computer resource by any means.
"Disruption" means any deviation from normal operations of any computer, computer system, or computer network.
"Injury" includes addition, alteration, damage, deletion, destruction, denial of access with respect to data in, or functions of, a computer system or computer network.
"Property" includes financial instruments, data, computer software, computer programmes, documents associated with computer systems and computer programmes, or copies, whether tangible or intangible, and data while in transit.
"authorisation" means the express consent of a person which may include an employee's job description to use said person's computer, computer network, computer programme, computer software, computer system, property, or services as those terms are defined in this section.
"access" means to gain entry to, instruct, or communicate with the logical, arithmetical, or memory function resources of a computer, computer system or computer network;
"property" means anything of value as defined by law, and includes financial instruments, information, including electronically produced data and computer software and computer programmes in either machine or human readable form, and any other tangible or intangible items of value;
"premises" includes land, buildings, movable structures and any conveyance by land, water and air;
"injury" means any alteration, deletion, damage, destruction of a computer system, computer network, computer programme, or data caused by the access;

"supporting documentation" includes, but is not limited to, all information, in any form, pertaining to the design, construction, classification, implementation, use, or modification of a computer, computer system, computer network, computer programme, or computer software, which information is not generally available to the public and is necessary for the operation of a computer, computer system, computer network, computer programme, or computer software;
"asymmetric cryptosystem" means a system capable of generating a secure key pair, consisting of a private key for creating a digital signature, and a public key to verify the digital signature;
"certification authority" means a person who or an organisation that issues a certificate;
"certification practice statement" means a statement issued by a certification authority to specify the practices that the certification authority employs in issuing certificates;
"Controller" means the Controller of Certification Authorities;
"correspond", in relation to private or public keys, means to belong to the same key pair;
"digital signature" means an electronic signature consisting of a transformation of an electronic record using an, asymmetric cryptosystem and a hash function such that a person having the initial untransformed electronic record and the signer's public key can accurately determine –
(a) whether the transformation was created using the private key that corresponds to the signer's public key; and
(b) whether the initial electronic record has been altered since the transformation was made;
"hash function" means an algorithm mapping or translating one sequence of bits into another, generally smaller, set (the hash result) such that –
(a) a record yields the same hash result every time the algorithm is executed using the same record as input;
(b) it is computationally infeasible that a record can be derived or reconstituted from the harsh result produced by the algorithm; and
(c) it is computationally infeasible that two records can be found that produce the same hash result using the algorithm;
"key pair", in an asymmetric cryptosystem, means a private key and its mathematically related public key, having the property that the public key can verify a digital signature that the private key creates;
"licensed certification authority" means a certification authority licensed by the Controller;
"operational period of a certificate" begins on the date and time the certificate is issued by a certification authority (or on a later date and time if stated in the certificate), and ends on the date and time it expires as stated in the certificate or is earlier revoked or suspended;
"private key" means the key of a key pair used to create a digital signature;
"public key" means the key of a key pair used to verify a digital signature;
"repository" means a system for storing and retrieving certificates or other information relevant to certificates;
"revoke a certificate" means to permanently end the operational period of a certificate from a specified time;
"security procedure" means a procedure for the purpose of
(a) verifying that an electronic record. is that of a specific person; or
(b) detecting error or alteration in the communication, content or storage of an electronic record since a specific point in time,
which may require the use of algorithms or codes, identifying words or numbers, encryption, answerback or acknowledgment procedures, or similar security devices;
"signed" or "signature" and its grammatical variations includes any symbol executed or adopted, or any methodology or procedure employed or adopted, by a person with the intention of authenticating a record, including electronic or digital methods;
"subscriber" means a person who is the subject named or identified in a certificate issued to him and who holds a private key that corresponds to a public key listed in that certificate;
"suspend a certificate" means to temporarily suspend the operational period of a certificate from a specified time;
"trustworthy system" means computer hardware, software, and procedures that –
(a) are reasonably secure from intrusion and misuse;
(b) provide a reasonable level reliability and correct operation;
(c) are reasonably suited to performing intended functions; and
(d) adhere to generally accepted security procedures;
"valid certificate" means a certificate that a certification authority has issued and -which the subscriber listed in it has accepted;
"verify a digital signature", in relation to a given digital signature, record and public key, means to determine accurately –
(a) that the digital signature was created using the private key corresponding to the public key listed in the certificate; and
(b) the record has not been altered since its digital signature was created.

Purposes and construction

3. This Act shall be construed consistently with what is commercially reasonable under the circumstances and to give effect to the following purposes:
(a) to facilitate electronic communications by means of reliable electronic records;
(b) to facilitate electronic commerce, eliminate barriers to electronic commerce resulting from uncertainties over writing and signature requirements, and to promote the development of the legal and business infrastructure necessary to implement secure electronic commerce;
(c) to facilitate electronic filing of documents with government agencies and statutory corporations, and to promote efficient delivery of government services by means of reliable electronic records;
(d) to minimise the incidence of forged electronic records, intentional and unintentional alteration of records, and fraud in electronic commerce and other electronic transactions;
(e) to help to establish uniformity of rules, regulations and standards regarding the authentication and integrity of electronic records; and
(f) to promote public confidence in the integrity and reliability of electronic records and electronic commerce, and to foster 'the development of electronic commerce through the use of electronic signatures to lend authenticity and integrity to correspondence in any electronic medium.

Application

4.-(1) Part 11 or IV shall not apply to any law requiring writing or signatures in any of the following matters:
(a) the creation or execution of a will;
(b) negotiable instruments;
(c) the creation, performance or enforcement of an indenture, declaration of trust or power of attorney with the exception of constructive and resulting trusts;
(d) any contract for the sale or other disposition of immovable property, or any interest in such property;
(e) the conveyance of immovable property or the transfer of any interest in immovable property;

(f) documents of title.
(2) The Central Govt. may by order publish the official Gazette and modify the provisions of subsection (l) by adding, deleting or amending any class of transactions or matters.
Variation by agreement
5. As between parties involved in generating, sending, receiving, storing or otherwise processing electronic records, any provision of Part 11 or IV may be varied by agreement.

PART II
ELECTRONIC RECORDS AND SIGNATURES
GENERALLY
Legal recognition of electronic records
6.-(1) For the avoidance of doubt, -it is hereby declared that information shall not be denied legal effect, validity or enforceability solely on the ground that it is in the form of an electronic record.
(2) A "duplicate of a computer data file or programme file" shall mean a file produced by the same impression as the original, or from the same matrix, or by mechanical or electronic recording, in the normal way such a duplicate is produced on a computer, or by other equivalent techniques that accurately reproduce the original.
(3) A duplicate of a computer data file or programme file shall be admissible in evidence as original itself unless (1) a genuine question is raised as to the authenticity of the original or (2) in the circumstances it would be unfair to admit the duplicate in lieu of the original.
(4) If data is stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, shall be an original subject to satisfying the requirements referred to in section 70, 71 & 72.

Requirement for writing
7. Where a law requires information to be written, in writing, to be presented in writing or provides for certain consequences if it is not, an electronic record satisfies that rule of law if the information contained therein is accessible so as to be usable for subsequent reference.
Electronic signatures
8.-(1) Where a law requires a signature, or provides for certain consequences if a document is not signed, an electronic signature satisfies that rule of law.
(2) An electronic signature may be proved in any manner-, including by showing that a procedure existed by which it is necessary for a party, in order to proceed further with a transaction, to have executed a symbol or security procedure for the purpose of verifying that an electronic record is that of such party.
Retention of electronic records
9.-(1) Where a law requires that certain documents, records or information be retained, that requirement is satisfied by retaining them in the form of electronic records if the following conditions are satisfied:
(a) the information contained therein remains accessible so as to be usable for subsequent reference,
(b) the electronic record is retained in the format in which it was originally generated, sent or received, or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;
(c) such information, if any, as enables the identification of the origin and destination of an electronic record and the date and time when it was sent or received, is retained; and
(d) the consent of the department or ministry of the Central Govt., State Govt., or the statutory corporation under Central or State Govt. which has supervision over the requirement for the retention of such records has been obtained.
(2) An obligation to retain documents, records or information in accordance with subsection (1)(c) shall not extend to any information necessarily and automatically generated solely for the purpose of enabling a record to be sent or received.
(3) A person may satisfy the requirement referred to in subsection 9(1) by using the services of any other person, if the conditions in paragraphs (a) to (d) of that subsection are complied with.
(4) Nothing in this section shall –
(a) apply to any provisions of law which expressly provides for the retention of documents, records or information in the form of electronic records;
(b) preclude any department or ministry of the Central Government, State Govt. or a statutory corporation under Central or State Govt. from specifying additional requirements for the retention of electronic records that are subject to the jurisdiction of such department, ministry of Central Govt., State Govt. or statutory corporation under Central Govt. or State Govt.

PART III
LIABILITY OF NETWORK SERVICE PROVIDERS
Liability of network service providers
10.-(1) A network service provider shall not be subject to any civil or criminal liability under any rule of law in respect of third- party material in the form of electronic records to which he merely provides access if such liability is founded on -
(a) the making, publication, dissemination or distribution of such materials or any statement made in such material; or
(b) the infringement of any rights subsisting in or in relation to such material.
(2) Nothing in this section shall affect –
(a) any obligation founded on contract;
(b) the obligation of a network service provider as such under a licensing or other regulatory regime established under written law; or
(c) any obligation imposed under any written law or by a court to remove, block or deny access to any material.
(3) For the purposes of this section -
"providing access", in relation to third-party material, means the provision of the necessary technical means by which third-party material may be accessed and includes the automatic and temporary storage of the third-party material for the purpose of providing access;
"third-party", in relation to a network service provider, means a person over whom the provider has no effective control.

PART IV
ELECTRONIC CONTRACTS
Formation and validity
11.-(1) For the avoidance of doubt, it is hereby declared that in the context of the formation of contracts, unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by means of electronic records.
(2) Where an electronic record is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole ground that an electronic record was used for that purpose.
Effectiveness between parties
12. As between the originator and the addressee of an electronic record, a declaration of intent or other statement shall not be denied legal effect validity or enforceability solely on the ground that it is in the form of an electronic record.
Attribution
13.-(1) An electronic record is that of the originator if it was sent by the originator himself.
(2) As between the originator and the addressee, an electronic record is deemed to be that of the originator if it was sent -
(a) by a person who had the authority to act on behalf of the originator in respect of that electronic record; or
(b) by an information system programmemed by or on behalf of the originator to operate automatically.
(3) As between the originator and the addressee, an addressee is entitled to regard an electronic record as being that of the originator and to act on that assumption if -
(a) in order to ascertain whether the electronic record was that of the originator, the addressee properly applied a procedure previously agreed to by the originator for that purpose; or
(b) the data message as received by the addressee resulted from the actions of a person whose relationship with the originator or with any agent of the originator enabled that
person to gain access to a method used by the originator to identify electronic records as its own.
(4) Subsection (3) shall not apply -
(a) from the time when the addressee has both received notice from the originator that the electronic record is not that of the originator, and had reasonable time to act accordingly;
(b) in a case within subsection (3)(b), at any time when the addressee knew or ought to have known, had it exercised reasonable care or used any agreed procedure, that the electronic record was not that of the originator; or
(c) if in all the circumstances of the case, it is unconscionable for the addressee to regard the electronic record as that of the originator or to act on that assumption.
(5) Where an electronic record is that of the originator or is deemed to be that of the originator, or the addressee is entitled to act on that assumption, then, as between the originator and the addressee, the addressee is entitled to regard-the electronic record received as being what the originator intended to send, and to act on that assumption.
(6) The addressee is not so entitled when the addressee knew or should have known, had the addressee exercised reasonable care or used any agreed procedure, that the transmission resulted in any error in the electronic record as received.
(7) The addressee is entitled to regard each electronic record received as a separate electronic record and to act on that assumption, except to the extent that the addressee duplicates another electronic record and the addressee knew or should have known, had the addressee exercised reasonable care or used any agreed procedure, that the electronic record was a duplicate.
(8) Nothing in this section shall affect the law of agency or the law on the formation of contracts.
Acknowledgment of receipt
14.-(1) Subsections (2), (3) and (4) shall apply where, on or before sending an electronic record, or by means of that electronic record, the originator has requested or has agreed with the addressee that receipt of the electronic record be acknowledged.
(2) Where the originator has not agreed with the addressee that the acknowledgment be given in a particular form or by a particular method, an acknowledgment may be given by -
(a) any communication by the addressee, automated or otherwise; or
(b) any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received.
(3) Where the originator has stated that the electronic record is conditional on receipt of the acknowledgment, the electronic record is treated as though it had never been sent, until the acknowledgment is received.
(4) Where the originator has not stated that the electronic record is conditional on receipt of the acknowledgment, and the acknowledgment has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed within a reasonable time, the originator –
(a) may give notice to the addressee stating that no acknowledgment has been received and specifying a reasonable time by which the acknowledgment must be received; and
(b) if the acknowledgment is not received within the time specified in paragraph (a), may, upon notice to the addressee, treat the electronic record as though it has never been sent, or exercise any other rights it may have.
(5) Where the originator receives the addressee's acknowledgment of receipt, it is presumed, unless evidence to the contrary is adduced, that the related electronic record was received by the addressee, but that presumption does not imply that the content of the electronic record corresponds to the content of the record received.
(6) Where the received acknowledgment, states that the related electronic record met technical requirements, either agreed upon or set forth in applicable standards, it is presumed, unless evidence to the contrary is adduced, that those requirements have been met.
(7) Except in so far as it relates to the sending or receipt of the electronic record, this Part is not intended to deal with the legal consequences that may flow either from that electronic record or from the acknowledgment of its receipt.
Time and place of despatch and receipt
15.-(1) Unless otherwise agreed to between the originator and the addressee, the despatch of an electronic record occurs when it enters an information system outside the control of the originator or the person who sent the electronic record on behalf of the originator.
(2) Unless otherwise agreed between the originator and the addressee, the time of receipt of an electronic record is determined as follows:
(a) if the addressee has designated an information system for the purpose of receiving electronic records, receipt occurs–
(i) at the time when the electronic record enters the designated information system; or
(ii) if the electronic record is sent to an information system of the addressee that is not the designated information system, at the time when the electronic record is retrieved by the addressee;
(b) if the addressee has not designated an information system, receipt occurs when the electronic record enters an information system of the addressee.

