

**REPORT OF THE  
COMMITTEE FOR PROPOSING LEGISLATION  
ON  
ELECTRONIC FUNDS TRANSFER AND  
OTHER ELECTRONIC PAYMENTS**



**JANUARY 1996**

**REPORT OF THE  
COMMITTEE FOR PROPOSING LEGISLATION  
ON  
ELECTRONIC FUNDS TRANSFER AND  
OTHER ELECTRONIC PAYMENTS**



**JANUARY 1996**

**RESERVE BANK OF INDIA  
BOMBAY**

प्रधान विधी परामर्शदाता  
PRINCIPAL LEGAL ADVISER



भारतीय रिज़र्व बैंक  
केन्द्रीय कार्यालय  
बम्बई  
RESERVE BANK OF INDIA  
CENTRAL OFFICE  
BOMBAY

January 18, 1996

The Governor  
Reserve Bank of India  
Bombay

Dear Sir,

Committee for proposing Legislation on  
Electronic Funds Transfer and Other Payments

I have the pleasure in submitting the Report of the above Committee appointed vide Memorandum dated August 1, 1995. I am happy to record that despite time constraint and the subject matter being in the developmental stage in India, the Committee has been able to formulate and recommend measures on each of the terms of reference. The members of the Committee have shared their rich experience and expertise during the deliberations of the Committee.

Yours faithfully,

(Smt. K.S. Shere)  
Pr. Legal Adviser  
Chairperson

# CONTENTS

Contents	Page
Acknowledgements	i
CHAPTER I	INTRODUCTORY
	• Background for the committee 1
	• Scope of the Terms of Reference 4
	• Approach and Methodology 5
	• Sub-Committees 6
	• Scheme of the Report 6
CHAPTER II	NATURE OF EFT AND THE LEGAL FRAMEWORK : A COMPARATIVE STUDY
	• Nature of Electronic Payment 8
	• Types of EFT Systems 11
	• Basic Characteristics of Electronic Payments 14
	• Common Issues in EFT 15
	• Legal framework in Other Countries 16
CHAPTER III	TECHNOLOGY IN INDIA - INDIAN AND OTHER LAWS
	PART I
	• Present Status of Technology in India 24
	PART II
	• Monetary and Credit Policy Considerations 29
	• Consumer Protection 31
	• The Competition Issues 33
	• Commercial Banks' Power to Transact EFT Business 34
	• Banker-Customer Relation in EFT 35
	• Finality of Payment 37
	• Irrevocability - Finality of Payment Order 40
	• Authentication of Paperless Payment Order 41
	• Security of Security Procedure 42
	• Errors and System Mal-functioning 43
	• Incidence of Insolvency 45

	<b>PART III</b>	
	• Cheque Truncation	47
	• Evidence and Burden of Proof	50
	• Preservation of Records	52
	• Confidentiality and Data Protection	53
	• Prevention of Frauds	58
	• Settlement of Inter-Bank Payment	62
	<b>PART IV</b>	
	• Summary of Findings	64
	• The Choice of Legal Framework	67
<b>CHAPTER IV</b>	<b>EFT SYSTEM PROPOSED BY THE RESERVE BANK</b>	
	• The Process Flow - Low Value Funds Transfer	70
	• High Value Funds Transfers	71
	• EFT - The Future Direction	72
	• Scope of Proposed EFT System	74
	• Legal Framework	76
	• Regulatory Issues	77
<b>CHAPTER V</b>	<b>RECOMMENDATIONS</b>	79
<b>APPENDICES</b>	<b>APPENDIX A</b>	
	• Glossary of Terms	91
	<b>APPENDIX B</b>	
	• (Draft) RBI (EFT) Regulations, 1996	99
	<b>APPENDIX C</b>	
	• (Draft) Model Customer Agreement	114
	<b>APPENDIX D</b>	
	• (Draft) Amendment to RBI Act	119
	<b>APPENDIX E</b>	
	• (Draft) Amendment to Bankers Books Evidence Act	121
	<b>APPENDIX F</b>	
	• Extract of the Customs and Central Excise Laws (Amendment) Act, 1988	123

## **APPENDIX G**

- Outline of the Proposed EFT Act 126

## **ANNEXURES**

### **ANNEXURE 1**

- Governor's Memorandum dated August 1, 1995 -  
Constitution and Terms of Reference of the  
Committee 133

### **ANNEXURE 2**

- Composition of Sub-Committees 136

### **ANNEXURE 3**

- Extract From the Code of Good Practice issues by the  
Office of Fair Trading (U.K.) 138

### **ANNEXURE 4**

- Extract from the Code of Good Banking Practice  
(1991) (U.K.) 147

### **ANNEXURE 5**

- Extract from the European Commission  
Recommendation on Payment Cards. 153

### **ANNEXURE 6**

- Extract of the Policies and Views of the U.K.  
Data Protection Registrar. 158

### **ANNEXURE 7**

- Extract From the U.K. Computer Misuse Act, 1990. 161

# ACKNOWLEDGEMENTS

Electronic Payments in India is in its infancy. There are not many published materials or research works in India on legal issues arising out of electronic payments and EFT Systems. The Committee had to undertake basic research on the legal framework of EFT systems prevalent in other countries and interactions with experts. The Committee has received help and support from innumerable persons. The purpose of this acknowledgement is to express and record, in particular, its **appreciation and thanks**.

1. **To Mr. Robert Keppler** from the Financial Sector Development Department of the World Bank, Washington D. C. for his useful interaction on the experience of the World Bank in developing Electronic Funds Transfer Systems for some of the developing countries and sharing with the Committee his views on various legal issues and also for providing supportive materials.
2. **To Dr. N. L. Mitra**, Prof. of Law, National Law School of India University, Bangalore who made a presentation on September 19, 1995, of the research work done by his team on Electronic Credit Transfers.
3. **To Mr. E. Patrikis**, Executive Vice President and General Counsel, Federal Reserve Bank of New York, **Mr. Joseph Sommer**, Attorney, Federal Reserve Bank of New York, **Mr. S. Sankar**, Senior Vice President, Asian Finance and Investment Corporation Ltd., Singapore for providing valuable materials on EFT Systems.
4. **To the Citibank, the Standard Chartered Bank, and the State Bank of India** for arranging presentations of working of electronic banking and hosting the Committee meetings.
5. **To the Department of Information Technology, Reserve Bank**, especially **Mr. A. P. Hota**, Asst. Adviser, for helping the Committee on technological issues and processes and providing useful discussion papers and other materials.
6. Lastly, to the Secretariat of the Committee in the Legal Department, Reserve Bank, especially **Mr. S. S. Hegde**, Deputy Legal Adviser, who, apart from organising meetings and agenda for the Committee, did a splendid research work, identified and presented various issues for consideration of the Committee, put in hard work in preparing the draft Regulations and major part of the draft Report; **Mr. A. Unnikrishnan**, Legal Officer, who provided secretarial support and **Smt. S. Jayaprakash** and **Mr. C.B. Paunekar**, who transcribed the records of the proceedings and this Report and have put in dedicated service to meet many-a-deadlines for the successful completion of the preparation of the Report.

## CHAPTER I

# INTRODUCTORY

### Background for this Committee

- 1.1. Cash and negotiable instruments are treated as the first and the second great revolutions respectively, in the history of payment systems. **Electronic Payments** undoubtedly, has to be recognised as the third.

The advent of electronics in banking, has brought about a sea change in the nature of banker-customer relation and perception of customer service in the banking business. The Indian banking sector is on the threshold of a computer revolution. Payment system is one area where electronic technology can bring about several salutary innovations. Realising the need for giving greater impetus and priority to adoption of technological innovations in payment system, the Governor of Reserve Bank had constituted a Committee on technology issues, headed by Shri W. S. Saraf, Executive Director, Reserve Bank, in June 1994 (**Saraf Committee**), to look into, among other things, technological issues relating to payment system and to make recommendations for widening the use of modern technology in the banking industry. The Saraf Committee recommended<sup>1</sup> institution of Electronic Funds Transfer (EFT) System in India. It was in this background that this Committee was constituted<sup>2</sup> by the Governor, Reserve Bank of India on August 1, 1995.

### The Terms of Reference

- 1.2. The terms of reference of the Committee are as under :

1. Defining the scope of "Electronic Funds Transfer" and determining the

---

<sup>1</sup> Report of the Committee on Technology Issues, Reserve Bank of India Bombay [December 1994], para 2.9.

<sup>2</sup> See, Memorandum dated August 1, 1995 of the Governor, Reserve Bank of India at Annexure 1. Originally ten members were appointed by the Governor. Shri A. S. Khan, Addl. Legal Adviser, Ministry of Law, Government of India, was co-opted as a member in September 1995



responsibilities and liabilities of the participants arising out of contractual obligations.

2. Defining the trigger events that determine the finality and irrevocability of the transfer of funds at different stages like sender finality, settlement finality, receiver finality etc., including the scope for countermanding and money-back guarantees.
3. Operational security; determination of liability in the event of operational failure at any stage.
4. Defining measures to ensure security, integrity and efficiency of communication network linkages (eg. checksum, encryption, firewall etc.)
5. Definition of "fraud" in electronic environment.
6. The extent to which paper documents are mandatory vis-a-vis the contractual obligations.
7. Consequences of bank failures and other systemic events - procedures to follow.
8. Admissibility of electronic media for the purpose of evidence, preservation period of electronic media etc.
9. Cheque truncation.
10. Any other matter relating to Electronic Funds Transfer such as securities transfer and other cash/ credit/debit transactions through Electronic Funds Transfer at Point of Sale (EFTPOS) devices and computer/ communication networks;
11. A comprehensive fresh legislation to deal not only with EFT, but also for bringing changes required in the existing Acts such as Negotiable Instruments Act, Bankers' Books Evidence Act, Securities and Contract Regulation Act (SCRA) etc.

## **Fundamental question**

- 1.3. The theme of the terms referred to this Committee centres round Electronic

**Payments.** Looked in retrospect, each revolution in the history of payment systems, had brought with it new concepts and issues. In the case of cash, new rules and concepts were to be first put in place to introduce the system. Law was an instrumentality of change in this case. But in the case of negotiable instruments, the legal principles followed the Law Merchant and the market practice. Introduction of legal principles was more by way of a response to emerging usage and practice. In jurisprudence, as we see in greater details later, each of the above sequence has great significance. These historical facts raise a fundamental question :

**Whether 'Legislation' is the only answer or only solution for introduction of EFT System?**

- 1.4. The Saraf Committee which went into the technological issues made among others, the following recommendations :

2.20 In view of the fact the EFT has so far not been introduced in India, there is no Act or Legislation specifically addressed to the issue of Electronic Fund Transfer. Since the banks at the destination centres would be required to credit the accounts of their customers entirely on the basis of electronic messages received from the clearing house, **the responsibility and the accountability of the concerned parties at each stage, have to be prescribed and agreed upon by the participating institutions with adequate legal backing.** A beginning can be made by getting the procedural guidelines of EFT adopted by the clearing houses of the centres covered under the Scheme. It is, however, imperative to enact a suitable legislation at the earliest, along the lines of Electronic Fund Transfer Act of 1978 in USA and Data Protection Act of 1984 in UK.

(Emphasis supplied)

- 1.5. An examination of the legal framework in operation in other countries<sup>1</sup> shows that there is a choice between three models : (i) statutory model, (ii) contractual model, (iii) regulatory model. Choice between any of these, or alternatively a combination of these depends upon several factors.
- 1.6. The Saraf Committee recommendation for 'legislation' was in the context of

---

<sup>1</sup> See, post para 2.24 to 2.42

proposal for introduction of a specific EFT System outlined in that report. That Committee had obviously not gone into the complex question of desirability at this stage, of any particular form of law - whether it should be statutory or whether it could be subordinate regulation or whether mere contractual rules could suffice. The term 'Legislation' as used by the Saraf Committee and in the Terms of Reference of this Committee has to be necessarily construed in its widest possible form -viz. rules, having a binding force. Rules can be established either by contract, or by subordinate legislation or by statute. This Committee accordingly proceeded on the basis that the **terms of reference made to it include the incidental question of examining and recommending which form of legal rules would be more suited to Indian conditions.**

## **Scope of the reference**

1.7. There are basically two distinct aspects in any payment system -

- **substantive issues of Regulatory nature**
- **formal issues of transactional nature.**

A payment system, by its very nature, has a direct implication on the **monetary and credit system**. There are also public interest issues like **consumer protection** and issues of **competition** among a regime of multiple systems. These are basically matters of regulatory policy formulations. Transactional aspects refer to the rules to establish the **predictability and certainty** to a given transaction. Structuring a legal frame-work for any economic activity must necessarily advert to both Regulatory as well as Transactional issues. These are complementary to each other and inseparable if the system has to function as a concomitant to overall economic and developmental objectives of the society.

1.8. Brief study of the EFT Systems in advanced countries shows that the need for Central Bank's empowerment for overall control and supervision of electronic payment systems was increasingly felt in the G-10 countries<sup>1</sup>. This arises mainly due to<sup>2</sup>:

---

<sup>1</sup> Bruce J. Summers, *Clearing and Payment Systems: The role of the Central Bank*, 82 Federal Reserve Bulletin, February 1991.

<sup>2</sup> For discussion of monetary and regulatory issues in EFT, see generally, UNCITRAL Legal Guide on EFT, United Nations, New York, (1987). Also see, Clifford Chance, People's Bank of China, Payment Systems Project, a World Bank assistance paper

- Possible risk transfer to central banks through float or daylight overdrafts (as in most cases the central bank manages clearing and settlement), since EFTs are generally believed to increase the level of float.
- Risk of systemic failure. Increased efficiency in terms of speed would increase the systemic risk, especially when the system is linked to securities transactions. Issues of accountability, soundness and safety of the banking system are central in any EFT system.
- Electronic Payments are prone to uncontrolled increase in money and credit supply. If central bank is not used for settlement, the system may also lead to inefficient use of bank balances.
- Electronic Payments have greater potential for abuse of banking system for money laundering, tax evasion and other unlawful funds transfers.

1.9. Law making is a long process in which policy formulation normally precedes to fill the contents of a legislation. Although literally interpreted, the terms of reference would suggest a reference for a **comprehensive legislation**, a closer look at these makes it clear that the objective is to define the transactional rules to govern the legal relationship, rights and obligations of the parties in EFT Systems. Unlike substantive issues of regulatory nature, transactional issues do not involve much of policy consideration.

1.10. An examination of the nature of the issues would clearly show that transactional issues need to be addressed immediately, as without this, it may be extremely difficult to implement/adopt any EFT System. On the other hand, the substantive issues need a very detailed probe not only from legal angle but also from the regulatory and monetary policy angles.

## **Our Approach and Methodology**

1.11. Having regard to the constraints of time, the need for deeper probing of substantive issues, and the growing and fast changing nature of technology in the country, it appeared to the Committee that for examining the issues arising under the terms of reference it needs to adopt a two fold approach, i.e., a long term and a short term. The Committee, therefore, decided to recommend

only the broad outlines of the legal mechanism, without specifying the drafting details of the legislation, which could be pursued as a long term measure. This would also facilitate future probing, if found appropriate, of substantive policy issues, by formulating the policy, to fill the legislation. On the other hand, the Committee went in greater details about the transactional issues that need to be addressed in the context of proposal for immediate implementation of a Funds Transfer System by the Reserve Bank. **The objective which the Committee set for itself in this task has been to strike a balance, within the confines of its terms of reference, between the competing demands of new rules to introduce a new system and the need to preserve flexibility so as not to discourage competition and innovation by excessive regulatory framework.**

## **Sub-Committees**

- 1.12. The Committee noticed that very little research work has been made so far in India in regard to regulatory and legal issues in electronic payments. The task of collection of information about systems in other countries for understanding the basic legal issues and the task of identifying the existing Indian laws that needed change for implementing electronic payment system were addressed through **two Sub-Committees<sup>1</sup>** within the Committee for more focussed analysis.

## **Meetings of the Committee**

- 1.13. The Committee held, in all, eight meetings and interacted with several experts. It would have been advantageous for the Committee members to visit some countries to make an on the spot study and understand the comparative legal structure adopted by them for their EFT Systems. Personal interaction with authorities or persons responsible for administration and regulation of such systems as well as experts in the field would have been also possible by such visits. The report of the Committee is thus based only on its deliberations on the basic research made by the Secretariat and the Sub-Committees.

## **Scheme of the Report**

- 1.14. This Report is presented in five Chapters including this Chapter. In the

---

<sup>1</sup> *The composition of the Sub-Committees is in Annexure 2.*

Second Chapter, the nature of Electronic Payments in general and Electronic Fund Transfers in particular as prevalent in other countries and the legal framework governing their operations are analysed for comparative study. Chapter III is in four parts. The first part analyses the status of technological development in the banking sector in India; the second part reviews the existing legal provisions having a bearing on the new crop of legal problems associated with EFT; the third part deals with other legal issues; and the fourth part summarises the Committee's findings and examines the need for legislation. Chapter IV gives a broad outline of the legal aspects of EFT System proposed by the Reserve Bank. The recommendations of the Committee are presented in Chapter V. The Appendices contains the draft Regulations, a Model Customer Agreement for the proposed EFT System, and drafts for various amendments required in existing laws for a smooth launch of EFT Systems, including an outline of the model legislation on EFT Systems. A glossary of terms in EFT Systems in other countries and extracts from select bibliographies are added to the Report as Annexures.

## CHAPTER II

# **NATURE OF EFT AND THE LEGAL FRAMEWORK: A COMPARATIVE STUDY**

## **NATURE OF ELECTRONIC PAYMENT**

- 2.1. Electronic Fund Transfer is a means. The end is payment. Payment as a legal concept signifies the satisfaction of a claim or discharge of an obligation or liability<sup>1</sup>. There is a wide variety of methods of payments. But the only form of payment, in which a recipient is obliged to accept it, is an amount in legal tender in coins and notes<sup>2</sup>. In other cases, payment is a matter of agreement between the parties.
- 2.2. Except in the case of payment by cash and payment by delivery of securities or goods, a bank is always involved and obligations are settled through banks. Law must however provide the default rule. For example, when a payment is made by delivery of a cheque, the law provides that payment is deemed to be made only if the cheque is honoured by the paying bank<sup>3</sup>. In the case of post dated cheques which may have been delivered before the due date and eventually honoured, payment is deemed to be made at the earliest point of time when it could have been encashed<sup>4</sup>. Whatever may be the method, law will have to provide the default rule about the finality of payment. It is in this context that one has to first understand the nature of EFT. So to begin at the

---

<sup>1</sup> *Parameshwar V. Atti AIR 1958 Punj. 7; Payment of money before the due date is in law payment at the day; for it cannot, in presumption of law, be any prejudice to him to whom the payment is made to have his money before the appointed time Cumber V. Wane (1719) Smith's LC, quoted in WHARTONS LAW LEXICON 14th Edn., Stevens (London) 1957. See also Akshoy Kumari Debi V. Nalini Ranjan AIR 1950 Cal.493; Annappurnamma V. Venkamma AIR 1938 Mad 323.*

<sup>2</sup> *For legal tender character of currency notes and coins see Reserve Bank of India Act, 1934, Sections 22 & 26 and the Indian Coinage Act 1906, Sections 11 to 15A.*

<sup>3</sup> *A.R. Krishnaswami Iyer V. M.N. Ramakrishna (1945) 15 Comp. Cas. 134; Jiwanlal Acharya V. Rameshwarlal AIR 1967 SC 118; Sumitra Baluja V. Bharat Cemicals (1983) 53 Comp. Cas. 561.*

<sup>4</sup> *Anil Kumar Sawhney V. Gulshan Rai (1994) 79 Comp. Cas.150. [SC].*

beginning, even at the cost of repetition, we may analyse what exactly is the nature of EFT.

- 2.3. There is a wide variety of definitions of EFT. The earliest definition appears to be the one provided in the United States Electronic Fund Transfer Act, 1978<sup>1</sup>. Section 903(6) of this Act defines:

**The term "Electronic Fund Transfer" means any transfer of funds, other than a transaction originated by a cheque, 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 or credit an account. Such term includes, but is not limited to, Point of Sale transfers, Automated Teller Machine transactions, direct deposits or withdrawals of funds and transfers initiated by telephone.**

This definition includes not only credit transfers but almost all forms of electronic payments like card payments, ATM transactions and tele-banking.

- 2.4. A little more focussed is the definition of Funds Transfer System found in Section 105 (5) of Article 4A of the Uniform Commercial Code (UCC) of the US. According to this definition:

**Funds Transfer System means a wire transfer network, automated clearing house or other communication system of a clearing house or other association of banks through which a payment order by a bank may be transmitted to the bank to which the order is addressed.**

- 2.5. The Jack Committee on banking services<sup>2</sup> defined EFT as

**A Funds Transfer effected through the banking system by electronic techniques with input and output methods being largely or completely in electronic form.**

- 2.6. A simpler definition is to be found in the UNCITRAL Model Law<sup>3</sup>, where EFT is defined as,

---

<sup>1</sup> Title IX, Consumer Protection Act 15 U.S.C.A. Section 1693 et seq.

<sup>2</sup> Report of Review Committee on Banking Services, HMS, London [1988]

<sup>3</sup> UNCITRAL Model Law on Credit Transfers, United Nations, New York, [1992]



**The Funds Transfer in which one or more of the steps in the process that were previously done by paper based technique are now done by electronic technique.**

- 2.7. From a judicial point of view<sup>1</sup>. EFT is an authority and instruction, from the customer to the bank, to transfer an amount standing to the credit of that customer with that bank to the credit of his account with another bank or to the account of another customer. In brief, an Electronic Funds Transfer is a payment transaction carried out between two parties without the use of cash or paper to effect the transaction<sup>2</sup>.
- 2.8. The essential legal nature of an EFT as we notice in each of the above definitions, is that a payment is effected by communication of electronically transmitted message to his bank by a customer of a bank or a bank to another bank. The bank to which message is sent assumes an obligation to the beneficiary by crediting the beneficiary's account with the amount directed to be paid. Unlike in the case of a paper based fund transfer, the beneficiary's bank assumes a liability not on the strength of the funds paid to it by the drawer's bank but on request/message (without any correspondence arrangement) of the sending bank. The expressions, "Electronically Transmitted Payment" or "Electronic Payment" or "Electronic Funds Transfer" convey the same meaning. The communication network established by banks and service providers for this purpose is the System.
- 2.9. In essence, there are three types of transactions that can be performed by electronic means.
- (i) Debiting or crediting one's own account,
  - (ii) transferring funds between two accounts by issuing a credit instruction to one's own institution and
  - (iii) transferring funds between two accounts by authorising a debit authorisation to another party.

Debiting and crediting one's own account in a bank is done through ATMs. The second type of transaction consists of issuing a credit instruction to one's

---

<sup>1</sup> Webster. J, in *Royal Products V. Midland Bank Ltd.* [1981] 2 Lloyd's Rep. 194

<sup>2</sup> Anu Arora, *Electronic Banking and the Law*, IBC, London.[1988]

own bank requiring it to transfer funds to the account of another person. The third type, also known as debit transfers enables utilities like telephone service, electricity service, etc. to collect bills. EFT in a more restricted sense is used only to denote credit transfers of this type.