(3) Subsection (2) shall apply notwithstanding that the place where the information system is located may be different from the place where the electronic record is deemed to be received under subsection (4).
(4) Unless otherwise agreed between the originator and the addressee, an electronic record is deemed to be despatched at the place where the originator has its place of business, and is deemed to be received at the place where the addressee has its place of business.
(5) For the purposes of this section –
(a) if the originator or the addressee has more than one place of business, the place of business is that which has the closest relationship to the underlying transaction or, where there is no underlying transaction, the principal place of business;
(b) if the originator or the addressee does not have a place of business, reference is to be made to the usual place of residence; and
(c) "usual place of residence" in relation to a body corporate, means the place where it is incorporated or otherwise legally constituted.
(6) This section shall not apply to such circumstances as may be prescribed by appropriate regulation by the President.

PART V
SECURE ELECTRONIC RECORDS AND SIGNATURES
Secure electronic record
16.-(1) If a prescribed security procedure or a commercially reasonable security procedure agreed to by the parties involved has been properly applied to an electronic record to verify that the electronic record has not been altered since a specified point in time, such record shall be treated as a secure electronic record from such specified point in time to the time of verification.
(2) For the purposes of this section and section 17, whether a security procedure is commercially reasonable shall be determined having regard to the purposes of the procedure and the commercial circumstances at the time the procedure was used, including -
(a) the nature of the transaction;
(b) the sophistication of the parties;
(c) the volume of similar transactions engaged in by either or all parties;
(d) the availability of alternatives offered to but rejected by any party;
(e) the cost of alternative procedures; and
(f) the procedures in general use for similar types of transactions.
Secure electronic signature
17. If, through the application of a prescribed security procedure or a commercially reasonable security procedure agreed to by the parties involved, it can be verified that an electronic signature was, at the time it was made –
(a) unique to the person using it;
(b) capable of identifying such person;
(c) created in a manner or using a means under the sole control of the person using it; and
(c) is linked to the electronic record to which it relates in a manner such that if the record was changed the electronic signature would be invalidated,
such signature shall be treated as a secure electronic signature.
Presumptions relating to secure electronic records and signatures
18.-(1) In any proceedings involving a secure electronic record, it shall be presumed, unless evidence to the contrary is adduced, that the secure electronic record has not been altered since the specific point in time to which the secure status relates.
(2) In any proceedings involving a secure electronic signature, it
shall be presumed, unless evidence to the contrary is adduced, that –
(a) the secure electronic signature is the signature of the person to whom it correlates; and
(b) the secure electronic signature was affixed by that person with the intention of signing or approving the electronic record.
(3) In the absence of a secure electronic record or a secure electronic signature, nothing in this Part shall create any presumption relating to the authenticity and integrity of the electronic record or an electronic signature.
(4) For the purposes of this section -
"secure electronic record" means an electronic record treated as a secure electronic record by virtue of section 16 or 19;
"secure electronic signature" means an electronic signature treated as a secure electronic, signature by virtue of section 17 or 20.

PART VI
EFFECT OF DIGITAL SIGNATURES
Secure electronic record with digital signature
19. The portion of an electronic record that is signed with a digital signature shall be treated as a secure electronic record if the digital signature is a secure electronic signature by virtue of section 20.
Secure digital signature
20. When any portion of an electronic record is signed with a digital signature, the digital signature shall be treated as a secure electronic signature with respect to such portion of the record, if -
(a) the digital signature was created during the operational period of a valid certificate and is verified by reference to the public key listed in such certificate; and
(b) the certificate is considered trustworthy, in that it is an accurate binding of a public key to a person's identity because -
(i) the certificate was issued by a licensed certification authority operating in compliance with the regulations made under section 42;
(ii) the certificate was issued by a certification authority outside India recognised for this purpose by the Controller pursuant to regulations made under section 43;
(iii) the certificate was issued by a department or ministry of the Central Government, State Govt. or a statutory corporation of Central or State Govt. approved by Central Govt. to act as a certification authority on such conditions as he may by regulations impose or specify; or
(iv) the parties have expressly agreed between themselves (sender and recipient) to use digital signatures as a security procedure, and the digital signature was properly verified by reference to the sender's public key.
Presumptions regarding certificates
21. It shall be presumed, unless evidence to the contrary is adduced, that the information listed in a certificate issued by a licensed certification authority is correct, except for information identified as subscriber information which has not been verified, if the certificate was accepted by the subscriber.
Unreliable digital signatures

22. Unless otherwise provided by law or contract, a person relying on a digitally signed electronic record assumes the risk that the digital signature is invalid as a signature or authentication of the signed electronic record, if reliance on the digital signature is not reasonable under the circumstances having regard to the following factors :
(a) facts which the person relying on the digitally signed electronic record knows or has notice of, including all facts listed in the certificate or incorporated in it by reference;
(b) the value or importance of the digitally signed record, if known;
(c) the course of dealing between the person relying on the digitally signed electronic record and the subscriber and any available indicia of reliability or unreliability apart from the digital signature; and
(d) usage of trade, particularly trade conducted by trustworthy systems or other electronic means.

PART VII
GENERAL DUTIES RELATING TO DIGITAL SIGNATURES
Reliance on certificates forseeable
23. It is foreseeable that persons relying on a digital signature will also rely on a valid certificate containing the public key by which the digital signature can be verified.
Prerequisites to publication of certificate
24. No one may publish a certificate or otherwise make it available to a person known by that person to be in a position to rely on the certificate or on a digital signature that is verifiable with reference to a public key listed in the certificate, if that person knows that –
(a) the certification authority listed in the certificate has not issued it;
(b) the subscriber listed in the certificate has not accepted it; or
(c) the certificate has been revoked or suspended, unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation.
Publication for fraudulent purpose
25. Any person who knowingly creates, publishes or otherwise makes available a certificate for any fraudulent or unlawful purpose shall be guilty of an offence and shall be liable on conviction to a fine not exceeding Rs. 1,00,000 or to imprisonment for a term not exceeding 7 years or to both.
False or unauthorised request
26. Any person who knowingly misrepresents to a certification authority his identity or authorisation for the purpose of requesting for a certificate or for suspension or revocation of a certificate shall be guilty of an offence and shall be liable on conviction to a fine not exceeding Rs. 50,000 or to imprisonment for a term not exceeding 3 years or to both.

PART VIII
DUTIES OF CERTIFICATION AUTHORITIES
Trustworthy system
27. A certification authority must utilise trustworthy systems in performing its services.
Disclosure
28.-(1) A certification authority shall disclose -
(a) its certificate that contains the public key corresponding to the private key used by that certification authority to digitally sign another certificate (referred to in this section as a certification authority certificate);
(b) any relevant certification practice statement;
(c) notice of the revocation or suspension of its certification authority certificate; and
(d) any other fact that materially and adversely affects either the reliability of a certificate that the authority has issued or the authority's ability to perform its services.
(2) In the event of an occurrence that materially and adversely affects a certification authority's trustworthy system or its certification authority certificate, the certification authority shall -
(a) use reasonable efforts to notify any person who is known to be or foreseeably will be affected by that occurrence; or
(b) act in accordance with procedures governing such an occurrence specified in its certification practice statement.
Issuing of certificate
29.-(1) A certification authority may issue a certificate to a prospective subscriber only after the certification authority -
(a) has received a request for issuance from the prospective . subscriber; and
(b) has -
(i) if it has a certification practice statement, complied with all of the practices and procedures set forth in such certification practice statement including procedures regarding identification of the perspective subscriber; or
(ii) in the absence of a certification practice statement,
complied with the conditions in subsection (2).
(2) In the absence of a certification practice statement, the certification authority shall confirm by itself or through an authorised agent that -
(a) the prospective subscriber is the person to be listed in the certificate to be issued;
(b) if the prospective subscriber is acting through one or more agents, the subscriber authorised the agent to have custody of the subscriber's private key and to request issuance of a certificate listing the corresponding public key;
(c) the information in the certificate to he issued is accurate;
(d) the prospective subscriber rightfully holds the private key
corresponding to the public key to be listed in the certificate;
(e) the prospective subscriber holds a private key capable of creating a digital signature; and
(f) the public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the prospective subscriber.
Representations upon issuance of certificate
30.-(1) By issuing a certificate, a certification authority represents, to any person who reasonably relies on the certificate or a digital signature verifiable by the public key listed in the certificate, that the certification authority has issued the certificate in accordance with any applicable certification practice statement incorporated by reference in the certificate, or of which the relying person has notice.
(2) In the absence of such certification practice statement, the certification authority represents that it has confirmed that -

(a) the certification authority has complied with all applicable requirements of this Act in issuing the certificate, and if the certification authority has published the certificate or otherwise made it available to such relying person, that the subscriber listed in the certificate has accepted it;
(b) the subscriber identified in the certificate holds the private key corresponding to the public key, listed in the certificate;
(c) the subscriber's public key and private key constitute a functioning key pair;
(d) all information in the certificate is accurate, unless the certification authority has stated in the certificate or incorporated by reference in the certificate a statement that the accuracy of specified information is not confirmed; and
(e) that the certification authority has no knowledge of any material fact which if it had been included in the certificate would adversely affect the reliability of the representations in paragraphs (a) to (d).
(3) Where there is an applicable certification practice statement which has been incorporated by reference in the certificate, or of which the relying person has notice, subsection (2) shall apply to the extent that the representations are not inconsistent with tile certification practice statement.
Suspension of certificate
31. Unless the certification authority and the subscriber agree otherwise, the certification authority that issued a certificate shall suspend the certificate as soon as possible after receiving a request by a person whom the certification authority reasonably believes to be -
(a) the subscriber listed in the certificate;
(b) a person duly authorised to act for that subscriber; or
(c) a person acting on behalf of that subscriber, who is unavailable.
Revocation of certificate
32. A certification authority shall revoke a certificate that it issued after -
(a) receiving a request for revocation by the subscriber named in the certificate; and confirming that the person requesting revocation is the subscriber, or is an agent of the subscriber with authority to request the revocation;
(b) receiving a certified copy of the subscriber's death certificate, or upon confirming by other evidence that the subscriber is dead; or
(c) upon presentation of documents effecting a dissolution of the subscriber or upon confirming by other evidence that the subscriber has been dissolved or has ceased to exist.
Revocation without subscriber's consent
33.-(1) A certification authority shall revoke a certificate, regardless of whether the subscriber listed in the certificate consents, if the certification authority confirms that -
(a) a material fact represented in the certificate is false;
(b) a requirement for issuance of the certificate was not satisfied;
(c) the certification authority's private key or trustworthy system was compromised in a manner materially affecting the certificate's reliability;
(d) an individual subscriber is dead; or
(e) a subscriber has been dissolved, wound-up or otherwise ceased to exist.
(2) Upon effecting such a revocation, other than under subsection (1)(a) or (e), the certification authority shall immediately notify the subscriber listed in the revoked certificate.
Notice of suspension
34.-(1) Immediately upon suspension of a certificate by a certification authority, the certification authority shall publish a signed notice of the suspension in the repository specified in the certificate for publication of notice of suspension.
(2) Where one or more repositories are specified, the certification authority shall publish signed notices of the suspension in all such repositories.
Notice of revocation
35.-(1) Immediately upon revocation of a certificate by a certification authority, the certification authority shall publish a signed notice of the revocation in the repository specified in the certificate for publication of notice of revocation.
(3) Where one or more repositories are specified, the certification authority shall publish signed notices of the revocation in all such repositories.