## **TYPES OF EFT SYSTEMS**

- 2.10. Electronic payments are called differently, depending on the type of use, value of funds, who initiates the transfer or mechanisms of settlement systems. We may note them briefly to understand the scope of EFTs.

### **Credit transfers and debit transfers**

- 2.11. Funds transfers are divided into two categories determined by whether the **instruction** to pay is given by the person making payment or the person receiving payment. If the instruction is given by the **person making the payment**, the transfer is commonly referred to as a **credit Transfer**. If the instruction is given by the **person receiving payment**, the transfer is commonly referred to as a **Debit Transfer**. Historically, credit transfers owe their origin to the banking practice in running a standing order service to facilitate the payment of fixed amounts at regular intervals.

### **Credit Transfers**

- 2.12. A credit transfer system enables a person to make payments through his bank either to other customers of the same bank or those of other banks. A person without a bank account also can use the system and avoid sending cash or postal order or money orders through post. The system can also be used by institutions or individuals who have to make a large number of payments regularly for varying amounts to different payees. To understand the transactional details of a credit transfer, we may state a simple credit transfer transaction. 'X', who owes money to 'Y' and wants to pay the money, can do so by delivering/sending Y a cheque which enables Y to obtain payment from a bank through clearing. Instead of doing this, X may transmit an instruction to his bank to credit Y's account with the amount specified. In EFT parlance, such an instruction is called a payment order of X (Originator or issuer). Y is the beneficiary. X's bank thereafter transmits an instruction electronically to Y's bank (beneficiary's bank) to carry out X's payment order. This is normally known as execution by X's bank of the payment order. The instruction of X's

bank may be directly conveyed (normally if there is a correspondent arrangement, otherwise Y's bank may not take the risk of crediting Y's account without actual receipt of payment from X's bank), or through intermediary banks. In such a Funds Transfer System, normally a settlement institution takes responsibility for settling the obligation between banks by debiting the sending bank's account and crediting the beneficiary's bank's account, with it. In this system, the beneficiary's bank normally (depending upon the arrangement) relies on the credit and makes the payment to the beneficiary before it actually receives the payment. In other words, by accepting a payment order, the Y's bank obliges itself to Y. Thus, in a credit transfer system, payment is made by substitution of obligations without there being any actual movement of funds.

## **Debit Transfers**

- 2.13. In debit transfers, banks make payments out of their customer's account to third person who instructs the bank to transfer the amount to his own account with his bank. This will be done if the customer of the paying bank gives it an appropriate mandate for the purpose. The payment is, therefore, initiated by the payee and because of the possibility of a fraud, the banks normally give direct debit facilities only to payees of high financial standing.

## **High Value and Low Value Transfers**

- 2.13. Credit transfers, depending upon the value of payment order, manner of execution and settlement are divided into two types - **bulk transfers** (high volume low value transfers) on the one hand and **high value transfers** (also called as wire transfers) on the other. Generally, high volume - low value fund transfer instructions are executed in batches through an Automated Clearing House (ACH). The settlement of obligations between banks is done on an end of the day netting basis. On the other hand, wire transfers or high value transfers are executed on real time basis and settlement is normally done on gross basis in respect of each transfers.

## **Automated Teller Machine (ATM)**

- 2.14. The modern ATMs have become an accepted part of the facilities offered by banks in developed countries and many developing countries, although in India it is only an emerging phenomenon at present. The ATM System

generally is operated through an electronic device and is used for withdrawing of cash, depositing of cash and cheques and connected operations like transfer of funds from one account to another account. The relation between bank and customer is determined by contract.

## **Electronic Funds Transfer at Point of Sale (EFTPoS)**

- 2.15. EFTPoS is a payment system which enables goods or services to be paid for, by transmitting over a communications network, details of the transaction to both the customer's and the retailer's bank without the use of paper vouchers. EFTPoS is basically an Electronic Clearing System which can accept credit card entries and transaction cards or debit cards, ATM Cards and charge cards. Normally, the parties involved in ATMs and EFTPoS are an issuer (a person who in the course of his business makes available to the member of the public a payment device **pursuant to a contract** concluded with him), a system provider (a person who makes available a financial product under a specified trade name and usually with a network and thereby enabling payment devices to be used for the operations), contracting holder (a person who **pursuant to a contract** concluded between him and issuer holds a payment device), and of course the retailer and the bank. The legal relation between the participants are normally built by a complex chain of contracts.
- 2.16. In EFTPoS, the two minimum parties to a credit card transaction are the purchaser who uses the card to pay and the merchant who accepts the payment. Additional parties include the bank that issued the card to the purchaser and the bank which enrolled the merchant in the credit card system and the credit card corporation who usually processes the transaction.

## **Cheque Truncation**

- 2.17. Cheque truncation is a process in which the image or relevant data of a cheque is electronically captured and transmitted to enable payment of that cheque to the payee's account and simultaneously debiting the account of the drawer without the physical movement of the cheque itself. This system is in vogue in some of the European countries like France, West Germany, Spain, Austria, etc. Cheque truncation as a concept has not become popular in U.K. as actual physical presentment is required by law<sup>1</sup>. It is in operation in U.K., only when

---

<sup>1</sup> *Bills of Exchange Act 1882, Section 45. For the progress made in U.K., see generally, Jack Committee Report Page 56-57.)*

the drawer and payee of a cheque have accounts at different branches of the same bank.

## BASIC CHARACTERISTICS OF ELECTRONIC PAYMENTS

- 2.18. Our study of the different types of electronic payments and fund transfer systems show that essentially payment or funds transfer is effected through electronic techniques. EFTs are payment messages transmitted either through magnetic material such as magnetic tapes, disks and cassettes; or through purely electronic media such as telephone, telex and electronic transmission between computers or between a terminal and a terminal. To understand what types of problems and legal issues are associated with EFT transactions, it would be advantageous to first notice the special characteristics that distinguish EFT from the existing paper based payments.
- 2.19. By its very nature **speed** is the first distinguishing character that distinguishes an EFT from any paper based system of payment. The characteristics of paper based instructions and undertakings are that they embody a transaction in permanent form, are typically expressed in words and figures and are authenticated by a signature identifying a party giving the payment message. Paper based messages cannot readily be erased without this fact appearing on the face of the document. Finally, delivery of the payment message usually takes a significant period of time - hours, days or even weeks. The payment message in electronic payment system is expressed in computer code. The hand written signature is replaced by an electronic key designed to authenticate a message, and in contrast to a paper message, where the message itself is permanent and is retained on the original paper, the message on tape, disk etc. may in the absence of security measures, be erased or transferred to other magnetic material without this fact being discoverable from an examination of the medium<sup>1</sup>.
- 2.20. Having noted the different types of electronic payment mechanisms in use, and the special characteristics which distinguish them, we may now advert to what new problems they bring from the point of view of legal rights and obligations.

---

<sup>1</sup> For a detailed analysis of distinguishing characteristics of EFT see generally, R. M. Goode, *Electronic Banking -The Legal Implications*, Institute of Bankers, London, [1985].)

## **COMMON ISSUES IN EFT**

- 2.21. The following substantial issues of regulatory nature emerge in an EFT context:**
- **Monetary and Credit Policy Considerations**
  - **Consumer Protection Issues**
  - **Economics (Competition) and Development Issues**
- 2.22. The following transactional issues which have also legal implications emerge from the characteristics pointed out above:**
- **Authentication of instructions**
  - **Countermanding or reversal of instructions**
  - **Operational security of the systems**
  - **Liability for loss in case of fraud, technical failure and errors.**
  - **Allocation of loss in case of insolvency.**
- 2.23. There are also some issues of general nature which have a special significance for EFT Systems. These are :**
- **Cheque truncation.**
  - **Evidence and burden of proof.**
  - **Preservation of records.**
  - **Data protection.**
  - **Dispute resolution.**
  - **Prevention of fraud.**
  - **Settlement of inter-bank payment obligations.**

- 2.24. It would be instructive to see how the above issues are dealt with in countries where EFTs have been prevalent for quite some years.

### **Legal framework in other countries**

#### **1. United Kingdom (U.K.)**

- 2.25. Historically, the most proximate legal system to India is the legal system in U.K. In the U.K., there are 6 EFT systems<sup>1</sup>.
- Automated Teller Machine (ATM's) - started in 1967
  - Bankers Automated Clearing Services (BACS) - started in 1971
  - Society for Worldwide Interbank Financial Telecommunication (SWIFT) - started in 1973
  - Electronic Fund Transfer at Point of Sale (EFTPoS) - started in 1974
  - Home and Office Banking System - started in 1982
  - Clearing House Automated Payment System (CHAPS) - Started in 1984
- 2.26. In addition to the above, fund transfers in the U.K. are processed through one of the clearing houses established by APACS (Association for Payment Clearing Services) . APACS is an unincorporated association with leading banks of U.K. as its members and was set up in 1985 to manage the development of payment clearing service and to oversee transmission generally. Electronic clearings, however, are done by CHAPS for single high value same day credit transfers and BACS for high volume batch payment service for both credit transfers and direct debits.
- 2.27. To avail the services like EFTPOS, the customers verify and authorise by signing the transaction slips produced by the terminal or by entering thereby PIN by a special key. PIN authorised transaction is normally sent encrypted to the card issuing institution for verification with the transaction data.

---

<sup>1</sup> *Report of the Review Committee on Banking Services, HMSO London 1989, Page 76.*

- 2.28. It is interesting that there was no statute specifically designed when any of the above EFTs were started. The services were arranged by drawing up contracts between two system operators to govern their mutual rights and obligations. Nor was there any amendment to existing transactional laws. In the case of cards, bankers normally adopted standard terms and conditions on contractual basis. Problems, wherever they arose were resolved by and large by application of analogous laws like the Bill of Exchange Act and the general principles of common law<sup>1</sup>.
- 2.29. The sphere of contract law on which the EFTs were functioning in U.K. came to be under stress as system operators and institutions were criticised for abusing their positions. By and large in all EFT transactions especially in Card based EFTs, the terms of contract were so much one sided that the liability of the card holder was almost absolute. He was responsible for any payment order attributable to the card even though it resulted by fraud of third parties without any fault of the card holder. Banks availed themselves of the exemptions and exclusions to the maximum extent. The only way a cardholder could escape the liability on account of third party fraud was by giving notice of loss of the card or third party access to the card and request for cancellation of the card. Even then, his liability continued for all transactions, attributable to his card until the notice became effective.
- 2.30. The Unfair Contract Terms Act, 1977 though, to some extent, helped in restricting exclusion of liability by card issuers, did not effectively provide a solution<sup>2</sup>. Widescale abuse of the contract eventually led the British Government and the Bank of England to refer EFT related problems to a Committee set up in 1987 to review the law and practice governing banking services. Thus, it was basically from a customer service and consumer protection angle that the question of EFT legislation was considered. This Committee had submitted its report in 1988 concluding therein that a basic statutory framework was necessary although the statute must be confined to bare minimum provisions for regulatory purposes and a flexible legal structure through administrative legislation process should be designed. The Committee also made several recommendations in terms of **Best Banking Practices**.

---

<sup>1</sup> *Momm and Others V. Barclays Bank Intl. Ltd.* (1976)3 All. ER 588; *Mardorf Peach & Co., V. Attica Sea Carrier* (1977) AC 850 [HL].

<sup>2</sup> Generally see *Jack Committee Report*, Page 189.



- 2.31. At present although a comprehensive legislation separately covering all aspects of electronic payments and EFT of all types has not yet been enacted in UK, many of the regulatory and consumer interest issues have been addressed by amendment to some of the existing laws and through administrative regulations. For example, the Consumer Credit Act, 1974 was amended by the Banking Act, 1987 to deal with regulation of EFTPoS<sup>1</sup>. Similarly, the office of Fair Trading established under the Restrictive Trade Practices Act, 1977 have formulated a Code of Good Practices in regard to card business. An extract of this code is in Annexure 3. The British Bankers' Association (BBA) have also adopted effective from 16.3.1992, a Code of Good Banking Practices. Part B of this code dealing with card business by banks is in Annexure 4.

## **United States of America (USA)**

- 2.32. The world's first EFT Act was made in the United States in 1978. The Electronic Fund Transfer Act, 1978 was basically a consumer protection measure and in fact it is codified as title IX of the Consumer Protection Act<sup>2</sup>. This Act, apart from defining certain basic concepts, lays down the disclosure norms in regard to terms, pricing, etc. It also requires the service providers to supply transaction record. This Act, however, applies mostly to consumer activated consumer payment systems and other consumer related EFTs like EFTPOS and ATMs. Inter-bank and intra-bank fund transfers are not covered by Electronic Funds Transfer Act, 1978. This Act is administered by the Board of Governors of Federal Reserve System and the Board in turn has made its administrative regulations<sup>3</sup>.
- 2.33. Problems and abuse of contractual terms in regard to EFT devices was dealt with in the United States through a separate legislation. The U.S. Congress enacted the Fair Credit and Charge Card Disclosure Act, 1988. This is again

---

<sup>1</sup> Section 89 of the U.K. Banking Act 1987 introduced a new Section 187(3A) in the Consumer Credit Act, 1974 and Section 88 amended several sections of Consumer Credit Act to deal with EFTPoS.

<sup>2</sup> 15 USSCA Section 1693 et. seq.

<sup>3</sup> For the structure of the legal framework for EFT in the U.S., see generally Edward L. Rubin & Robert Cooter, *The Payment System*, American Case Book Series, West Publishing Company, Minnesota [1989]. Also see, Ernest Patrikis & Debra W. Cook, *International Payment Transactions - Practical Execution, Risks and Legal Regulation*.

a consumer driven legislation closely linked to the Expedited Funds Availability Act<sup>1</sup>.

- 2.34. The inter-bank and intra-bank funds transfers and international electronic payments are carried in the U.S. through two main Fund Transfer Systems: -
- **(CHIPS) Clearing House Interbank Payment System**
  - **Fedwire - Federal Reserve Fund Transfer System**
- 2.35. CHIPS is a multilateral system owned and operated by the New York Clearing Association although payments of all types may be through CHIPS. A large portion of the payment transferred over this system are in settlement of international transactions. The system works largely on voluntary regulations. The basic trigger events are now governed by Article 4A of Uniform Commercial Code. The settlement of payments carried on CHIPS is done through Federal Reserve Bank.
- 2.36. Upto 1991, CHIPS was governed by its rules and the agreement between CHIPS and the participants. The relationship between participants and between participants and their customers were governed by a confusing blend of contract and Torts law. The U.S. Codes were applied by analogy of the principles applicable to paper based payments for solving certain issues arising under CHIPS transactions. This confusion, however, was put to an end in 1991 when most of the States in the U.S. adopted Article 4A of the Uniform Commercial Code. The Headquarters of CHIPS is located in New York and the State of New York has adopted Article 4A.
- 2.37. Another most important in terms of volume of transactions, is **Fedwire Fund Transfer System**. This is a system operated by the Federal Reserve Banks for large value electronic fund transfer services provided by it. It is used primarily for domestic payments, bank to bank and third party transfers such as interbank overnight funds sales and purchases and settlement transactions

---

<sup>1</sup> *The Fair Credit and Charge Card Disclosure Act 1988 imposes additional disclosure requirements on credit card issuers. The Expedited Funds Availability Act 1991 was passed to cut the collection time taken by banks for collection of cheques. It compels the bank to credit the customers account with the amount of the cheque within the specified time. These measures are considered as reversal of deregulation moves followed in the seventies and early eighties.*

and corporate to corporate payments made through banks. Transfer of funds through Fedwire are governed by an unusual blend of law<sup>1</sup>. The wire transfer of funds are governed by a regulation administrative legislation promulgated by the Board of Governors of the Federal Reserve System pursuant to their powers under the Federal Reserve Bank Act, 1938. This regulation is known as Regulation J<sup>2</sup>. These regulations explicitly incorporate Article 4A of the Uniform Commercial Code. But to the extent, if there is any conflict between Article 4A and Regulation J, it is Regulation J which will prevail.

- 2.38. The object of Article 4A of Uniform Commercial Code, is to remove the confusion and uncertainty in the application of legal principles to various rights and obligations between parties in electronic fund transfers. It addresses basically issues relating to completion of funds transfer (finality of payment), issues relating to authentication (security procedure), issues relating to execution and acceptance of payment orders and issues relating to allocation of loss. The interesting point is that the statute provides essentially the default rules without taking away the traditional rights of parties to determine by contract, the security procedure and trigger events. It is thus clear that it is Article 4A which contains the basic statute to govern the type of funds transfer which this Committee is concentrating on.

## Other European Countries

- 2.39. Among European countries, **France and West Germany** were the earliest to start EFT systems. In fact, France is credited with having brought in the first electronic cards used in payments, but till date there is no specific statute in France governing the EFTs. The transactions are governed by contracts. West Germany also does not have any statute specifically designed for electronic payments. There are certain basic regulations made by the Central Bank for supervisory purposes in EFT transactions. Cheque truncation which has attained maximum acceptance in West Germany is carried on by interbank agreement. **Belgium** is another leading European country to have comprehensive EFT system including advanced cheque truncation system. However, like France, Belgium has also no statute law. EFTs are governed by

---

<sup>1</sup> For legal aspects of Fedwire System see generally Ernest T. Patrikis and Debra W. Cook, *International Payment Transactions, Practical Execution, Risks and Legal Regulations*.

<sup>2</sup> 12 CFR Sections 210.25 and 210.32.

contracts which covers matters including availability or otherwise of computer print outs, revocability and completion of payment, customer's duty regarding safety and security procedure and loss of security devices. The contract also determines the liability between the banks and customers. Under the general law of Belgium, burden of proof is on any claimant.

- 2.40. **Denmark** has a statute known as Payment Card Act, 1985 which again is a consumer protection legislation. Denmark is the only country having a fully developed truncated cheque clearing system.

## **Other developing countries**

- 2.41. Not much information was available to us regarding other developing countries. In **Malaysia**, a Committee was set up in 1988 to go into the question of EFT legislation. On the basis of the report of that Committee, the Banking Act of Malaysia was amended to enable the Central Bank there to make administrative regulations. No comprehensive statutory framework to govern transactional issues however, appears to have been made so far in Malaysia<sup>1</sup> **Singapore** also does not have a separate statute for electronic fund transfer. The largest developing country, **China** is reported to be in the final stage of implementing a comprehensive electronic payment system through the aid and project assistance of the World Bank. The outline of this system as made available to the Committee by the World Bank would show that EFT system in China will be a single countrywide system for interbank and intra-bank funds transfer covering both high value and low value transactions. The People's Bank of China would own and operate the system. It will also act as a Settlement Bank. Similar payment system with the project assistance of the World Bank is being developed in **Vietnam**.
- 2.42. The **UNCITRAL**, the trade law wing of the United Nations, has been working on EFTs since early eighties for developing uniform EFT regulations throughout the world. It came up with a complete guide on EFT in 1987. It was prepared to aid legislators and lawyers considering the rules for a particular network.

---

<sup>1</sup> The Committee was informed by the Legal Department of Bank Negara Malaysia, by their Fax message of Nov. 7, 1995 that although there is no separate EFT Act, the Banking and Financial Institutions Act 1989 (Malaysian BAFIA) by Section 119 made elaborate provision enabling the central bank to regulate EFT Systems. This Act prohibits any person from operating any electronic fund transfer system without the central banks authorization in writing.

As many as 41 legal issues arising in the use of EFT system were identified in this guide. This is a valuable work of reference to the regulators in the EFT field especially, regulators in the developing countries. In 1992, UNCITRAL has finalised a Model Law for EFT, but these rules are mainly concerned with, international credit transfers between banks.

- 2.43. The above study shows that not all countries, where EFTs have been functioning, have separate legal framework for EFTs. Some countries like USA have comprehensive legislative framework while some countries like UK have considered it unnecessary to have a separate legal framework. However, concerns are being felt in every country about the need for having some regulatory framework to take care of the substantive issues associated with EFTs.

## CHAPTER III

# TECHNOLOGY IN INDIA, INDIAN AND OTHER LAWS

### Introduction

- 3.0.1. Law has many facets and functions. Infrastructure of a legal framework consists of a hierarchy of legal rules - statutes, rules and regulations made under statutes, case law or rulings of superior courts and finally, contracts. Each of them have their own advantages and disadvantages. When the underlying matter is an emerging and evolving subject, like the EFT Systems, where the technology is growing and fast changing, structuring a legal framework involves judgement about a proper blend of basic statutory provisions and an appropriate rule making mechanism and contractual arrangements. The legal infrastructure needs to be tuned so as to be adaptable to the needs of changing environment. A responsive and flexible infrastructure not only adapts to the needs of emerging issues but can also function as an instrument for effecting desired developments. On the other hand, a rigid legal framework can hamper, and at times, virtually seal the development in an evolving and emerging scenario. Whether a comprehensive statute framework is needed or a flexible subordinate legislative structure would better subserve or whether the matter should be left entirely to the domain of freedom of contract, is a matter that will have to be judged on a number of factors.
- 3.0.2. Whenever a new legislative framework is to be provided in a comparatively virgin field, the temptation to copy an already existing model is very high. But copying legal models on a subject like payment systems, without paying attention to the ground realities of existing laws and the status of existing technology and banking habits, may lead only to appearance of modernisation. But it may easily miss the objectives and in the process, create irreversible damage to the economic fabric and its environment<sup>1</sup>. The object of our study

---

<sup>1</sup> For dangerous effects of copying economic models, see generally, Ibrahim F.I. Shihata, "The World Bank in a Changing World" Martinus Nijhoff Publishers, Dordrecht (1991)

of the legal structure governing EFT in other countries was only to understand the basic legal issues that need to be addressed.

- 3.0.3. This Chapter is structured in four parts. In the First Part, a review of the existing ground realities in India in regard to the status of technology is made. In the Second Part, the existing legal provisions having a bearing on the substantial and transactional issues in EFT are analysed. The Third Part addresses other legal issues in EFT. The Fourth Part contains the summary of the Committee's findings and an analysis of relevant considerations for recommending a legal framework for EFT in India.

## **PART - I**

### **PRESENT STATUS OF TECHNOLOGY IN INDIA**

#### **Payment system mainly paper-based.**

- 3.1.1. Payment system in India is primarily paper-based. Currency notes and paper instruments like cheque, draft, dividend and interest warrants, refund order, gift cheque, travellers cheques and stockinvest etc., are the commonly used methods of settling payment transactions. Use of computer and communications technology in payment system in India is a relatively new phenomenon. Although computers are in use in some banks right from late sixties, they were used mainly for corporate data-base maintenance and statistical analysis. Telegraphic Transfer of funds is the only popular mode of paperless funds transfer in payment system. Funds transfer through EFTPoS, Home banking, Debit Card etc. are still to strike roots in India. Even the few available ATMs are used mainly as cash dispensers and not for funds Transfer and Utility bill payments as elsewhere. Telephone banking is yet to take firm shape.