PART IX
DUTIES OF SUBSCRIBERS
Generating key pair
36.-(1) If the subscriber generates the key pair whose public key is to be listed in a certificate issued by a certification authority and accepted by the subscriber, the subscriber shall generate that key pair using a trustworthy system.
(2) This section shall not apply to a subscriber who generates the key pair using a system approved by the certification authority.
Obtaining certificate
37. All material representations made by the subscriber to a certification authority for purposes of obtaining a certificate, including all information known to the subscriber and represented in the certificate, shall be accurate and complete to the best of the subscriber's knowledge and belief,- regardless of whether such representations are confirmed by the certification authority.
Acceptance of certificate
38.-(1) A subscriber shall be deemed to have accepted a certificate if he -
(a) publishes or authorises the publication of a certificate;
(i) to one or more persons; or
(ii) in a repository; or
(b) otherwise demonstrates approval of a certificate while knowing or having notice of its contents.
(2) By accepting a certificate issued by himself or a certification authority, the subscriber listed in the certificate certifies to all who reasonably rely on the information contained in the certificate that -
(a) the subscriber rightfully holds the private key corresponding to the public key listed in the certificate;
(b) all representations made by the subscriber to the certification authority and material to the information listed in the certificate are true; and
(c) all information in the certificate that is within the knowledge of the subscriber is true.

Control of private key

39.-(1) By accepting a certificate issued by a certification authority, the subscriber identified in the certificate assumes a duty to exercise reasonable care to retain control of the private key corresponding to the public key listed in such certificate and prevent its disclosure to a person not authorised to create the subscriber's digital signature.

(2) Such duty shall continue during the operational period of the certificate and during any period of suspension of the certificate.

Initiating suspension or revocation

40. A subscriber who has accepted a certificate shall as soon as possible request the issuing certification authority to suspend or revoke the certificate if the private key corresponding to the public key listed in the certificate has been compromised.

PART X

REGULATION OF CERTIFICATION AUTHORITIES

Appointment of Controller and other officers

41.-(1) The Central Govt. shall appoint a Controller of Certification Authorities for the purposes of this Act and, in particular, for the purposes of licensing, certifying, monitoring and overseeing the activities of certification authorities.

(2) The Controller may, after consultation with the Central Govt., appoint such number of Deputy and Assistant Controllers of Certification Authorities and officers as the Controller considers necessary to exercise and perform all or any of the powers and duties of the Controller under this Act or any regulations made thereunder.

(3) The Controller, the Deputy and Assistant Controllers and officers appointed by the Controller under subsection (2) shall exercise, discharge and perform the powers, duties and functions conferred on the Controller under this Act or any regulations made thereunder subject to such directions as may be notified by the President of India.

(4) The Controller shall maintain a publicly accessible database containing a certification authority disclosure record for each licensed certification authority which shall contain all the particulars required under the regulations made under this Act.

(5) In the application of the provisions of this Act to certificates issued by the Controller and digital signatures verified by reference to those certificates, the Controller shall be deemed to be a licensed certification authority.

Regulation of certification authorities

42.-(1) The Central Govt. may make regulations for the regulation and licensing of certification authorities and to define when a digital signature qualifies as a secure electronic signature.

(2) Without prejudice to the generality of subsection (1), the Central Govt. may make regulations for or with respect to –

(a) applications for licences or renewal of licences of certification authorities and their authorised representatives and matters incidental thereto;

(b) the activities of certification authorities including the manner, method and place of soliciting business, the conduct of such solicitation and the prohibition of such solicitation from members of the public by certification authorities which are not licensed;

(c) the standards to be maintained by certification authorities;

(d) prescribing the appropriate standards with respect to the qualifications, experience and training of applicants for any licence or their employees;

(e) prescribing the conditions for the conduct of business by a certification authority;

(f) providing for the content and distribution of written, printed or visual material and advertisements that may be distributed or used by a person in respect of a digital certificate or key;

(g) prescribing the form and content of a digital certificate or key;

(h) prescribing the particulars to be recorded in,. or in respect of, accounts kept by certification authorities;

(i) providing for the appointment and remuneration of an auditor appointed under the regulations and for the costs of an audit carried out under the regulations;

(j) providing for the establishment and regulation of any electronic system by a certification authority, whether by itself or in conjunction with other certification authorities, and for the imposition and variation of such requirements, conditions or restrictions as the Controller may think fit;

(k) the manner in which a holder of a licence conducts its dealings with its customers, conflicts of interest involving the holder of a licence and its customers, and the duties of a holder of a licence to its customers with respect to digital certificates ;

(l) prescribing any forms for the purposes of the regulations; and

(m) prescribing fees to be paid in respect of any matter or thing required for the purposes of this Act or the regulations.

(3) Regulations made under this section may provide that a contravention of a specified provision shall be an offence and may provide penalties not exceeding a fine of Rs. 2,00,000 or imprisonment for a term not exceeding 12 months or both.

Recognition of foreign certification authorities

43.- The Central Govt. may by regulations provide that the Controller may recognise certification authorities outside India that satisfy the prescribed -requirements for any of the following purposes:

(a) the recommended reliance limit, if any, specified in a certificate issued by the certification authority;

(b) the presumption referred to in sections 20(b)(ii) and 21.

Recommended reliance limit

44.-(1) A licensed certification authority shall, in issuing a certificate to a subscriber, specify a recommended reliance limit in the certificate.

(2) The licensed certification authority may specify different limits in different certificates as it considers fit

Liability limits for licensed certification authorities

45. Unless a licensed certification authority waives the application of this section, a licensed certification authority –

(a) shall not be liable for any loss caused by reliance on a false or forged digital signature of a subscriber, if, with respect to the false or forged digital signature, the licensed certification authority complied with the requirements of this Act;

(b) shall not be liable in excess of the amount specified in the certificate as its recommended reliance limit for either –

(i) a loss caused by reliance on a misrepresentation in the certificate of any fact that the licensed certification authority is required to confirm; or

(ii) failure to comply with sections 29 and 30 in issuing the certificate.

Regulation of repositories

46. The Central Govt. may make regulations for the purpose of ensuring the quality of repositories and the services they provide including provisions for the standards, licensing or accreditation of repositories.

PART XI
GOVERNMENT USE OF ELECTRONIC RECORDS AND SIGNATURE

Acceptance of electronic filing and issue of documents

47.-(1) Any department or ministry of Central Government, State Govt. or statutory corporation under Central or State Govt. that, pursuant to any written law –

(a) accepts the filing of documents, or requires that documents be created or retained;

(b) issues any permit, licence or approval; or

(c) provides for the method and manner of payment, may, notwithstanding anything to the contrary in such written law –

(i) accept the filing of such documents, or the creation or retention of such documents in the form of electronic records; -

(ii) issue such permit, licence -or approval in the form of electronic records; or

(iii) make such payment in electronic form.

(2) In any case where a department or ministry of Central Government, State Govt. or statutory corporation under Central or State Govt. decides to perform any of the functions in subsection (1)(i), (ii) or (iii), such agency may specify –

(a) the manner and format in which such electronic records shall be filed, created, retained or issued;

(b) where such electronic records have to be signed, the type of electronic signature required (including, if applicable, a requirement that the sender use a digital signature or other secure electronic signature);

(c) the manner and format in which such signature shall be affixed to the electronic record, and the identity of or criteria that shall be met by any certification authority used by the person filing the document;

(d) control processes and procedures as appropriate to ensure adequate integrity, security and confidentiality of electronic records or payments; and

(e) any other required attributes for electronic records or payments that are currently specified for corresponding paper documents.

(3) Nothing in this Act shall by itself compel any department or ministry of the Central Government, State Govt. or statutory corporation under Central or State Govt. to accept or issue any document in the form of electronic records.

PART XII
GENERAL

Obligation of confidentiality

48.-(1) Except for the purposes of this Act or for any prosecution for an offence under any written law or pursuant to an order of court, no person who has, pursuant to any powers conferred under this Part, obtained access to any electronic record, book, register, correspondence, information, document or other material shall disclose such electronic record, book, register, correspondence, information, document or other material to any other person.

(2) Any person who contravenes subsection (1) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding Rs. 2,00,000 or to imprisonment for a term not exceeding 3 years or to both.

Offence by body corporate

49. Where an offence under this Act or any regulations made thereunder is committed by a body corporate, and it is proved to have been committed with the consent or connivance of, or to be attributable to any act or default on the part of, any director, manager, secretary or other similar officer of the body corporate, or any person who was purporting to act in any such capacity, he, as well as the body corporate, shall be guilty of that offence and shall be liable to be proceeded against and punished accordingly.

Authorised officer

50.-(1) The Controller may in writing authorise any officer or employee to exercise any of the powers of the Controller under this Part.

(2) The Controller and any such officer shall be deemed to be a public servant for the purposes of the Penal Code.

(3) In exercising any of the powers of enforcement under this Act, an authorised officer shall on demand produce to the person against whom he is acting the authority issued to him by the Controller.

Controller may give directions for compliance

51.-(1) The Controller may by notice in writing direct a certification authority or any officer or employee thereof to take such measures or stop carrying on such activities as are specified in the notice if they are necessary to ensure - compliance with the provisions of this Act or any regulations made thereunder.

(2) Any person who fails to comply with any direction specified in a notice issued under subsection (1) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding Rs. 2,00,000 or to imprisonment for a term not exceeding 3 years or to both.

Power to investigate

52.-(1) The Controller or an authorised officer may investigate the activities of a certification authority in relation to its compliance with this Act and any regulations made thereunder.

(2) For the purposes of subsection (1), the Controller may in writing issue an order to a certification authority to further its investigation or to secure compliance with this Act or any regulations made thereunder.

Access to computers and data

53.-(1) The Controller or an authorised officer shall-

(a) be entitled at any time to-

(i) have access to and inspect and check the operation of any computer system and any associated apparatus or material which he has reasonable cause to suspect is or has been in use in connection with any offence under this Act;

(ii) use or caused to be used any such computer system to search any data contained in or available to such computer system; or

(b) be entitled to require -

(i) the person by whom or on whose behalf the Controller or authorised officer has reasonable cause to suspect the computer is or has been so used; or

(ii) any person having charge of, or otherwise concerned with the. operation of, the computer, apparatus or material,

to provide him with such reasonable technical and other assistance as he may require for the purposes of paragraph (a).

(2) Any person who obstructs the lawful exercise of the powers under subsection (1)(a) or who fails to comply with a request under subsection (1)(b) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding Rs. 1,00,000 or to imprisonment for a term not exceeding 6 months or to both.

Obstruction of authorised officer

54. Any person who obstructs, impedes, assaults or interferes with the Controller or any authorised officer in the performance of his functions under this Act shall be guilty of an offence.

Production of documents, data, etc

55. The Controller or an authorised officer shall, for the purposes of the execution of this Act, have power to do all or any of the following:

(a) require the production of records, accounts, data and documents kept by a licensed certification authority and to inspect, examine and copy any of them;

(b) require the production of any identification document from any person in relation to any offence under this Act or any regulations made thereunder-; and

(c) make such inquiry as may be necessary to ascertain whether the provisions of this Act or any regulations made thereunder have been complied with.

General penalties

56. Any person guilty of an offence under this Act or any regulations made thereunder for which no penalty is expressly provided shall be liable on conviction to a fine not exceeding 1,00,000 or to imprisonment for a term not exceeding 6 months or to both.