#### **Telegraphic Transfer**

- 3.1.2. In early eighties, some of the major banks installed inhouse telex/communication systems and employed them for routing funds transfer messages. This marked an advent of electronic technology for inter-branch funds transfer within a bank. Others used the telex/telegram service of the Department of Posts and Telegraph. Even today, at inter-branch level it is the popular mode of funds transfer. However, a funds transfer mechanism

involving inter-bank funds settlement at the national level is conspicuous by its absence. The Reserve Bank has a Remittance Facilities Scheme for banks which caters to their limited needs for currency chest operations and Government transactions but the ordinary customers of banks do not enjoy any such facility.

## **MICR Clearing**

- 3.1.3. So far, the focus of technology upgradation in payment system has been on improving productivity and efficiency in processing of paper based instruments. As a result, in India, we have had rationalisation of draft issuance procedure, courier arrangements for collection of inter-city cheques, computerisation of the Service Branches and the Clearing Section of the large branches and computerisation of clearing houses etc. The Reserve Bank had introduced MICR clearing at the four metropolitan cities and plans to extend the same shortly to 26 new centres. Under the MICR clearing, unlike in the manual system, debits to individual banks were raised on the basis of the data captured mechanically during the cheque sorting process. Drawee banks are provided with the **cheques** as well as the **print-outs** indicating the details of the cheques and the amount debited.

## **Electronic Credit Clearing**

- 3.1.4. MICR clearing provided a wealth of information to the Reserve Bank on the instruments passing through the clearing system. An analysis of the data revealed that about 23 percent of cheques are in the category of interest/dividend/refund payments by the companies/corporations and Government Departments. These also represented relatively low value payments compared to other types of instruments and are repetitive in nature. Such instruments generally owed their origin to corporate bodies who made interest payments to the same set of beneficiaries at periodic intervals. It was considered in the Reserve Bank that such payments involving a single, albeit large debit (to the corporate body) and multiple smaller credits (to the beneficiaries) could be effected directly by the banking system without the intermediation of paper instruments. Therefore, a Scheme called Electronic Clearing Service (Credit Clearing) was launched by the Reserve Bank in April 1995. The Scheme envisages presenting of payments data on magnetic media by a corporate body to its banks who in turn will forward the same to the Clearing House with an authorisation to debit its account and credit the accounts of the



beneficiaries as recorded on the magnetic media. The procedural guidelines for operating such a Scheme were prepared and a provision was made to get these guidelines adopted by the member banks of the clearing house so that all banks would be bound by a common discipline.

- 3.1.5. The Electronic Clearing Service at present is not entirely automated. The input to Clearing House is on electronic media, but the banks of the beneficiaries are presently provided with printed credit reports by the clearing house. Soon the credit data would be supplied as an electronic data file duly encrypted before transmitting/handing over the data to banks. The service branches of banks would generate credit reports at their end.

## **Electronic Debit Clearing**

- 3.1.6. A Debit Clearing system is also on trial run at Madras Clearing House. Under this system, Telephone Department of Govt. of India collects telephone bills of some telephone subscribers of one of the telephone exchanges at Madras. This operates on the principle of "authorised debit". The telephone subscribers willing to participate in the Scheme give a mandate to their banks to debit their accounts when they would receive debit advice from the Debit Clearing system. The subscriber may indicate a cap amount in the mandate. The bank would be within its right to dishonour the claim from Debit Clearing system if the amount exceeds this cap. Like the Credit Clearing, Debit Clearing was also introduced after passing a resolution in the General Body Meeting of the Clearing House. Department of Telephone submits the debit clearing data on magnetic media (Reserve Bank itself being the banker to the Telephone Department) and inter-bank funds settlement is effected by debiting various banks and crediting the account of the Telephone Department. Debit advices are presently on paper format and would be shortly made electronic.

## **Floppy Input Clearing**

- 3.1.7. Floppy Input Clearing is another mode of electronic clearing introduced at 14 centres where Reserve Bank manages the Clearing Houses. All clearings, except the MICR clearing at the four metropolitan centres are claim-based. Banks sort the cheques bank-wise, exchange the same amongst themselves and lodge a claim through the clearing system for the amounts for which they had presented cheques to other banks through a claim statement. The claim statements from various banks were forwarded together to arrive at final

settlement statement. The manual system was followed at all centres where clearing houses have been set up. Subsequently with the advent of microprocessors and minis, the claim statements were used as "input" for data entry at the clearing house. While this had the advantage that data entry systems needed to be installed only at clearing house, it also suffered from the disadvantage of erroneous input data preparation going unchecked at Clearing Houses and the difficulty in fixing responsibility. Hence a system called "Floppy Input Clearing" was evolved by Reserve Bank. According to this system data preparation was shifted to the banks away from the clearing houses and was also made the sole responsibility of the participating banks. Banks were required to submit the data on electronic format and the clearing house would consolidate the data and generate the settlement statement. This system has been implemented in 1995 at all the Reserve Bank managed clearing houses and will shortly be introduced at the clearing houses managed by State Bank of India also.

### **Total Branch Computerisation (TBC).**

- 3.1.8. After signing of the agreement between the unions and IBA in 1993, the pace of computerisation in the banking industry has quickened. Of the 4000 branches of the 27 public sector banks required to be upgraded under Total Branch Computerisation, around 550 branches are fully computerised. These branches are now capable of receiving data electronically and processing them without use of paper documents. As the pace of computerisation grows (the number of TBC branches may go up to 1000 by March 1996), electronic banking would get a further push. Banks having a good number of TBC branches have already started products like "Any Branch Banking" and Electronic Funds Transfer between selected branches. Banks are increasingly using technology to enhance their competitive strengths.
- 3.1.9. Some foreign banks, and newly established private sector banks have relatively superior technological infrastructure and fully computerised banking environment. Some of them have also started telebanking service.

### **SWIFT**

- 3.1.10. India joined the Society for World-wide Inter-bank Financial Telecommunication (SWIFT) in 1991 as the 74th country. Initially, 41 banks in India participated. More banks are now participating and the number of branches registering

under SWIFT's Bank Identification Code (BIC) Directory is also on the increase. SWIFT is not a payment system per se, but has helped considerably in the transmission of international payment messages.

## **BANKNET**

- 3.1.11. A communication network called BANKNET has been setup in 1991 connecting four metropolitan centres of Bombay, Madras, Delhi and Calcutta along with Bangalore, Hyderabad and Nagpur. The Communication switches (X.25) are located at the four metro centres and at Nagpur. All five switches are interconnected to provide alternate routes. Bangalore and Hyderabad centres are connected through remote PADs to the switch at Madras.
- 3.1.12. A communication software (called "Comet") had been designed primarily for templates-based applications. This is now supplemented by a communication software named "RBInet". This software provides dialup connectivity and has the facility of ASCII file transfer which was not available under "Comet". RBInet has also message tracking facility which was not available under COMET. Usage of RBInet is growing and Reserve Bank plans to use this network as the main electronic link with banks.

## **PART - II**

### **REVIEW OF EXISTING LAWS IN INDIA**

- 3.2.1. Having noted the existing status of technology, we may look at the existing position of law in India that has a bearing on the EFT issues outlined in paragraph 2.21 and 2.22 of Chapter II.

#### **Substantial issues of regulatory nature**

- 3.2.2. We had listed the following three issues of substantial nature involving policy formulation:
- Monetary and credit policy considerations
  - Consumer protection
  - Economics of competition and development

## MONETARY AND CREDIT POLICY CONSIDERATIONS

- 3.2.3. Payment systems, in all forms have a direct bearing on the financial sector in general and banking sector in particular. There is a growing recognition that at a particular stage of development, electronic funds transfer system supports sound financial market development through improved certainty and timeliness of payments. But, every new system would bring a new crop of problems for the regulators<sup>1</sup>. EFT systems, especially due to their potential for generating unaccounted credit and money supply, have been viewed as a close concern of the central banking authorities<sup>2</sup>.

### Central Bank's Role

- 3.2.4. In EFT Systems, where the central bank acts as an intermediary or takes on itself (as is the usual case) the clearing and settlement responsibilities, the central bank is exposed to the risk through float (daylight overdrafts) and unless this is regulated an excessive volume of money gets pumped into the system. In card operations, the float may create an unaccounted increase in the volume of credit in the system. Further, because of the speed in the EFT System, systemic risk due to a bank failure would get an expedited transmission into the banking system. This will be more so when EFT Systems are organised without the involvement of the central banks' settlement machinery<sup>3</sup>. Apart from these, there are also the supervisory concerns relating to monitoring the volume and pattern of transactions in the payment system<sup>4</sup>. Misuse of the EFT System for evading exchange control, tax liability or for money laundering and other unlawful purposes needs to be specifically addressed.
- 3.2.5. The role of the central bank as monetary and credit authority leads us to examine whether the existing legal provisions are sufficient to take care of the monetary and regulatory issues that may crop up when EFT Systems are introduced.

---

<sup>1</sup> For a critical analysis, see Raj Bhala, "Towards A Payments System Law for Developing and Transition Economies" World Bank Discussion Papers, The World Bank, Washington DC (1995).

<sup>2</sup> Clifford Chance, "People's Bank of China Payment Systems Project" A World Bank Assistance Paper (1995).

<sup>3</sup> UNCITRAL Legal Guide on Electronic Funds Transfers, United Nations, New York (1987).

<sup>4</sup> Raj Bhala, Towards a Payments System Law for Developing and Transition Economy, World Bank Discussion Papers, The World Bank, Washington DC 1995 Page 28.

## **Powers of the Reserve Bank**

- 3.2.6. In India, the powers and functions of the Reserve Bank, which is the central bank of the country, are contained in the Reserve Bank of India Act, 1934, (RBI Act), the Banking Regulation Act, 1949, (BR Act), and the Foreign Exchange Regulation Act, 1973 (FERA). The provisions of Public Debt Act (PD Act) could also be relevant in so far as the government securities transactions are concerned.
- 3.2.7. The existing provisions of the RBI Act do not specifically empower the Reserve Bank to make Regulations for defining rights and obligations of participants in an EFT transaction. Section 17(6), however, empowers the Reserve Bank to operate a remittance system for transfer of funds payable at its own offices or agencies. Section 58, which deals with the regulation making power of the Central Board of the Reserve Bank, empowers the Reserve Bank to make Regulations "consistent with the Act to provide for all matters for which provision is necessary or convenient for the purpose of giving effect to the provisions of the Act." The preamble of the Act provides that the Reserve Bank is constituted among other things, "to secure monetary stability and generally to operate the currency and credit system of the country to its advantage". But except for the provisions dealing with currency notes, there is no substantive provision in the Act specifically dealing with payment system as such. Sub-section (2) of Section 58 lists at clause (p), "the regulation of Clearing Houses for the banks including post office savings bank" as one of the items for which the Central Board may make Regulations. Therefore, by reading the provisions of Section 17(6) and Section 58(2) (p) with the preamble, a view can be taken that the Central Board of the Reserve Bank can make Regulations for an EFT System that may be set up and operated by the Reserve Bank<sup>1</sup>.
- 3.2.8. As far as banks alone are concerned, the Reserve Bank has adequate powers, under the BR Act, of issuing directions binding on them.
- 3.2.9. In the context of the growing and fast changing technology and the need for

---

<sup>1</sup> It is interesting to note that in the U.S., the authority for the Board of Governors of the Federal Reserve System to frame Regulation "J" Part B, which governs the Fedwire system, is traced to Sections 13 and 19(f) of the Federal Reserve Act. These provisions do not specifically mention electronic payment or electronic funds transfer, as such. They more or less correspond to the relative provisions in the Reserve Bank of India Act regarding issue of notes and remittance of funds.

improving the payment systems to be in tune with the overall financial sector development, a question may arise for permitting one or more banks to organise different/multiple types of payment systems to cater to the needs of different sectors. In such a scenario, special powers of monitoring and controlling the multiple EFT Systems in the country may be required to be exercised by the Reserve Bank. This would need an amendment to the RBI Act.

## CONSUMER PROTECTION

3.2.10. Legal issues concerning consumer protection in regard to EFT operations center around the following aspects:

- Transparency of charges (protection by proper disclosure)
- Access to information in case of disputes
- Confidentiality, unfair conditions, frauds, mistakes and errors.

3.2.11. It may be pointed out that in the United States, the movement for an EFT legislation was essentially driven by consumer protection considerations. The EFT Act of 1978 is codified as title IX of the Consumer Protection Act. This Act requires EFT service providers to disclose the terms and conditions and also to supply records of transactions, thereby increasing consumer information. The Act also creates disputes resolution procedure and imposes caps on consumer liability, thus removing consumer liability from the general contract law. This Act, however, governs only EFTs involving consumer payments. It does not govern the Fedwire System or Credit Transfers. It is worthwhile to note that the Act is designed as a typical socio-economic legislation with maximum flexibility. Wide ranging rule making powers are given to the Board of Governors of the Federal Reserve System (Fed Reserve). The responsibility of implementing the Act has been entrusted to Fed Reserve who have issued Regulation E for implementation of the Act.

3.2.12. The European Commission (EC) had adopted in November 1988, certain specific provisions in regard to consumer issues and required the member countries to make specific legal provisions to ensure that service providers draw full and fair terms of contract in writing<sup>1</sup>. In the U.K., the Consumer

---

<sup>1</sup> Extract of the European Commission Recommendations on payment cards is in Annexure 5

Credit Act, 1974, the Restrictive Trade Practices Act, 1977, the Unfair Contract Terms Act, 1977 and the Banking Act, 1987, have specific provisions addressing consumer protection issues that cover EFT Systems. A Code of Good Practice proposed by the Office of Fair Trading (established under the Restrictive Trade Practices Act, 1977) specifically covers issues of consumer concern in card and EFT transactions. An extract of this code is in **Annexure 3**.

- 3.2.13. The consumer movement in India has gained momentum after the enactment of the Consumer Protection Act, 1986. "Banking services" have been brought within the purview of the Consumer Protection Act<sup>1</sup>. The definition of "unfair trade practice" in the Consumer Protection Act is comprehensive enough to ensure complete and true disclosures about pricing, quality, standard etc. of services<sup>2</sup>. This Act, however, as it stands today, does not cover within its purview the problem of "unconscionable" or "unfair terms" in contract. It may be observed that annulment of any term of contract needs sanction of law. In England, the Unfair Contract Terms Act, 1977 was enacted to render unfair terms in a contract as well as in noncontractual notices unenforceable, if such term or notice restricts liability in contract or torts. This Act is however, related more to the "exclusion of liability" clauses in contracts or noncontractual notices<sup>3</sup>. We do not have any corresponding law in India. The Courts in India, however, have by applying the **doctrine of unconscionable bargain** sought to protect a weaker party in a bargain against unfair terms, if such terms could be regarded as **opposed to public policy** or obtained by **undue influence**<sup>4</sup>. The Committee understands that a Bill is presently pending in the Parliament for amending the Consumer Protection Act. This Bill proposes to give more teeth to the Consumer Protection Agencies in regard to unfair terms in a contract.
- 3.2.14. The consumer protection issue, so far as bank customers are concerned, is, to some extent addressed by the BR Act also. Most of the regulatory powers of the Reserve Bank under the BR Act are aimed at protection of depositors. In particular, Section 35A enables the Reserve Bank, when it is satisfied in public interest or in the interest of banking policy or to secure the interest of

---

<sup>1</sup> Section 2(1)(o), Consumer Protection Act 1986.

<sup>2</sup> Section 2(1)(r), Consumer Protection Act 1986.

<sup>3</sup> Chitty, *Contracts, Sweet & Maxwell*, 25th Edn. London, (1983) Para 910 etc.

<sup>4</sup> *Delhi Transport Corporations V. DTC Majdoor Congress*, AIR 1991 SC 101; *Central Inland Water Transport Corpn* AIR 1986 SC 1571.

depositors, to give any direction to banking companies. Reserve Bank is empowered to pursue any policy in the interest of the banking system or in the interest of monetary stability or sound economic growth and specify it from time to time as banking policy<sup>1</sup>. Many issues covered by the Consumer Credit Act of 1974 in the U.K., could be effectively dealt with here in terms of Sections 21 and 35A of the BR Act. As we have seen earlier, EFT is basically a funds transfer or "remittance", which by virtue of Section 6(1) of the BR Act, banks are empowered to undertake. Therefore, there should not be much doubt about the Reserve Bank's regulatory powers under the BR Act extending to consumer protection issues in EFT, like reasonableness of terms of services, pricing, disclosure norms, transparency in operations, etc.

- 3.2.15. For the purpose of Consumer Protection Act, EFT may have to be regarded as a **banking service**. Recently, the Reserve Bank has taken measures to ensure better customer service through expeditious redressal of customer grievances by the Banking Ombudsman Scheme, 1995. The Reserve Bank would therefore, have to take a decision whether or not, EFT related customer services should be covered by the Banking Ombudsman Scheme.

## THE COMPETITION ISSUES

- 3.2.16. The question here is, whether growth of separate EFT Systems (multiple systems) is essential and if so, whether these should be allowed to grow by bringing them under common regulations. Under the existing laws, there is no prohibition for such separate/multiple systems being set up by different groups of banks and financial institutions. However, the settlement arising thereunder would have to be under the aegis of the Reserve Bank. Since larger issues of policy as well as the compatibility of the multiple systems are involved and it is also not clear whether this forms part of the terms of reference made to this Committee, the Committee does not consider itself competent to offer any views in the matter. However, in case the Reserve Bank considers it desirable to encourage multiple systems subject to its Regulations, an amendment to the RBI Act would be necessary.

## TRANSACTIONAL ISSUES

- 3.2.17. Important transactional issues have been listed in para 2.22. Before analysing

---

<sup>1</sup> Section 5(ca) of the BR Act 1949.



the existing provisions of law having a bearing on these issues, two incidental questions need to be reviewed. These are:

1. Can the banks in India undertake/provide EFT services of all types?
2. What is the legal relation between a bank and its customer and bank and third parties in regard to EFT services provided by the bank?

### **Commercial banks' power to transact EFT business**

3.2.18. EFT, as prevalent in other countries is basically an additional payment or fund transfer mechanism through the banking system. In India, under Section 6(1) of the BR Act, business which the banking companies can undertake includes "collecting and transmitting of money and securities". This expression should cover every type of EFT operations.

3.2.19. The Income-Tax Act, 1961, however, will have some bearing on the funds transfer through an EFT System. Section 40A of this Act, dealing with deductible expenses, restricts the benefit only if the payment is made, where it exceeds Rs. 10,000/-, by a crossed cheque or a crossed bank draft. Similarly, Chapter XX-A dealing with acquisition of immovable properties require payments in excess of specified limits to be made only by crossed cheque or crossed bank draft. Chapter XX-B (from Section 269SS to Section 269TT), dealing with "mode of acceptance, payment or repayment" in certain cases, requires payment in excess of Rs. 20,000 to be made only by a cheque crossed "A/c. Payee" or a draft crossed "A/c. Payee". The object of these provisions of the Income Tax Act is to counteract evasion of tax by requiring that payment is to be made only to an identified account in the banking system. In an EFT, unless restricted by statute or regulation, funds can be transferred by anybody to anybody otherwise than from and to an identified bank account. But normally, in most of the EFT Systems operated in other countries, the originator is required to indicate an identified account from which funds are to be transferred to an identified account of the beneficiary. If the EFT is restricted to funds transfer from a designated account to a designated account within the banking system, that would, by itself, serve the same purpose for which requirement of crossed cheque or "A/c. Payee" cheque is stipulated under the Income-Tax Act. In the light of this, whether any change or clarification to the existing provisions of the Income-Tax Act is required needs to be considered.

## **Banker-Customer relation - General**

- 3.2.20. As in many other countries, the banker-customer relation in India, by and large, is contractual. In some cases, the rights and obligations are specifically defined by special laws in regard to particular services<sup>1</sup>. The contract can be express and in default, courts have been applying the theory of implied contract between banks and their customers. The implied contract covers rights and obligations in regard to operations of customer's accounts, maintenance of confidentiality of the affairs of the customer's account and the general duty of care in regard to the services.

## **Banker-customer relation in EFT**

- 3.2.21. The nature of contractual relation between banks and their customers differs depending upon the particular services provided by the banks. When a bank extends to a customer an EFT facility for transfer of funds from his account, a relation of principal and agent would come into existence between the bank and its customer. Funds remittance and payment on behalf of customers is basically an agency function. Depending on the funds availability arrangement made between a bank and its customer, EFT may result, especially in card based transactions, in credit being extended to the customer. In that case, a creditor debtor relation may also ensue between the bank and the customer.
- 3.2.22. In an EFT, the bank may have to execute the customer's payment instruction through another bank and in some cases an intermediary bank may also come into the picture. Would the intermediary bank and the bank that acts as beneficiary's bank become a substituted agent? This would be significant from the point of view of determining the rights and obligations by default rule. It would appear that if the banker-customer contract does not expressly provides otherwise, there is every possibility of an intermediary and beneficiary bank being regarded as a substituted agent of the customer. This would of course, depend on the customer's knowledge of engagement by his bank of another bank and the terms of customer agreement<sup>2</sup>. If the transaction results in a substituted agency, then in law a direct privity between the customer and the

---

<sup>1</sup> For example, opening and maintenance of account for disbursement of Government pension have separate rules.

<sup>2</sup> *Punjab National Bank V. Ishwarbai Lalbai Patel* AIR 1971 Bom.348.

intermediary or as the case may be, the beneficiary's bank would come into existence. The question, who should bear the loss on account of insolvency or suspension of payment, before the beneficiary's account is credited by the beneficiary's bank or the intermediary bank in such cases revolves on the incidence of substituted agency<sup>1</sup>. The customer cannot make his bank liable for the loss in such cases.

- 3.2.23. A further question which would be of considerable significance is about the status of the beneficiary's bank and the relation between the beneficiary and the beneficiary's bank in relation to the EFT transaction. When a beneficiary's bank executes a payment order received by it from another bank, it credits the beneficiary's account. Does the bank in such case act as an agent of beneficiary? If so, it would be only a receiving hand<sup>2</sup>. The bank, however, assumes an obligation to the sending bank by committing itself to the payment order at the instance of the sending bank. It would appear that the mechanism of execution of payment order is by substitution of the obligation of the sender by an obligation of the beneficiary's bank<sup>3</sup>. In that case, it would be more appropriate to regard the beneficiary's bank as acting as an agent of the sending bank rather than its own customer. This position, however, will have a direct bearing on the bank's right to recover money from the beneficiary by reversing the credit given to his account, if there was an error in crediting his account. The law relating to recovery of payments made under mistake is contained in Section 72 of the Indian Contract Act. The Supreme Court has held that when the bank is acting only as an agent of its customer in receiving funds to the credit of his account, it will not have any right to unilaterally correct an error in the account without the consent of the customer<sup>4</sup>. On the other hand, if the bank acted as an agent of the person who made the payment, it will have every right available under Section 72 for recovery of payment made under mistake. The existing provisions of Contract Act, however, do not provide a clear and unambiguous answer about whether the beneficiary's bank acts as an agent of the beneficiary in regard to an EFT.

---

<sup>1</sup> For the incidence of substituted agency, see Sections 194 and 195 of the Indian Contract Act 1872.