Sanction of Public Prosecutor

57. No prosecution in respect of any offence under this Act or any regulations made thereunder shall be instituted except by or with the sanction of the Public Prosecutor.

Jurisdiction of Courts

58. A District Court or a Magistrate's Court shall have jurisdiction to hear and determine all offences under this Act and any regulations made thereunder, notwithstanding anything to the contrary in the Criminal Procedure Code, shall have power to impose the full penalty or punishment in respect of any offence under this Act or any regulations made thereunder.

Composition of offences

59.-(1) The Controller may, in his discretion, compound any offence under this Act or any regulations made thereunder which is prescribed as being an offence which may be compounded by collecting from the person reasonably suspected of having committed the offence a sum not exceeding Rs. 1,00,000.

(2) The Central Govt. may make regulations prescribing the offences which may be compounded.

Power to exempt

60. The Central Govt. may exempt, subject to such terms and conditions as he thinks fit, any person or class of persons from all or any of the provisions of this Act or any regulations made thereunder.

Regulations

61. The Central Govt. may make regulations to prescribe anything which is required to be prescribed under this Act and generally for the carrying out of the provisions of this Act.

Savings and transitional

62.-(1) Where a certification authority has been carrying on or operating as a certification authority before the appointed day and it has obtained a licence in accordance with the regulations made under section 42 within 6 months after the appointed day, all certificates issued by such certification authority before the commencement of this Act, to the extent that they satisfy the requirements under this Act or any regulations made thereunder, shall be deemed to have been issued under this Act by a licensed certification authority and shall have effect accordingly.

(2) In this section, "appointed day" means the date of commencement of this Act.

PART XIII

COMPUTER CRIME AND DATA PROTECTION

Offences

63.-(1) For the purpose of this act, except as provided in subsection (6), any person who commits any of the following acts is guilty of public offence of computer crime:

(a) Knowingly or intentionally accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer data base, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.

(b) Knowingly or intentionally accesses and without permission takes, copies, or makes use of any data or computer data base from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network. Any programme or data held in any removable storage medium which is for the time being in the computer; and a computer is to be regarded as containing any programme or data held in any such medium.

(c) Knowingly or intentionally and without permission uses or causes to be used computer services.

(d) Knowingly or intentionally accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, computer programmes or computer data base which reside or exist internal or external to a computer, computer system, or computer network.

(e) Knowingly or intentionally and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorised user of a computer, computer system, or computer network.

(f) Knowingly or intentionally and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section.

(g) Knowingly or intentionally and with the intent to defraud, obtains, or attempts to obtain, or aids or abets another in obtaining, any commercial computer service by false representation, false statement, unauthorised charging to the account of another, by installing or tampering with any facilities or equipment or by any other means.

(h) Knowingly or intentionally and without permission accesses or causes to be accessed any computer, computer system, or computer network.

(i) Knowingly or intentionally introduces or allows the introduction of any computer contaminant or computer virus into any computer, computer system, or computer network.

(j) Destruction of computer equipment without authorisation, intentionally or recklessly tempers with, takes, transfers, conceals, alters, damages or destroys any equipment used in computer system, or intentionally or recklessly causes any of the foregoing to occur.

(k) Whoever knowingly, wilfully and without authorisation or without reasonable grounds to believe to have such authorisation, destroys, uses, takes, injures, or damages equipment or supplies used for intended to be used in a computer, computer system, or computer network,

or whoever willfully, knowingly, and without authorisation or without reasonable grounds to believe to have authorisation, destroys, injures, takes, or damages any computer, computer system, or computer network.
(2)-(A) Any person who commits offence as per any of the provisions of paragraphs (a), (b), (d), (e), (g) and (j) of subsection (1) is punishable by a fine up to Rs. 2,00,000 or by imprisonment up to three years, or by both.
(B) Any person who commits offence as per para (c) of subsection (1) is punishable as follows :
(i) For the first violation which does not result in injury, and where the value of the computer services used does not exceed Rs. 10,000, by a fine not exceeding Rs. 1,00,000, or by imprisonment not exceeding one year, or by both.
(ii) For any violation which results in damage of an amount greater than Rs. 1,00,000 or in an injury, or if the value of the computer services used exceeds Rs. 10,000, or for any second or subsequent violation, by a fine not exceeding Rs. 2,00,000, or by imprisonment up to three years, or by both.
(C) Any person who commits offence as per para (f), (h) or (i) of subsection (1) is punishable as follows :
(i) For a first violation which does not result in injury, an infraction punishable by a fine not exceeding Rs. 10,000.
(ii) For any violation which results in a damage of an amount not greater than Rs. 50,000, or for a second or subsequent violation, by a fine not exceeding Rs. 1,00,000 or by imprisonment not exceeding one year, or by both.
(iii) For any violation which results in a victim loss/damage in an amount greater than Rs. 50,000, by a fine not exceeding Rs. 2,00,000, or by imprisonment up to three years, or by both.
(D) Any person who commits the offence at paragraph (k) of subsection (1) is punishable as follows:
(i) Any person who commits the offence at paragraph (j) of subsection (1) is punishable of a fine not exceeding Rs. 1,00,000 if the damage to such computer, equipment or supplies or to the computer, computer system or computer network is less than Rs. 20,000.
(ii) Any person who violates any of the provisions of paragraph (j) of subsection (1) is punishable by a fine up to Rs. 5,00,000 if the damage to such computer equipment or supplies or to computer, computer system or computer network exceeds Rs. 20,000, or if there is an interruption or impairment of governmental operation, public transportation, supply of water, gas or public utility service.
(3) In addition to any other civil remedy available, the owner or lessee of the computer, computer system, computer network, computer programme, or data may bring a civil action against any person convicted under this section for compensatory damages, including any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer programme, or data was or was not altered, damaged, or deleted by the access.
(4) No activity exempted from prosecution under paragraph (a) of subsection (1) which incidentally violates paragraph (d) or paragraph (h) of subsection (1) shall be prosecuted under those prosecutions.
(5)(i) Subsection (1) does not apply to any person who accesses his or her employer's computer system, computer network, computer programme or data when acting within the scope of his or her lawful employment.
(ii) Paragraph (C) of subsection (1) does not apply to any employee who accesses or uses his or her employer's computer system, computer network, computer programme or data when acting outside the scope of his or her lawful employment, so long as the employer's activities do not cause an injury to the employer or another, or so long as the value of supplies and computer services, which are used and do not exceed an accumulated total of Rs. 10,000.
Tampering with computer source documents
64.-(1) Whoever knowingly or intentionally conceals, destroys, or alters or intentionally or knowingly causes another to conceal, destroy, or alter any computer source document used for a computer, computer programme, computer system, or computer network, when the computer source document is required to be kept by law, shall be guilty of an offence of computer crime.
(2) Whoever knowingly or intentionally conceals, destroys, or alters or intentionally, knowingly conceals, destroys, or alters or intentionally or knowingly causes another to conceal, destroy, or alter any computer source document used for a computer, computer programme, computer system, or computer network, when the computer source document is required to be kept by law, with the intent to obstruct an official investigation by any state agency authrised by law to conduct any civil or criminal investigation, shall be guilty of public offence of computer crime.
(3) Any person who commits offence at subsection (1) is punishable by a fine up to Rs. 2,00,000 or by imprisonment up to six months, or by both.
(4) Any person who commits offence at subsection (2) is punishable by a fine up to Rs. 3,00,000 or by imprisonment up to six months, or by both.
Forfeiture
65.-(1) Any person who commits the offence of computer crime as set forth in Section 63 and Section 64 shall forfeit, according to the provisions of this Section, any monies, profits or proceeds, and any interest or property which the sentencing court determines he has acquired or maintained, directly or indirectly, in whole or in part, as a result of such offence. Such person shall also forfeit any interest in, security, claim against, or contractual right of any kind which affords him a source of influence over any enterprise which he has established, operated, controlled, conducted or participated in conducting, where his relationship to or connection with any such thing or activity directly or indirectly, in whole or in part, is traceable to any item or benefit which he has obtained or acquired through computer fraud.
(2) Any computer, computer system, computer network, or any software or data, owned by the person, which is used during the commission of any public offence described in section 63 and section 64 or any computer, owned by the person, which is used as a repository for the storage of software or data illegally obtained in violation of section 63 and section 64 shall be subject to forfeiture.
Computer related crime – specific violation by college or university student
66. A community college, state university, or academic institution accredited by Central Govt. or State Govt. is required to include computer-related crimes as a specific violation of college or university student conduct policies and regulations that may subject a student to disciplinary sanctions up to and including dismissal from the academic institution.

PART XIV
MISCELLANEOUS
Territorial scope of offences
67.-(1) Subject to sections 63, 64, 65 and 66 the provisions of this Act shall have effect, in relation to any person, whatever his nationality or citizenship, outside as well as within India and where an offence under this Act is committed by any person in any place outside India, he may be dealt with as if the offence had been committed within India.
(2) For the purposes of subsection (1), this Act shall apply if, for the offence in question –
(a) the accused was in India at the material time; or

(b) the computer, programme or data was in India at the material time.
(3) For the purpose of bringing a civil or criminal action under section 63, 64 and 65 a person who causes by any means, the access of a computer, computer system or computer network in one jurisdiction from another jurisdiction he or she is deemed to have personally accessed the computer, computer system or computer network in his or her jurisdiction.

Jurisdiction of courts
68. A District Magistrate, Addl. District Magistrate or Executive Magistrate shall have jurisdiction to hear and determine all offences under this Act and shall have power to impose the full penalty or punishment in respect of any offence under this Act alongwith other courts as per Criminal Procedure Code.
Order of payment of compensation
69.-(1) The court before which a person is convicted of any offence under this Act may make an order against him for the payment by him of a sum to be fixed by the court by way of compensation to any person for any damage caused to his computer, programmeme or data by the offence for which the sentence is passed.
(2) Any claim by a person for damages sustained by reason of the offence shall be deemed to have been satisfied to the extent of any amount which has been paid to him under an order for compensation, but the order shall not prejudice any right to a civil remedy for the recovery of damages beyond the amount of compensation paid under the order.
(2) An order of compensation under this section shall be recoverable as a civil debt.
Evidence from computer records
70.-(1) Notwithstanding sections 75 and 76 of the Indian Evidence Act, 1872 in any proceedings under this Act, any relevant computer output shall be admissible as evidence of any fact stated therein if it is shown –
(a) that there is no reasonable ground for believing that the output is inaccurate because of improper use of the computer and that no reason exists to doubt or suspect the truth or reliability of the output; or
(b) that at all material times the computer was operating properly, or if not, that any respect of which it was not operating properly or was out of operation was not such as to affect the production of the output or the accuracy of its contents.
(2) For the purpose of deciding whether or not such output is so admissible, the court may draw any reasonable inference from the circumstances in which the output was made or otherwise came into being.
Supplementary provisions on evidence

71.-(1) In any proceedings where it is desired to admit computer output in evidence in accordance with section 70, a certificate –
(a) identifying the computer output and describing the manner in which it was produced;
(b) giving such particulars of any device involved in the production of that computer output as may be appropriate for the purpose of showing that the output was produced by a computer;
(c) dealing with any of the matters mentioned in section 70(1); and
(d) purporting to be signed by a person occupying a responsible position in relation to the operation of the computer at all relevant times, shall be admitted in those proceedings as evidence of anything stated in the certificate.
(2) If the person referred to in subsection (1) (d) who occupies a responsible position in relation to the operation of the computer did not have control or access over any relevant records and facts in relation to the production by the computer of the computer output, a supplementary certificate signed by another person who had such control or access and made in accordance with subsection (1) (a) to (c) shall be evidence of anything stated in the certificate.
(3) For the purposes of subsections (1) and (2), it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.
(4) Notwithstanding subsection (1) and (2), a court may require oral evidence to be given of anything of which evidence could be given by a certificate under that subsection.
(5) Any person who in a certificate tendered under subsection (1) and (2) in a court makes a statement which he knows to be false or does not believe to be true shall be guilty of an offence and shall be liable on conviction to a fine not exceeding Rs. 2,00,000 or to imprisonment for a term not exceeding 2 years or to both.
(6) In estimating the weight, if any, of any admissible computer output, regard shall be had to all the circumstances from which any inference can reasonably be drawn as to the accuracy or otherwise of the output and, in particular –
(a) to the question whether or not the information which the output reproduces or is derived from was supplied to the relevant computer, or recorded for the purpose of being supplied to it, contemporaneously with the occurrence or existence of the facts dealt with in that information; and
(b) to the question whether or not any person concerned with the supply of information to that computer, or with the operation of that computer, or any equipment by means of which the admissible computer output was produced by it, had any incentive to conceal or misrepresent the facts.
(7) For the purpose of subsection (6), information shall be taken to be supplied to a computer whether it is supplied directly or (with or without human intervention) by means of any appropriate equipment.
Proof of document or copy thereof
72. Notwithstanding the provisions of the Evidence Act, where in any proceedings any computer output is admissible in evidence in accordance with section 70, it may be proved –
(a) by the production of that computer output; or
(b) (whether or not that computer output is still in existence) by the production of a copy of that output, or of the material part of it, authenticated in such manner as the court may approve.
Powers of Police officers to investigate and require assistance
73.-(1) In connection with the exercise of his powers of investigations under the Criminal Procedure Code, a police officer not below the rank of Deputy Superintendent of Police –
(a) shall be entitled to investigate and at any time to have access to, and inspect and check the operation of, any computer and any associated apparatus or material which he has reasonable cause to suspect is or has been in use in connection with any offence under this Act; and
(b) may require-
(i) the person by whom or on whose behalf the police officer has reasonable cause to suspect the computer is or has been so used; or

(ii) any person having charge of, or otherwise concerned with the operation of, the computer, apparatus or material,
to provide him with such reasonable assistance as he may require for the purposes of paragraph (a)
(2) Any police officer not below the rank of Inspector of Police may arrest without warrant any person reasonably suspected of committing an offence under this Act.