<sup>2</sup> See Pagets 'Law of Banking' Tenth Edn. Butterworths, (1989) Page 415.

<sup>3</sup> Edward L Rubin & Robert Cooter, *The Payment System, American Casebook Series*, WEST PUBLISHING COMPANY, Minnesota (1989) Page 736-741.

<sup>4</sup> *Jammu and Kashmir Bank V. Attar-Ul-Nisa* (1967) 37 Comp Cas 62.

## FINALITY OF PAYMENT

- 3.2.24. Payment in law, is the discharge or satisfaction of an obligation. When can a payment be considered to have been made and what constitutes the payment are delicate issues. Payment by cash does not require acceptance by the payee<sup>1</sup>. All other methods of payment involve an element of acceptance by the payee. In other words, the method of payment is a matter of agreement between the parties. Law, however, provides the default rule. For example, in the case of negotiable instruments, Section 85 of the Negotiable Instruments Act provides discharge to the bank when it pays in due course. Section 128 similarly provides the default rule in regard to payment of a crossed cheque.
- 3.2.25. A distinguishing feature of a cheque is that it needs to be presented by the payee to the paying banker. Presentment of a cheque, especially when the cheque is paid in clearing, cannot obviously take place without the express or implied consent of the beneficiary. Based on these default rules, courts have held that payment of a cheque is conditional when the cheque is delivered<sup>2</sup>. Payment is not deemed to be made unless the cheque is honoured. But once the cheque is honoured, the payment relates back to the date of delivery of the cheque to the beneficiary<sup>3</sup>. Even in the case of a post-dated cheque, the payment time, when the cheque is eventually honoured, would be the earliest point of time when the cheque could have been encashed, irrespective of the actual date of payment<sup>4</sup>.
- 3.2.26. Unlike a cheque, in an EFT, funds are credited to the account of a beneficiary without an apparent consent of the beneficiary. By banking practice, it can be safely assumed that bankers have the implied authority of the customers to receive payments to the credit of the customer. Credit to an account in any case is a tender of payment. Section 38 of the Contract Act also gives some clue about the default rule in law in regard to tender of a payment. As between the customer who initiates an EFT and the beneficiary of the EFT, the credit to the latter's bank account can be regarded as discharging such customer's obligation if the conditions stated in that section are complied with. To give a valid discharge, Section 38 requires a tender to be unconditional and for the full

---

<sup>1</sup> See, Paragraph 2.1 *ibid*.

<sup>2</sup> *A.R. Krishnaswamy Iyer V. M.N.Ramakrishna* (1945) 15 Comp Cas 134.

<sup>3</sup> *Jiwanlal Acharya V. Rameshwarlal Agarwalla* AIR 1967 SC 1118.

<sup>4</sup> *Anilkumar Sawhany V Gulshan Rai* (1994) 79 Comp. Cas. 150 (SC).

amount of the obligation. A tender of part payment does not qualify for discharge under Section 38. So is the case if the tender is made before the due date<sup>1</sup>. Section 38, however, does not provide an answer to the question whether credit to the account, in order to amount to a valid discharge needs to be advised to the beneficiary. This Section may not also be useful in deciding the default rule about part payment or payment before due date.

- 3.2.27. The Court of Appeal in England had an occasion to consider the question regarding payment by card. It was held that there was no general principle of law that, whenever a method of payment was adopted which involved a risk of non-payment by a third party there was a presumption that the acceptance of payment through the third party was conditional on the third party making the payment. Depending on the contractual arrangement in a credit card scheme, a card holder would be liable to pay to the card issuing company, whether or not, that company had paid to the supplier. Payment by credit card in such an event was an absolute, not a conditional discharge of the buyer's liability and the card holder's obligations to the supplier were absolutely discharged by the supplier accepting the voucher signed by the card holder. Thus, if the credit issuing company goes into liquidation before making payment to the supplier, the supplier had no remedy against the card holder<sup>2</sup>.
- 3.2.28. The above analysis of the existing law in India shows that the question, as to at what point of time a payment can be deemed to have been made in an EFT, is not answered by the existing provisions of law. Unless defined by a rule of law or by contract between the parties the following interpretations are possible :
- Payment is made when the beneficiary is advised of the credit from his bank. (receipt of credit advice by the beneficiary).
  - Payment is made when the beneficiary's bank despatches credit advice to the beneficiary.
  - Payment is made when the beneficiary's bank credits the beneficiary's account.

---

<sup>1</sup> *E Shahuq Molla V Abdul Bari Haldar* (1904) 31 Cal 183.

<sup>2</sup> *Re Charge Card Services Ltd.* (1988) 3 All ER 702.

- Payment is made when the beneficiary's bank receives the payment order for credit to the beneficiary's account.

- 3.2.29. Which of the above interpretation would apply as a default rule depends on how a funds transfer is to be construed in law. Is it an assignment of funds? The question would then be at what point of time the title to the funds changes or gets transferred from the originator to the beneficiary.
- 3.2.30. As with other payment systems, the EFT payment is a transfer of funds from the payer's account at his bank and a corresponding credit in the payee's account at the beneficiary's bank. There could, however, be a time gap between the point of time when the originator's account is debited and the point of time when the beneficiary's account is credited. Could this give rise to a **constructive trust** between the originator and his bank? Or alternatively, if the irrevocability rule is applied at the stage of receipt of the payment instruction by the originator's bank, can this be regarded as an assignment of a debt? (In regard to customer's deposit accounts, the banker customer relation is that of debtor and creditor). In such a situation, if the payment instruction is regarded as equitable assignment, obviously all the conditions of a valid assignment referred to in Section 131 of the Transfer of Property Act should apply.
- 3.2.31. The existing law, does not provide any satisfactory clarification to the exact nature of a funds transfer instruction and the exact point of time of applicability or nature of **default rule of payment**. It would, therefore, leave considerable uncertainty, unless this aspect of the transaction is specifically covered by express agreement between the parties or through a separate provision of law on the lines of Section 85 of the Negotiable Instruments Act. In the U.K., EFT is not treated as an assignment or trust. It is simply treated as a matter of agency contract. Even in the U.S. where the finality principles are defined by statute, an EFT is not treated as arising under an assignment or trust. The basic principles of agency are applied in the statute, to define the principles of finality.
- 3.2.32. In the Indian context, at this stage, having regard to the present status of technology, the question about rule of finality needs to be considered in the light of the present banking practice, risk to an originator and the beneficiary as also compatibility with the underlying technology. Later on, as technology progresses, the question may be reviewed to define by statute the synchronizing

point of finality with that of the discharge of the underlying obligation.

## **IRREVOCABILITY - FINALITY OF PAYMENT ORDER**

3.2.33. Generally, the issue of irrevocability refers to the point of time upto which a payment instruction could be changed or cancelled by the issuer. In the case of payment by cheque, the implied contract between the banker and customer obliges a bank to honour any stop payment order received from the customer, until a cheque is actually paid. Thus in the case of cheque, finality of payment and irrevocability are one and the same. This may not be the case in EFT. In the absence of an express contract, the default principle of law that would appear to apply is the **law of estoppel**. Under this principle, if the sending banker has altered his position (by executing the payment order), on the basis of the customer's payment instruction, it will not be open to the customer to bind the bank with any cancellation or any revocation even though at the time of such cancellation or revocation, the beneficiary's account may not have been actually credited.

3.2.34. Different principles are applied abroad for determining the irrevocability rules:

- **A payment order becomes irrevocable once it is issued by the originator.**
- **Payment order becomes irrevocable when the sending bank issues it or executes it.**
- **Payment order becomes irrevocable when the beneficiary bank receives it.**
- **Payment order becomes irrevocable when the beneficiary bank credits the beneficiary's account with the amount of the payment order.**
- **Payment order becomes irrevocable when the beneficiary's bank commits itself irrevocably by issue of advice of credit to the beneficiary.**

Which of the above rules should be adopted would depend largely on system compatibility and considerations of fairness as also the need for making EFT a user friendly system.

## AUTHENTICATION OF PAPERLESS PAYMENT ORDER

- 3.2.35. In the traditional paper based payment system, the authority of a bank to debit its customer's account for any amount paid by it to the customer or on behalf of the customer, is based either on express or implied contract. The courts have also recognised the authority of the bank to debit the customer's account for the amount of cheques lawfully paid by it and to recover the amount from the customer<sup>1</sup>. A payment is authorised for this purpose, if there is a mandate. For all practical purposes, a mandate means the signature or some way of authentication by the customer. There is a plethora of decided cases establishing the position that if a banker pays a cheque in which the drawer's signature is forged, forgery being nullity, the banker cannot debit the customer's account as in such cases, there is no mandate<sup>2</sup>.
- 3.2.36. Verification of authenticity in relation to paper based payment is verification of customer's signature. When the instruction becomes paperless, the question that would arise is when can a banker bind the customer with the payments made electronically to him or on his behalf. The signature is replaced by what is known as **security procedure**. Certain electronic devices like encryption, identification numbers or other procedures like call back are established, to determine/verify the authenticity of the instructions received by the bank purporting to be that of the customer. The existing legal provisions in India do not have any specific provision either permitting or prohibiting authentication procedure otherwise than by signature. This, therefore, can be established by a contract between the parties. Our study of the legal framework in other countries shows that while in the United States certain specific legal provisions are made through statutes<sup>3</sup> and administrative regulations, in other countries this is left to be determined by contract. But the important point which is established either by statute or by decided cases<sup>4</sup> is that the authentication procedure, if established at the instance of the bank should be **commercially reasonable**.

---

<sup>1</sup> *State Bank of India V. Vathi Samba Murthy* AIR 1988 Orissa 50; *Bank of Maharashtra V. United Construction Co.* AIR 1985 Bom. 432.

<sup>2</sup> *Canara Bank V. Canara Sales Corporation* AIR 1987 SC 1603.

<sup>3</sup> See Article 4A, Section 202 of Uniform Commercial Code. Also see Section 210.27 of Regulation 'J' Part B 12 CFR 210

<sup>4</sup> *Walker V. Texas Commercial Bank* NA 635 F. Supp 678; *Gatoil Inc. V Forest Hill State Bank* 1 UCC Rep. Serv.2d 171.



3.2.37. The concept of "commercially reasonable security procedure", has developed considerably both in English Law and American jurisprudence<sup>1</sup>. This question is treated as a question of law. This raises the question about the procedure to be recognised for establishing the security procedure for verification of authentication of payment orders. Further, even after establishing the security procedure, there are issues like **when and under what circumstances and to what extent the customer is not liable to pay to the bank even if the bank had executed payment order in good faith complying with the security procedure**. Generally, the considerations like **customer protection and level of technology** have determined the rules in this regard. In India, since this procedure is yet to take a shape, the question of any rule having been developed in this regard does not arise. The only question therefore, to be considered is whether the rules regarding security procedure and the liability for unauthorised payment should be defined and provided for by law or be left to be decided by contract between parties.

## SECURITY OF SECURITY PROCEDURE

3.2.38. An issue closely connected with authentication is regarding confidentiality and safety of the system. Security procedure established by agreement between the parties needs to be kept secured. Any unauthorised access to security procedure by a third party, popularly known as **interloper fraud**, can result in EFT being executed by the bank without actual authority although the payment instruction may comply with the security procedure. Who should be responsible for maintaining confidentiality of the security procedure? Whether a customer is responsible or not for third party frauds? These are matters which are normally determined by contracts. In the United States, however, these are provided by statute<sup>2</sup>.

3.2.39. The design of the computer to computer transmission system and the automated data processing assumes significance in considering issues of interloper frauds and banker's responsibility of maintaining secrecy of the customer's data. It is in this context that the UNCITRAL Legal Guide on Electronic Funds Transfers, pointed out that banks may have to assume a broader duty to establish a

---

<sup>1</sup> See generally, Jack Committee Report Page 82-87; Also, Official Commentary on UCC Article 4A-202.