PART XV
RELATED AMENDMENTS IN EXISTING ACTS
Related amendments to the Indian Evidence Act, 1872
74. The Indian Evidence Act, 1872 is amended by renumbering section 67 as subsection (1) of that section, and hy inserting immediately thereafter the following subsection :
a) "(2) This section shall not apply to any electronic record or electronic signature to which the Information Technology Act, 1998 applies.".
b) inserting immediately after section 3(e) the following subsection :
3(f) : "Electronic Document/Data/Record/Data Message – information generated, sent, received or stored by electronic, optical, computer or similar means including, but not limited to, Electronic Data Interchange (EDI), electronic mail, telegram, telex or telecopy".
c) inserting immediately after section 63(5) the following subsection :
"Electronic Document/Data/Record/Data Message – information generated, sent, received or stored by electronic, optical, computer or similar means including, but not limited to, Electronic Data Interchange (EDI), electronic mail, telegram, telex or telecopy".
d) Inserting immediately after section 74(1)(iii) the definition of Electronic Document through an explanation clause.
e) Notification by State Govt. concerned declaring an officer as an authorised officer under Section 76 (Explanation) of the Indian Evidence Act, 1872 as custodian of records of right to authenticate the computer printout taken from the computerised land records.
Related amendments to the Indian Penal Code, 1860
75. The Indian Penal Code, 1860 is amended by inserting in section 29 the following subsection :
"Electronic Document/Data/Record/Data Message – information generated, sent, received or stored by electronic, optical, computer or similar means including, but not limited to, Electronic Data Interchange (EDI), electronic mail, telegram, telex or telecopy".
Related amendments to the General Clauses Act, 1897
76. The General Clauses Act, 1897 is amended by inserting immediately after section 3(18) the following subsection :
"Electronic Document/Data/Record/Data Message – information generated, sent, received or stored by electronic, optical, computer or similar means including, but not limited to, Electronic Data Interchange (EDI), electronic mail, telegram, telex or telecopy".
Amendment to RBI Act, 1934
77. In the Reserve Bank of India Act, 1934, after Chapter IIIC, the following Chapter III D shall be inserted, namely:
Chapter III D
U(1) If the Bank is satisfied that in the interest of development of efficient payment systems it is necessary to promote and establish multiple electronic funds transfer systems, it may by order, allow banking companies, financial or other institutions, or any other person desirous of setting up an EFT System to apply for authorisation from the Bank to commence and operate an Electronics Funds Transfer System.
(2) An application for approval under sub-section (1) shall be submitted in the form specified by the Bank from time to time, alongwith a scheme of operations of the proposed system and the documents relating to rights, duties and liabilities of the person participating in such system.
(3) The Bank may, before granting approval for any such proposed system, require the applicant or the proposed participants in the system to submit such further information and particulars as considered necessary and the Bank may also cause such inspection of the premises, equipments, machineries, books or other documents, or accounts and transactions, relating to the proposed system as considered essential by the Bank.
(4) The Bank may, subject to such modifications and alterations to the scheme and any contract and documents submitted therewith as are considered desirable, approve or reject any application submitted for approval under sub-section (2).
Provided that while approving the scheme, the Bank may impose such terms, restrictions, limitations and conditions as it may deem fit, on the applicant or the proposed participant or any other person likely to be affected or benefitted thereby.
Provided further, that before rejecting any such application the Bank may serve notice on the applicant requiring it to showcause as to why the application should not rejected and if so requested by the applicant, an opportunity for hearing should also be given.
(5) Any Regulation framed by the Bank for regulation of multiple payment systems shall be binding on the applicant, the proposed participants and any other person likely to be affected or benefitted thereby.
(6) No person, other than a person whose application is approved by the Bank under sub-section (4) shall commence or operate any Electronic Funds Transfer System.
Explanation;
For the purpose of this Section,
(a) "EFT System" means the Electronic Fund Transfer System established by these Regulations for carrying out interbank and intrabank funds transfers within India, through EFT centres connected by a network, and providing for settlement of payment obligations arising out of such funds transfers, between participating banks or institutions.
(b) "banking company" means a company as defined in Section 5 of the Banking Regulation Act, 1949, and includes the State Bank of India, constituted by the State Bank of India Act, 1955, a Subsidiary Bank constituted under the State Bank of India (Subsidiary Banks) Act, 1959, a Corresponding New Bank constituted under the Banking Companies (Acquisition and Transfer of Undertakings) Act, 1970 or the Banking Companies (Acquisition and Transfer of Undertakings) Act, 1980, a cooperative bank, as defined in Section 56 of Part V of the Banking Regulation Act, 1949 and such other banks as may be specified from time to time.
(c) "Financial Institutions" shall bear the meaning assigned to it in Section 4A(1) of the Companies Act, 1956 and includes an institution notified under Sub-section (2) of that Section.
(d) "Institution" means a public financial institution and includes a department or agency of the Central or State Government or any other organisation approved by the Reserve Bank as eligible to open a settlement account with it.
(7) In Section 58 of the Act, in sub-section (2), the following clause (PP) shall be inserted after existing clause (P), namely:-
'(PP) The regulation of multiple payment systems'
Amendment in Banker's Book Evidence Act of 1891
78. In Section 2 of the Banker's Books Evidence Act, 1891 (hereinafter referred to as "the Act"),

(a) for sub-section (3), the following sub-section shall be substituted, namely:-
"(3)" banker's books" include ledgers, day-books, cash books, account-books and other records used in the ordinary business of the bank, whether these records are in written form or are kept in micro-film, magnetic tape or any other form of mechanical or electronic data retrieval mechanism".
(b) in sub-section (8) after the existing provisions, the following words shall be added, namely:
a print-out of any entry in the books of a bank on micro-film, magnetic tape or any other form of mechanical or electronic data retrieval mechanism obtained by a mechanical or other process which in itself ensures the accuracy of such print out, is a copy of such entry and when such print-out contains the certificate as provided in this sub-section, it is a certified copy of such entry in the books of a bank.
Amendment of Section 4
In Section 4 of the Act, the existing provisions shall be numbered as sub-section (2) and the following shall be inserted as sub-section (1), namely:-
Any entry in any Banker's books shall be deemed to be primary evidence of such entry and any such banker's books a "document" for the purpose of Section 62 of the Indian Evidence Act, 1872 (Act 1 of 1872).
Notification of Electronic Fund Transfer System Regulation
79. Notification of Regulation for Electronic Fund Transfer System under Section 58 of Reserve Bank of India Act, 1934 (2 of 1934).

ANNEXURE-I

REGULATION FOR RESERVE BANK EFT SYSTEM
Reserve Bank of India (Electronic Funds Transfer System) Regulations 1996
1.-(1) In exercise of the powers conferred by Section 58 of the Reserve Bank of India Act, 1934 [2 of 1934], the Central Board of the Reserve Bank of India, with the previous sanction of the Central Government, is pleased to make the following Regulations, namely :-
(2) Short title, commencement and applicability :
(i) These Regulations may be called the RBI (EFT System) Regulations, 1996.
(ii) They shall come into force with immediate effect.
(iii) They shall apply to every credit transfers executed or payments made, through the EFT system established under these Regulations.
(3) Objects of the Regulations :
The objects of these Regulations are :
(i) to establish an Electronic Funds Transfer System to facilitate an efficient, secure, economical, reliable and expeditious system of funds transfer and clearing in the banking sector throughout India and to relieve the stress on the existing paper based funds transfer and clearing system.
(ii) To define and regulate the nature, scope and process of the funds transfer and the legal rights and obligations between the participants in the EFT system.
(iii) To provide for determination and allocation of loss and the procedure for resolution of disputes arising out of Funds Transfer and all other matters connected with or incidental to the EFT System.
(4) Definitions :
In these Regulations, unless the context otherwise requires –
(a) "Acceptance" means execution of a payment order.
(b) "Bank" means a banking company as defined in Section 5 of the Banking Regulation Act, 1949, and includes the State Bank of India, constituted under the State Bank of India (Subsidiary Banks) Act, 1959, a Corresponding New Bank constituted under the Banking Companies [Acquisition and Transfer of Undertakings] Act, 1970 or the Banking Companies [Acquisition and Transfer of Undertakings] Act, 1980, a co-operative bank, as defined in Section 56 of Part V of the Banking Regulation Act, 1949 and such other banks as may be specified from time to time.
(c) "Beneficiary" means the person designated as such, and to whose account payment is directed to be made, in a payment order.
(d) "Beneficiary bank" means the branch of the bank identified in a payment order in which the account of the beneficiary is to be credited.
(e) "EFT" means Electronic Funds Transfer.
(f) "EFT Centre" means any office designated by the Nodal Department in each of the centres to which EFT system is extended, for receiving, processing and sending the EFT data file and the debiting and crediting of accounts of the pareticipating banks and institutions for settlement of payment obligations or one or more of these functions. EFT Centre is referred to as "Sending EFT Centre" when it receives EFT data file from the participating sending banks and institutions. EFT Centre is referred to as "Receiving EFT Centre" when it receives EFT data file from a sending EFT centre.
(g) "EFT Data File" means an electronic data file of a batch of payment orders for funds transfers, processed and consolidated in the manner specified for transmission of consolidated payment orders and communications concerning payment orders between EFT service branch and EFT centre or between EFT Centres.
(h) "EFT Service Branch" means an office or branch of a bank or institution in a centre designated by that bank or institution to be responsible for processing, sending or receiving EFT data file of that bank or institution in that Centre and to do all other functions entrusted to an EFT service branch by or under these Regulations. EFT Service Branch is referred to as Sending EFT Service Branch when it originates an EFT Data File for Funds Transfer. EFT Service Branch is referred to as Receiving EFT Service Branch when it receives EFT Data File from Receiving EFT Centre.
(i) "EFT System" means the Electronic Funds Transfer System established by these Regulations for carrying out interbank and intrabank funds transfers within India, through EFT centres connected by a network, and providing for settlement of payment obligations arising out of such funds transfers, between participating banks or institutions.
(j) "Execution" of a payment order in relation to sending bank means the transmission or sending of the payment order by it to the EFT Service Branch; in relation to a Service Branch it means transmission of the consolidated payment order in the encrypted EFT data file; in relation to the sending EFT Centre it means the transmission of the payment orders to the receiving EFT Centre; in relation to the receiving EFT Centre, it means the transmission of the payment order to the receiving EFT Service Branch and in relation to the beneficiary's bank, it means the crediting the beneficiary's account.
(k) "Funds Transfer" means the series of transactions beginning with the issue of originator's payment order to the sending bank and completed by acceptance of payment order by the beneficiary's bank, for the purpose of making payment to the beneficiary of the order.

(l) "Institution" means a public financial institution and includes a department or agency of the Central or State Government or any other organisation approved by the Reserve Bank as eligible to open a settlement account with it.
(m) "Nodal Department" means the department or the agency of the Reserve Bank to which the responsibility of implementation, administration and supervision of the EFT System is entrusted.
(n) "Notified" means communicated electronically or in writing.
(o) "Originator" means the person who issues a payment order to the sending bank.
(p) "Participating Bank or Institution" means a bank or as the case may be, an institution admissted for participating into the EFT System pursuant to Regulation 7, and whose Letter of Admission has not been cancelled.
(q) "Payment Order" means an unconditional instruction issued by an originator in writing or transmitted electronically to a sending bank to effect a funds transfer for a certain sum of money expressed in Indian rupees, to the designated account of a designated beneficiary by debiting correspondingly an account of the originator.
(r) "Public Financial Institution" shall bear the meaning assigned to it in Section 4A(1) of the Companies Act, 1956 and includes an institution notified under Sub-section (2) of that Section.
(s) "Reserve Bank" means the Reserve Bank of India established under the Reserve Bank of India Act, 1934 (2 of 1934).
(t) "Security Procedure" means a procedure (specified) for the purpose of
(i) verifying that a payment order, a communication cancelling a payment order or an EFT Data File is authorised by the person from whom it purports to be authorised; and
(ii) for detecting error in the transmission or the content of a payment order, a communication or an EFT Data File.
A security procedure may require the use of algorithms or other codes, identifying words or number, encryptions, call back procedures, authentication key or similar security devices specified from time to time.
(u) "Sending bank" means the branch of a bank, maintaining an account of and to which payment order is issued by the originator. When the originator is a participating institution, reference to sending bank shall be construed as referring to the sending EFT Centre.
(v) "Settlement Account" means an account maintained by a participating bank or institution for the purpose of settlement of payment obligations under EFT System.
(w) "Specified" means specified by procedural guideli>

Transfer interrupted!

APPENDIX G

THE ELECTRONIC FUNDS TRANSFER ACT (PROPOSED)

AN OUTLINE

AUTHORITY : The Parliament has got the legislative competence to enact this EFT Act. The subject matter is covered by entries 38, 45, 46 and 48 of List-I of Union List under Schedule VIII of the Constitution of India. The provisions of the proposed Act do not contravene any fundamental rights or any other express provisions of the Constitution of India and they are not inconsistent or repugnant to any other existing law.

PREAMBLE

An Act to provide for the orderly growth of Electronic Payments and Funds Transfer Systems, consistent with the country's monetary and credit systems and to define the rights and obligations arising out of electronic payments and Electronic Funds Transfer Systems.

CHAPTER I

PRELIMINARY

1. SCOPE AND APPLICABILITY

(1) Scope of the Act:

(i) The Act covers credit transfers, debit transfers, funds transfer at the point of sale (EFTPoS), Automated Teller Machines (ATMs), and every other type of payments made electronically through an automated data processing system or electronic communication network system.

(ii) The Act extends to whole of India.

(2) Applicability:

This Act will apply to every Electronic Funds Transfer Systems and every electronic payment, other than the EFT System operated by the Reserve Bank

under the Reserve Bank of India (Electronic Funds Transfer System) Regulations, 1996.

2. DEFINITIONS:

Basic concepts like "funds transfer", "funds transfer system", "credit transfer", "debit transfer", "EFTPoS", "ATMs", "payment order", "service provider", "acceptance of payment order", "execution of payment order", "sender/issuer/ originator", "bank/sending bank/receiving bank/ intermediary bank", "system design", "security procedure", "beneficiary", "credit card", "debit card", etc. should be designed with reference to the EFT Systems that may have already developed and at the same time keeping in view a futuristic vision for upgradation of the payment systems on par with intenational standards. As far as possible, while drafting the definitions, the need for harmonization of our concepts with internationally accepted terminology should be recognised.

[The Banking Committee of the International Organisation for standardisation has developed international standards (ISO, TC 68) for various aspects of automated banking operations and has prepared the international standard (DIS 7982), for data elements and terms used in describing, processing and formating messages relating to credit transfers transmitted over computer to computer telecommunications network[1].]

3. OVERRIDING EFFECT:

(1) The provisions of the Act shall have overriding effect on any agreement, Memorandum or Articles of Association.

(2) The provisions of the Act shall not be in derogation of the provisions of the Reserve Bank of India Act, 1934 and the Banking Regulation Act, 1949. The Act shall have overriding effect on any other Act or laws in force for the time being.

CHAPTER II

Authorisation and Regulation of EFT Systems

4. PRIOR AUTHORISATION NECESSARY:

A prohibition against organising, promoting or operating any EFT System by any

[1] *See, UNCITRAL LEGAL GUIDE ON ELECTRONIC FUNDS TRANSFERS, United Nations, New York (1987).*

ANNEXURE-K

person, except with the prior authorisation in writing by the Reserve Bank, should be enacted.

5. REGULATION OF EFT SYSTEMS

(1) The Reserve Bank may be vested with the power to authorise, with or without conditions, subject to Regulations made by the Reserve Bank to provide for an objective procedure for authorisation, supervision and monitoring of every EFT Systems, having regard to public interest, interest of the consumers, operational security of the system, monetary and credit policies.

(2) The Regulations made by the Reserve Bank pursuant to clause (1) of this Section may provide for the procedure for submission of application, particulars and information required to be furnished by the applicant, examination of application by the Reserve Bank with reference to the operational security, the design, the terms and conditions of operation, the constitution of the promoters etc.

(3) The Reserve Bank may consider the application, having regard to the need for the proposed system, the technical standards of the design of the system, the operational security, the terms and conditions of operation, the constitution of the promoters, the interest of the consumer, public interest and monetary and credit policy considerations. After considering the application the Reserve Bank may authorise in writing the establishment of an EFT System with or without condition or reject the application.

6. SUPERVISION AND CONTROL

(1) Power may be conferred on the Reserve Bank to require prescribed information and furnishing of documents by any EFT System operator. Reserve Bank may prescribe various returns, statements and particulars to be furnished to it by every EFT System operator, from time to time.

7. INSPECTION

(1) Power may be conferred on the Reserve Bank to inspect the premises, the equipments, computer hardware and software, books of accounts of the proposed system and any other relevant document, to satisfy itself before authorising the establishment of any EFT System, that the system if authorised would serve the objectives and would be in compliance with the provisions of the Act.

(2) Power may be conferred on the Reserve Bank to enable it to inspect the

premises, the equipments, the computer hardware, software and any other communication system, books of accounts and any other relevant document of any EFT system. A duty on every person responsible for the EFT System, to furnish to the Reserve Bank or an officer authorised by it, any information or document when required, should be provided.

(3) Provision should be made for empowering the Reserve Bank to cancel the authorisation if a system contravenes the provisions of the Act or the terms and conditions of authorisation.

8. POWER OF THE RESERVE BANK TO GIVE DIRECTIONS

(1) Provision enabling the Reserve Bank to issue directions generally to EFT Systems or to any EFT System in particular, or in respect of any form of electronic payments if the Reserve Bank is satisfied that issuing of such directions is necessary in public interest, in the interest of the banking policy, in the interest of the monetary policy, or in the interest of the operational security of the EFT Systems, etc.

CHAPTER III

Consumer Protection Measures

9. DISCLOSURE OF TERMS AND CONDITIONS

(1) Every EFT System should be required to disclose the terms and conditions of funds transfer or payments in the language and in a manner easilly understandable by the potential users of the system. Such disclosures should cover terms including the limitation of liability, the charges, etc.

10. DOCUMENTATION OF TRANSACTION

(1) The funds transfer system should be required to provide to the users, periodic statements and in the case of a consumer activated system, automatic computer print outs of the transaction. Such print out should clearly set forth the amount involved, the date, the type, the identity of the account, the identity of the party to whom or from whom funds are transferred.

(2) Every financial institution and every other EFT system provider shall be required to provide to the consumer/customer with a periodic statement for each account of such consumer/customer of all EFT transactions carried out during such period.

(k2)

CHAPTER IV

Rights and obligations of service providers

11. MAINTENANCE OF SYSTEM

(1) Provision shall be made for maintaining technical standards of the design and operational security of the system. System providers liability for loss attributable to errors and frauds by deficiency in the system or negligence may be defined.

(2) Provision shall be made to define the responsibilities of the system providers in regard to security procedure and unauthorised payments. Finality of payment with reference to the sender, the receiving bank, the intermediary bank and the beneficiary's bank shall also be defined.

(3) Provision shall be made for limiting the liability of the consumer in case of third party frauds.

CHAPTER V

Investigation and resolution of disputes

12. INVESTIGATION AND RESOLUTION OF CLAIMS

(1) Provision shall be made for establishment of a machinery to investigate any claim arising out of errors, system malfunctioning, negligence or fraud.

(2) Principles for determining the liability in case of errors, negligence, system failure or fraud shall be laid down.

(3) A dispute resolution machinery to resolve the disputes arising in EFT System may be provided.

CHAPTER VI

Evidence and Data Protection

13. ADMISSIBILITY OF EVIDENCE

(1) Rules of evidence in regard to computer print outs and records kept in micro-film disc, floppy or any other electronic data retrieval system may be

provided. The conditions for admissibility of such evidence may be defined. Computer print-outs, subject to specified conditions, shall be accorded the status of prima facie evidence.

(2) Liability of the service provider in regard to confidentiality shall be provided for.

(3) There shall be a provision, defining the circumstances under which the service provider or holder of EFT information shall not be responsible for unauthorised access to personal data.

CHAPTER VII

Offences and penalties

14. OFFENCES

(1) Unauthorised access to computer material shall be made an offence if a person

(a) causes a computer to perform any function with intent to secure access to any programme or data held in any computer;

(b) the access he intend to secure is unauthorised; and

(c) he knows the nature of the function, at the time when he causes the computer to perform the function, and causes such function.

(2) Additional penalty for unauthorised access with intention or knowledge of commiting or facilitating the commission of any further offence, shall be provided for.

(3) Unauthorised modification of computer material shall be made punishable if a person does any act which causes an unauthorised modification of the contents of any computer and at the time when does the act he has the requisite intent or the requisite knowledge.

(4) For the purposes of the above offences intention to impair the operation of any computer, to prevent or hinder access to any programme or data held in any computer, to impair the operation of any such programme or the reliability of any such data shall be sufficient although such intention need not be directed at any particular computer or any particular programme or data of any particular kind.

(k3)

(5) It shall be an offence for any person to commit any of the above offences or to contravene any of the provisions of the Act and such contravention shall be punishable with specified penalties, which may include imprisonment and fine.

(6) Special rules of evidence in prosecution of offences under the Act shall be provided for. Such rules may raise presumption of required intention or knowledge and put the burden of disproving such intention on the part of the accused.

(7) Provision for cognizance of the offence may be made.

CHAPTER VIII

Miscellaneous

15. ESTABLISHMENT OF CONTINGENCY FUND

(1) Every EFT System shall be required to establish a contingency fund by contributing a portion of the fees/charges collected by it.

(2) The administration of the Contingency Fund shall be subjected to the supervisory and regulatory control of the Reserve Bank.

(3) The funds from the Contingency Fund may be utilised to off-set the loss caused on account of insolvency of any participants in the EFT System.

(4) The provision of this Section should have overriding effect on the restriction placed under the General Insurance Act.

16. BAR OF CIVIL SUITS

17. REGULATION MAKING POWER OF THE RESERVE BANK

(K4)

(DRAFT) AMENDMENT TO RBI ACT, 1934

1. In the Reserve Bank of India Act, 1934, after Chapter III C, the following Chapter III D shall be inserted, namely:

Chapter III D

45 U (1) If the Bank is satisfied that in the interest of development of efficient payment systems, it is necessary to promote and establish multiple electronic funds transfer systems, it may, by order, allow banking companies, financial or other institutions, or any other person desirous of setting up an EFT System to apply for authorisation from the Bank to commence and operate an Electronic Funds Transfer System.

(2) An application for approval under sub-section (1) shall be submitted in the form specified by the Bank from time to time, along with a scheme of operations of the proposed system and the documents relating to rights, duties and liabilities of the persons participating in such system.

(3) The Bank may, before granting approval for any such proposed system, require the applicant or the proposed participants in the system to submit such further information and particulars as considered necessary and the Bnk may also cause such inspection of the premises, equipments, machineries, books or other documents, or accounts and transactions, relating to the proposed system as considered essential by the Bank.

(4) The Bank may, subject to such modifications and alterations to the scheme and any contract and documents submitted therewith as are considered desirable, approve or reject any application submitted for approval under sub-section (2).

Provided that while approving the scheme, the Bank may impose such terms, restrictions, limitations and conditions as it may deem fit, on the applicant or the proposed participant or any other person likely to be affected or benefitted thereby.

ANNEXURE-L

(L1)

Provided further, that before rejecting any such application the Bank may serve notice on the applicant requiring it to showcause as to why the application should not be rejected and if so requested by the applicant, an opportunity for hearing should also be given.

(5) Any Regulations framed by the Bank for regulation of multiple payment systems shall be binding on the applicant, the proposed participants and any other person likely to be affected or benefitted thereby.

(6) No person, other than a person whose application is approved by the Bank under sub-section (4) shall commence or operate any Electronic Funds Transfer System.

Explanation ;

For the purpose of this Section,

(a) "EFT System" means .....

(b) "banking company" means .....

(c) "Financial Institution" means .....

(d) "Institution" means .....

In Section 58 of the Act, in sub-section (2), the following clause (PP) shall be inserted after existing clause (P), namely :-

'(PP) The regulation of multiple payment systems.'

(Le)

APPENDIX E

(DRAFT) AMENDMENT TO BANKERS BOOKS EVIDENCE ACT, 1891

Statement of objects and reasons

1. There have been multi-fold increase in the volume of banking transactions in the past few years as a consequence of which, voluminous records are required to be kept in the banks. The requirements of preservation of bankers' records in the traditional ways have created acute shortage of space for banks. Modern technology like micro-filming of records and keeping the record of entries and transactions on magnetic tape and other electronic data retrieval mechanism, offers distinct advantages in reducing the problem of space constraints and labourious paperwork. In most of the advanced and developing countries, the relative provisions in the law of evidence have been amended to enable banks to adopt the system of keeping the records and entries of transactions on micro-film and other devices like electronic data retrieval mechanism. In the context of globalization of the Indian economy, there is a need to provide necessary environment for the Indian Banking System to be more competitive in the matter of utilization of the facilities made available by the modern technologies. To keep pace with the international standards, it is necessary to amend the existing provisions of the Banker's Books Evidence Act so as to recognize records kept by banks on micro-film, disc or other device of electronic data retrieval mechanism as primary evidence of any entry in such records.

2. The bill seeks to achieve the above objective by amending the definition of "Banker's Books" in Section 2 of the Banker's Books Evidence Act 1891 so as to include within the definition, records of banks kept on micro-film, magnetic tape or on any other form of mechanical or electronic data retrieval mechanism and further by amending the definition of "certified copy" provides that a print-out of any entry from the Banker's Book, containing the necessary certificate, be treated as a certified copy. The bill also seeks to specifically recognise as primary evidence, the banker's books whether they are in written form or kept on micro-film, magnetic tape or any other form of mechanical or electronic data retrieval mechanism.

ANNEXURE-M (M)

THE BANKER'S BOOKS EVIDENCE AMENDMENT BILL, 1996 (PROPOSED)

A
BILL

Further to amend the Banker's Books Evidence Act, 1891.

Be it enacted by the Parliament in the Forty-fifth year of the Republic of India as follows :-

1. Short Title

   i) This Act may be called the Banker's Books Evidence (Amendment) Act, 1996.

2. Amendment of Section 2 of the Act 18 of 1891

   In Section 2 of the Banker's Books Evidence Act, 1891 (hereinafter referred to as "the Act"),

   (a) for sub-section (3), the following sub-section shall be substituted, namely :-

   "(3)" banker's books" include ledgers, day-books, cash books, account-books and other records used in the ordinary business of the bank, whether these records are in written form or are kept on micro-film, magnetic tape or any other form of mechanical or electronic data retrieval mechanism".

   (b) in sub-section (8) after the existing provisions, the following words shall be added, namely :

   a print-out of any entry in the books of a bank on micro-film, magnetic tape or any other form of mechanical or electronic data retrieval mechanism obtained by a mechanical or other process which in itself ensures the accuracy of such print out, is a copy of such entry and when such print-out contains the certificate as provided in this sub-section, it is a certified copy of such entry in the books of a bank.

3. Amendment of Section 4

   In Section 4 of the Act, the existing provisions shall be numbered as sub-section (2) and the following shall be inserted as sub-section (1), namely :-

   (1) Any entry in any banker's books shall be deemed to be primary evidence of such entry and any such banker's books a "document" for the purpose of Section 62 of the Indian Evidence Act, 1872 (Act 1 of 1872)".

(M2)

(DRAFT) REGULATION FOR RESERVE BANK EFT SYSTEM

RESERVE BANK OF INDIA
CENTRAL OFFICE
BOMBAY

RESERVE BANK OF INDIA (ELECTRONIC FUNDS TRANSFER SYSTEM) REGULATIONS 1996

In exercise of the powers conferred by Section 58 of the Reserve Bank of India Act, 1934 [2 of 1934], the Central Board of the Reserve Bank of India, with the previous sanction of the Central Government, is pleased to make the following Regulations, namely :-

CHAPTER I

INTRODUCTORY

1. Short title, commencement and applicability

(1) These Regulations may be called the RBI (EFT System) Regulations, 1996.

(2) They shall come into force with immediate effect.

(3) They shall apply to every credit transfers executed or payments made, through the EFT System established under these Regulations.

2. Objects of the Regulations

The objects of these Regulations are :

(1) to establish an Electronic Funds Transfer System to facilitate an efficient, secure, economical, reliable and expeditious system of funds transfer and clearing in the banking sector throughout India and to relieve the stress on the existing paper based funds transfer and clearing system.

ANNEXURE-N (N1)

(2) to define and regulate the nature, scope and process of the funds transfer and the legal rights and obligations between the participants in the EFT System.

(3) to provide for determination and allocation of loss and the procedure for resolution of disputes arising out of Funds Transfer and all other matters connected with or incidental to the EFT System.

3. Definitions

In these Regulations, unless the context otherwise requires-

(a) "Acceptance" means execution of a payment order.

(b) "Bank" means a banking company as defined in Section 5 of the Banking Regulation Act, 1949, and includes the State Bank of India, constituted by the State Bank of India Act, 1955, a Subsidiary Bank constituted under the State Bank of India (Subsidiary Banks) Act, 1959, a Corresponding New Bank constituted under the Banking Companies [Acquisition and Transfer of Undertakings] Act, 1970 or the Banking Companies [Acquisition and Transfer of Undertakings] Act, 1980, a co-operative bank, as defined in Section 56 of Part V of the Banking Regulation Act, 1949 and such other banks as may be specified from time to time.

(c) "Beneficiary" means the person designated as such, and to whose account payment is directed to be made, in a payment order.

(d) "Beneficiary bank" means the branch of the bank identified in a payment order in which the account of the beneficiary is to be credited.

(e) "EFT" means Electronic Funds Transfer.

(f) "EFT Centre" means any office designated by the Nodal Department in each of the centres to which EFT system is extended, for receiving, processing and sending the EFT data file and the debiting and crediting of accounts of the participating banks and institutions for settlement of payment obligations or one or more of these functions. EFT Centre is referred to as "Sending EFT Centre" when it receives EFT data file from the participating sending banks and institutions. EFT Centre is referred to as "Receiving EFT Centre" when it receives EFT data file from a sending EFT centre.

(g) "EFT Data File" means an electronic data file of a batch of payment orders for funds transfers, processed and consolidated in the manner specified for transmission of consolidated payment orders and communications concerning payment orders between EFT service branch and EFT centre or between EFT Centres.

(h) "EFT Service Branch" means an office or branch of a bank or institution in a centre designated by that bank or institution to be responsible for processing, sending or receiving EFT data file of that bank or institution in that Centre and to do all other functions entrusted to an EFT service branch by or under these Regulations. EFT Service Branch is referred to as Sending EFT Service Branch when it originates an EFT Data File for Funds Transfer. EFT Service Branch is referred to as Receiving EFT Service Branch when it receives EFT Data File from Receiving EFT Centre.

(i) "EFT System" means the Electronic Funds Transfer System established by these Regulations for carrying out interbank and intrabank funds transfers within India, through EFT centres connected by a network, and providing for settlement of payment obligations arising out of such funds transfers, between participating banks or institutions.

(j) "Execution" of a payment order in relation to a sending bank means the transmission or sending of the payment order by it to the EFT Service Branch; in relation to a Service Branch it means transmission of the consolidated payment order in the encrypted EFT data file; in relation to the sending EFT Centre it means the transmission of the payment orders to the receiving EFT Centre; in relation to the receiving EFT Centre, it means the transmission of the payment order to the receiving EFT Service Branch and in relation to the beneficiary's bank, it means the crediting the beneficiary's account.

(k) "Funds Transfer" means the series of transactions beginning with the issue of originator's payment order to the sending bank and completed by acceptance of payment order by the beneficiary's bank, for the purpose of making payment to the beneficiary of the order.

(l) "Institution" means a public financial institution and includes a department or agency of the Central or State Government or any other organization approved by the Reserve Bank as eligible to open a settlement account with it.

(m) "Nodal Department" means the department or the agency of the Reserve Bank to which the responsibility of implementation, administration and supervision of the EFT System is entrusted.

(n) "Notified" means communicated electronically or in writing.

(o) "Originator" means the person who issues a payment order to the sending bank.

(p) "Participating Bank or Institution" means a bank or as the case may be, an institution admitted for participating into the EFT System pursuant to Regulation 7, and whose Letter of Admission has not been cancelled.

(q) "Payment Order" means an unconditional instruction issued by an originator in writing or transmitted electronically to a sending bank to effect a funds transfer for a certain sum of money expressed in Indian rupees, to the designated account of a designated beneficiary, by debiting correspondingly an account of the originator.

(r) "Public Financial Institution" shall bear the meaning assigned to it in Section 4A(1) of the Companies Act, 1956 and includes an institution notified under Sub-section (2) of that Section.

(s) "Reserve Bank" means the Reserve Bank of India established under the Reserve Bank of India Act, 1934 (2 of 1934).

(t) "Security Procedure" means a procedure (specified) for the purpose of

(i) verifying that a payment order, a communication cancelling a payment order or an EFT Data File is authorised by the person from whom it purports to be authorised; and

(ii) for detecting error in the transmission or the content of a payment order, a communication or an EFT Data File.

A security procedure may require the use of algorithems or other codes, identifying words or numbers, encryptions, call back procedures, authentication key or similar security devices specified from time to time.

(u) "Sending bank" means the branch of a bank, maintaining an account of and to which payment order is issued by the originator. When the originator is a

participating institution, reference to sending bank shall be construed as referring to the sending EFT centre.

(v) "Settlement Account" means an account maintained by a participating bank or institution for the purpose of settlement of payment obligations under EFT System.

(w) "Specified" means specified by procedural guidelines issued from time to time by the Nodal Department pursuant to these Regulations.

4. Establishment of EFT System

(1) An EFT System shall be established. Depending on the administrative exigencies, EFT system may be extended in a phased manner throughout the country and different categories of banks and institutions may be admitted in stages depending upon the infrastructure and technology available for the efficient functioning of the EFT System.

(2) The administration and supervision of the EFT System including establishment of EFT Centres and procuring of technological support and implements may be entrusted to the Nodal Department.

(3) The operational details and procedure to be followed by participating banks and institutions shall be specified from time to time by the Nodal Department.

(4) Personnel for the Nodal Department and EFT Centres wherever required, may be drawn by selection from among the officers and other employees of the Reserve Bank or on deputation from banks and institutions or other outside agencies or by direct recruitment or on contract or tenure basis.

CHAPTER II

Admission of banks and Institutions

5. Admission necessary for participation

No person shall be entitled to effect a funds transfer in the EFT system, unless the sending bank or institution and the beneficiary bank or institution as the case may be, is admitted for participation in the EFT System.

(N3)

6. Eligibility for admission

To be eligible to apply for admission, an applicant must

(1) be a bank or institution,

(2) have attained and continues to comply with capital adequacy norms, if any, applicable to it,

(3) is willing and able to comply with the technical operational requirements of EFT System,

(4) be approved by the Reserve Bank as eligible to maintain a settlement account with it.

Provided that, having regard to the pattern of ownership and such other relevant factors, all or any of the above conditions may be relaxed or dispensed with, if so decided by the Governor.

7. Procedure for Admission

(1) Any bank or institution eligible to be admitted in the EFT System may submit to the Nodal Department, duly authenticated application in triplicate, containing full particulars in the form specified. Every application shall be accompanied by an undertaking in the specified form to abide by the Regulations in the event of admission.

(2) The Nodal Department shall issue a Letter of Admission in the specified form to every bank or institution admitted into the EFT System.

(3) A directory of participating banks and institutions shall be prepared as on 31st December of each year and supplied to every bank and institution. Additions and deletions in the directory may be notified from time to time.

8. Suspension

(1) If a participating bank or institution has defaulted in meeting its settlement obligations or paying any charges or fees or complying with any Regulations or procedural guidelines issued thereunder or for any reasons specified in

sub-regulation (1) of Regulation 10, the Letter of Admission issued to it i liable to be kept under suspension for such period as may be specified in th order of suspension.

(2) Every order of suspension shall be notified immediately to all the participatin banks and institutions including a bank or institution against which the orde of suspension is passed.

(3) An order of suspension may be reviewed and may be revoked at any time b the Governor upon representation received from the concerned bank o institution or on his own. Every revocation shall be notified immediately to al participating banks and institutions.

(4) A participating bank or an institution shall not, while any order of suspensio is in force against it, be entitled to send or receive any EFT data file o otherwise to effect any funds transfer in the EFT System.

Provided that a suspension shall not affect the obligations of the suspende bank or institution, whether incurred before or after the suspension.

9. Withdrawal

(1) Any participating bank or institution may, by giving a notice of one month withdraw from the EFT System.

(2) No notice under this Regulation shall be effective unless it is given in writin and before the expiry of one month from the date of receipt of notice by th Nodal Department.

(3) Notwithstanding its withdrawal, a bank or institution shall discharge all i payment obligations arising out of fund transfers attributable to it, wheth effected before or after the withdrawal became effective.

(4) The withdrawal of any participating bank or institution shall be notified to the participating banks and institutions.

10. Cancellation of Letter of Admission

(1) A Letter of Admission issued to any bank or institution may be cancelled the Governor on his being satisfied that such bank or institution has

N4

(i) defaulted in complying with any Regulations or procedural guidelines issued thereunder from time to time.

(ii) been placed under an order of moratorium or an order prohibiting acceptance of fresh deposits or an order of winding up or in respect of which a provisional liquidator has been appointed.

(iii) stopped or suspended payment of its debts.

(iv) failed to get the order of suspension passed against it under Regulation 8 revoked within a period of three months from the date of order of suspension.

(v) has conducted its transactions in the EFT System in a manner prejudicial to the interest, integrity or efficiency of the System.

(2) No order of cancellation shall be passed without first giving an opportunity of hearing to the concerned bank or the institution.

(3) Every order of cancellation shall be notified to the concerned bank or the institution.

(3) Every order of cancellation shall be notified to the concerned bank or institution and also to all other participating banks and institutions in the EFT System.

(4) Notwithstanding the order of cancellation of Letter of Admission passed against it, such bank or institution shall discharge all its payment obligations arising out of the funds transfers effected in the EFT System.

CHAPTER III

Funds Transfer in the EFT System

Batch Processing

(1) Any payment order below a sum specified shall be eligible for funds transfer under the EFT System only through the batch processing. If in a single

payment instruction the originator directs payments to several beneficiaries, each payment direction shall be treated as a seperate payment order.

(2) The parties to a funds transfer in the batch processing are the sending bank, the sending service branch, the sending EFT Centre, the receiving EFT Centre, the receiving Service Branch and the beneficiary's bank.

(3) The Nodal Department shall specify

[i] the days in a week on which the EFT System shall be in operation for funds transfer through batch processing ("EFT business days")

[ii] the cut-off time in an EFT business day for receipt of payment order by the EFT Service Branches from sending banks.

[iii] the cut-off time in an EFT business day for receipt of the EFT data file by the sending EFT Centres from EFT Service Branches.

[iv] the security procedure for verification of authenticity of payment orders or as the case may be, the EFT data file.

[v] the procedure for processing, sending and receiving the EFT data file.

[vi] the procedure for settlement of payment obligations of participating banks or institutions.

[vii] the charges or fees payable in respet of each Funds Transfer effected through the EFT System.

[viii] any other matter necessary to ensure the efficiency, safety,cost-effectiveness, reliability and integrity of the EFT System.

(4) Every admitted bank and institution, before accepting any payment order for execution through the EFT System, shall obtain from the originator written undertaking to be bound by these Regulations and a contract in the form approved by the Nodal Department.

(5) For the purpose of determination of rights and liabilities arising out of a funds transfer in the batch process, each branch or office of a bank or as the case may be, an institution and each EFT Centre shall be treated as a seperate unit

N5

(6) Funds transfer in execution of a payment order under the EFT System shall be completed before the close of business on the third EFT business day or such other earlier day, as may be specified, following the EFT business day on which the payment order was received by the sending bank. The originator shall be entitled to claim interest at the Bank Rate from the sending bank for the period of delay in the completion of funds transfer.

(7) A payment order issued for execution in the batch processing of the EFT System shall become irrevocable when it is executed by the sending bank. Any revocation, after the payment order is executed by the sending bank shall not be binding on any other party in the EFT System.

(8) Every participating bank and admitted institution shall open and maintain in every EFT Centre a settlement account for settlement of payment obligations arising under the funds transfers executed in the EFT System.

(9) The payment obligation between participating banks and institutions shall be settled on a netting basis at the end of each EFT business day by debiting or crediting the settlement accounts maintained with the EFT Centres.

12. High Value Funds Transfer Processing

(1) The Nodal Department may procure the required technology for carrying out funds transfer in the EFT System, on real time basis and notify the participating banks and institutions of the availability of High Value Funds Transfer facility in the EFT System.

(2) Every payment order above a sum specified shall be eligible for funds transfer under the EFT System only on real time basis.

(3) Every participating bank institution shall, before execution of a payment order in the High Value funds transfer processing, ensure availability of adequate funds in its settlement account with the sending EFT Centre.

(4) The Nodal Department may specify, the charges payable by a participating bank or participating institution for execution of any payment order in the High Value funds transfer processing and the procedure in regard to issue, acceptance, execution and settlement of payment orders, and such other matters as are necessary for ensuring the integrity, efficiency or reliability of the High Value funds transfer processing of the EFT System.

CHAPTER IV

Rights and obligations

13. **General rights and obligations of participating banks and institutions**

(1) Every participating bank or institution admitted in the EFT System shall, subject to compliance with the specified procedural guidelines, be entitled to execute any payment order for Funds Transfer to a beneficiary of the payment order, issued or accepted by it.

(2) Every participating bank or institution shall maintain the security, integrity and efficiency of the System.

14. **Obligations of sending bank**

(1) The sending bank shall not execute a payment order without complying with the security procedure. No payment order shall be accepted for execution in the EFT System if the beneficiary's bank is not a participating bank or institution.

(2) The sending bank shall be responsible for the accuracy of the name of the beneficiary, the nature and style of the account and account number of the beneficiary, the name of the beneficiary's bank and the authenticity of every payment order executed by it.

(3) The sending bank shall bear the liability for loss if any caused to any participant in the EFT System on account of the acceptance by it of any revocation of a payment order after it has executed it.

(4) The sending bank shall not be entitled to bind any other participants in the EFT System with any "special circumstances" attached to a payment order accepted by it.

(5) The sending bank shall maintain duly authenticated record of all payment orders executed by it for a period for which bank records are required to be preserved under the applicable rules.

(6) The sending bank shall, upon completion of funds transfer of a payment

(N6)

order, furnish to the originator on request by him, a duly authenticated record of the transaction.

15. Obligations of the sending EFT Service Branch

(1) The sending EFT Service Branch shall be responsible for the accuracy of the contents of EFT data file and the authenticity of the payment orders contained therein as received by the EFT Centre in compliance with the security procedure.

(2) The sending EFT Service Branch shall be responsible for settlement of all payment obligations in regard to payment orders executed by it.

(3) The sending EFT Service Branch shall be responsible for ensuring execution of the EFT data file complying with security procedure and time schedule.

(4) The sending EFT Service Branch shall ensure, before execution of any EFT Data File that the balance in its settlement account are adequate to cover its settlement obligation and ensure that the ceiling, if any, specified for it is not exceeded and the requirement of collateral if specified by the Nodal Department is adequate for execution of the EFT data file executed by it.

(5) The sending EFT Service Branch shall generate, dispatch and maintain records of transaction in accordance with procedure specified.

16. Obligations of the sending EFT Centre

(1) The sending EFT Centre shall be responsible for receiving the EFT data files from the EFT Service Branches in compliance with the security procedure.

(2) The sending EFT Centre shall be responsible for processing and sorting the payment orders and preparing the EFT data file centre-wise in accordance with the procedure specified.

(3) The sending EFT Centre shall execute the payment orders received before the cut-off time in an EFT working day. EFT data files if any, received after the cut-off time, or payment orders for which the Sending Service Branch has not made adequate provision for settlement may be treated as received on the opening of the next EFT working day and dealt with accordingly.

(4) Sending EFT Centre shall generate and dispatch and maintain in accordance with the procedure specified, records and reports of the transactions processed and executed by it.

17. Obligations of receiving EFT Centre

(1) Receiving EFT Centre shall be responsible for receiving and processing the EFT data files complying with the security procedure and time schedule specified for the purpose.

(2) Receiving EFT Centre shall in compliance with time schedule and security procedure, process and sort out the EFT data files bank-wise and after crediting the settlement accounts with the corresponding value, transmit the EFT data file to respective receiving EFT Service Branches.

(3) Receiving EFT Centre shall generate, despatch and maintain, in accordance with the procedure specified.

18. Obligations of the Receiving EFT Service Branch

(1) Receiving EFT Service Branch shall be responsible for receiving the EFT data file from the receiving EFT Centre in compliance with the security procedure.

(2) Receiving EFT Service Branch shall process the EFT data file in compliance with the security procedure and sort-out the payment orders branch wise, and transmit to the respective branches the payment orders for execution in accordance with the time schedule and in compliance with the security procedure.

(3) Receiving EFT Service Branch shall generate, despatch and maintain records of transaction in accordance with the procedure specified.

19. Rights and obligations of beneficiary bank

(1) The beneficiary bank shall execute the payment order on the EFT working day on which the payment order is received by it unless it notices one or more of the following deficiencies :-

(a) The beneficiary specified in the payment order has no account or the account of the beneficiary maintained by the beneficiary's bank does not tally with the account specified in the payment order.

(b) The beneficiary's bank is prevented by instructions of the beneficiary not to give or receive any credit to the account.

(c) The account designated in the payment order is closed.

(2) The beneficiary's bank may reject a payment order on one or more of the grounds mentioned in Clause (1) above. The beneficiary's bank shall notify, in the manner specified, the sending bank of the rejection of the payment order alongwith the reasons thereof.

CHAPTER V

Claims and Allocation of Loss

20. **Limitation of liability for loss**

Parties in the EFT System shall be liable for any loss arising on account of any reason other than for system failure, power failure or any other reason beyond the control of the participant.

21. **Originator not entitled to claim against any party other than the sending bank**

These Regulations shall not be construed as entitling the originator of the payment order executed in the EFT System, to make a claim against any party other than the sending bank in the EFT System.

22. **Determination of liability**

(1) Liabilities of parties in the EFT System to pay interest for the delayed period or for loss arising on account of any error shall be determined on the basis of fault.

(2) Every EFT Centre, participating bank and participating institution shall be responsible for the delay in the completion of the Funds Transfer or loss on acount of error, attributable to it. If the delay or loss is attributable to the non-compliance with the Regulations or procedural guidelines specified from time to time, a party responsible for such non-compliance shall be liable for the delay or loss.

(3) If there is more than one party at fault or responsible for non-compliance, in the absence of agreement between the parties, the liability shall be decided upon a reference to the EFT Ombudsman by one or more of the parties to the dispute. The decision of the EFT Ombudsman shall be binding on all the participants in the EFT System.

CHAPTER VI

Dispute Resolution

23. For the purpose of resolving by arbitration any dispute between parties in the EFT System or between an originator and a party in the EFT System, the Governor may provide for a dispute resolution machinery, as considered necessary.

CHAPTER VII

Miscellaneous

24. **Modification of procedural guideline**

The procedural guidelines may be modified from time to time by the Nodal Department.

Provided that no modification shall be effective before the expiry of fifteen days from the date of circulation of the modified guidelines.

N8