<sup>2</sup> Electronic Funds Transfer Act 1978. Section 909 limits consumer liability for unauthorised transfers and Section 910 defines the liability of Financial Institutions.

security system for the transmission of funds transfer instructions and their storage which limits the possibility of such access.

- 3.2.40. In the case of cheques, courts have held that the implied contract between the bank and customer obliges the customer to refrain from drawing a cheque in such a manner as may facilitate fraud or forgery and there is a duty to inform the bank of any forgery of a cheque purportedly drawn on the account as soon as the customer becomes aware of it.<sup>1</sup>
- 3.2.41. Contributory negligence, except in the case of fraud, prevents a bank customer from claiming damages against the bank for third party fraud. **Operational security** becomes more relevant in EFT. Banks in England have generally excluded liability for third party frauds until notification by the card holder of the loss of the card or the secrecy of personalised security procedure.

## ERRORS AND SYSTEM MAL-FUNCTIONING

- 3.2.42. Unlike in the paper based payment system, the paperless transfer is prone to errors of different kinds. The UNCITRAL guide on Electronic Funds Transfer lists the following 4 circumstances in which an error may affect the electronic funds transfer.
- (1) Non-standardisation of message format between the various electronic fund transfer systems resulting in re-keying of messages.
  - (2) Re-creation of messages
  - (3) Non-standardisation of procedures particularly in relation to international transfers.
  - (4) Equipments failure or software error.
- 3.2.43. Our study of the systems in other countries indicate that loss arising on account of errors may be different from loss arising on account of negligence though at times negligence may lead to error. The rule for allocation of loss

---

<sup>1</sup> *London Joint Stock Bank Ltd. V. Macmillan* (1918) AC 777. For customer's duty to bank, see generally *Paget's Law of Banking* (Tenth Edition) Butterworths, London, Page 159-170.

arising on account of errors are generally based on the principles of Contract and Torts.

- 3.2.44. If the chain of legal relation between the bank and the customer and other participants in the system are based on the principles of agency, the existing provisions of agency law in India are sufficient to regulate allocation of loss arising on account of errors. Generally, if the loss can be attributed to the conduct of a party to the transaction, that party becomes liable for it. Where neither party is directly liable under the principle of "**party at fault**", the equity rule provides that party whose conduct lead to the fraud to take place or caused an error to take place, must bear the loss. Consumer protection considerations in the United States have driven statutory rules for limiting the liability of consumers in EFT to specified monetary limits.
- 3.2.45. In the case of cheques, the problem is specifically dealt with in the Negotiable Instruments Act. Sections 85 and 128 read with Section 10 of this Act give statutory protection to a paying banker in regard to loss by interloper fraud subject to the conditions that the payment must have been made in good faith and in due course etc. Similarly, Section 131 protects a collecting banker. Although by analogy, these provisions seem capable of providing useful tests for determining liabilities in an EFT context, the concept of collecting banker and paying banker does not appear to be strictly applicable in EFT.
- 3.2.46. In the United States and some European countries, negligence invites astronomical measure of damages. The existing law and the extent to which damages are awarded by courts for breach of contract and liability in torts, is very conservative in India. Exemplary damages in contract are exceptions in India. Even in the actions based on Tort, the quantum of compensation awarded by courts is not something for which a new rule would be required to be made in regard to EFTs. The parties to the contract have a right to quantify the extent of loss at the time they make the contract. If the parties quantify the loss (liquidated damages) in the contract, courts cannot award compensation for breach of contract for an amount greater than the amount quantified<sup>1</sup>. If the parties have not quantified the loss by contract, the compensation for breach of contract would be decided in accordance with the principles laid down in section 73 of the Contract Act.

---

<sup>1</sup> Section 74 of the Contract Act 1872 provides for "reasonable compensation not exceeding the amount named in the contract" see, *Fateh Chand V. Balkishan Das* AIR 1963 SC 1405.

3.2.47. Section 73 entitles a party who suffers a breach of contract, to receive "compensation for any loss or damage caused to him thereby, which naturally arose in the usual course of things from such breach, **or which the parties knew when they made the contract to be likely to result from the breach of it**". This provision ordinarily restricts damages to actual loss. However, compensation for **consequential loss** is also payable if notice of **special circumstances** giving rise to consequential damages was given at the time of the contract. Having regard to the uncertainty about the extent of liability for consequential damages, the question that needs to be considered is whether special rules are required for limiting the liability of the banks and customers involved in EFT.

## INCIDENCE OF INSOLVENCY

3.2.48. EFT, as we have noticed earlier, is a method or means. But the incidence of insolvency of any bank involved in an EFT could be substantially different from those arising in a paper based payment. In EFT, there could be a float between the point of time a payment order is issued by a customer to the point of time when payment is complete. The issue that needs to be focussed here is, if payment is suspended by any bank participating in the EFT before settling its payment obligation, on whom does the loss fall? Should the beneficiary bear the loss? Should the initiator of the payment order bear the loss? Or, should the sending bank or beneficiary's bank bear the loss?

3.2.49. Under the English Law, on which most of Indian banking law principles are based, the following position is stated:

- If a bank having given a commitment to pay becomes insolvent before discharging its obligations, the bank to whom that commitment was given has no claim to any funds. It will only have a mere claim in the insolvency in competition with other creditors, while the creditor customer for whom the commitment constituted conditional payment has a right to demand payment from the debtor customer<sup>1</sup>.
- Where the receiving bank becomes insolvent after the payee's account has been credited, the creditor customer has to bear the loss<sup>2</sup>.

---

<sup>1</sup> See, *W J Alan & Co. Ltd. V. El Nasr Export and Import Co.* (1971) 1 Lloyd's Rep 401.

<sup>2</sup> See, *Royal Products Ltd. V. Midland Bank Ltd.* (1981) 2 Lloyd's Rep 194.

- If a bank goes into liquidation before it has collected a cheque, it has no right to borrow the sum in question back from its customer<sup>1</sup>.
- A credit transfer, once initiated, may be reversed by the paying bank up to midnight on the day of the transfer (but not later), even though the credit has not been communicated to the beneficiary. There is no reason to distinguish an in-house transfer from an external payment in this respect<sup>2</sup>.

3.2.50. The Companies Act or the BR Act in India, do not provide any satisfactory solution. In practice, by operation of Clearing House Rules, netting of transactions (clearing inward and clearing outward) on the date of suspension of payment by a bank is resorted to and the surplus, if any, is treated as money held in trust in the hands of the liquidator. These provisions also do not provide a satisfactory solution.

3.2.51. In the case of EFT, apart from the nature of legal relationship of the parties, the point of time at which the customer's account is debited and the point of time at which settlement between banks take place may have significance for considering the incidence of insolvency. The following options could be considered:

- Establishment of a contingency fund.
- Distribution of loss among the participants.
- Provision for collateral.
- Provision for insurance.

3.2.52. A predetermined fee towards the corpus of the contingency fund could be raised from the participating members. This, however, would not be possible unless, the existing provisions of the Insurance Act is amended. Alternatively, sharing of loss may be pursued on some principles like the size of the participants or volume of transaction for distribution of loss. The other alternative is to require each participant to keep collateral. This would involve

---

<sup>1</sup> See *Re Farrow's Bank Ltd.* (1923) ch 41.

<sup>2</sup> See *Momm V. Barclays Bank International Ltd.* (1977) QB 790.

policy consideration as it may immobilise resources of banks. Which of these alternatives may have to be pursued, will ultimately have a bearing on a suitable clearing and settlement procedure to be adopted.

- 3.2.53. In considering any of the above options, security and integrity of the system, accountability of the participants and the need for fairness have to be considered.

## **PART - III**

### **OTHER LEGAL ISSUES IN EFT**

#### **CHEQUE TRUNCATION**

- 3.3.1. Although not strictly an EFT, the modern method of truncating the physical movement of cheques by substituting it with electronic transmission of the image of the cheque or essential data of the cheque, has close resemblance to EFT. There are basically three issues which need to be considered:
1. Does our existing law permit cheque truncation?
  2. Does the advantage of cheque truncation outweigh the accompanying risk involved in the process?
  3. What changes are called for in law, at this stage of development of technology in India, for following cheque truncation system?

#### **Legal requirement of presentment**

- 3.3.2. Under the Negotiable Instruments Act, 1881 (N.I. Act) cheques have to be presented for payment to the bank on which these are drawn. Without such presentment, no cause of action arises against the drawer<sup>1</sup>. Section 64 of that Act declares that in default of presentment of a cheque to the drawee for payment, other parties to the cheque are not liable to the holder. A collecting bank, by implied contract assumes an obligation to present the cheque at the

---

<sup>1</sup> Section 64 and 84 of the Negotiable Instruments Act 1881.

drawee bank and that obligation is discharged only when the cheque is so presented<sup>1</sup>. The fact that presentment for this purpose means physical presentment is clear from the following addition made to section 64 by an amendment in 1885:

**"Where authorized by agreement or usage, a presentment through the post office by means of a registered letter is sufficient"**

By banking practice, both in India and in England, it is open to banks to agree to presentment at any place other than the branch, such as at a clearing house<sup>2</sup>.

- 3.3.3. The implication of the definition of payment in due course<sup>3</sup> may make it difficult for bankers to establish a truncation system by agreement between themselves. The statutory protection available under Section 85 of the N.I. Act may not be available in cases where payments are made under cheque truncation system. In view of the emphasis on the place where the cheque is made payable<sup>4</sup>, the bankers may not get statutory protection even in intra-bank truncation.
- 3.3.4. In the U.S.A. and the U.K., by law or banking practice, paying banks are required to deliver to the drawers paid cheques with due marking of payment. Such paid cheques are primary evidence of payment. But in India, under the Banking Companies (Period of Preservation of Records) Rules, 1985, paid cheques are required to be preserved by paying banker for a period of eight years. Section 45Z of the BR Act however permits a bank to retain only a copy of such cheque if the customer requires return of the paid cheques.
- 3.3.5. The Jack Committee in its report, recommended amendment to Section 45 of the U.K. Bills of Exchange Act to allow the Electronic presentation of data captured from a cheque and also amendment of Section 3 of Cheques Act, 1957 to accord a photocopy or some equivalent reproduction in legible form, of a

---

<sup>1</sup> *Barclays Bank Plc V. Bank of England* (1985) 1 A11 ER 385

<sup>2</sup> See, *Bhashyam & Adiga, the Negotiable Instruments Act, 15th Edn. Bharat Law House, New Delhi* (1990) Page 511.

<sup>3</sup> Section 10 of the NI Act requires payment in accordance with the apparent tenor of the instrument in good faith and without negligence.

<sup>4</sup> Section 72 of NI Act require a cheque to be presented at the bank upon which it is drawn.

cheque, suitably marked as paid and authenticated by the collecting banker, the status of evidence of the receipt by the payee of the sum payable by the cheque.

- 3.3.6. An important aspect that is noticed in comparative study of the progress achieved by banks in other countries in cheque truncation system is that the size of the country and the number of banks in the banking system are important. In the U. S., for example, in view of large number of banks functioning in the country, most of which have branches in particular States only, it was felt almost impossible to set up a communications network linking them altogether. Consequently, cheques continue to be physically moved in the U. S. In the U. K., on the other hand, due to the number of banks participating in the clearing system being limited and the size of the country also being relatively small, banks have been able to pursue the truncation system even without any change in the law.

## **Risk to the banks**

- 3.3.7. The right of the paying bank to require physical presentation and possession of the cheque is designed to provide it with an opportunity to examine the signature or other authentication of the cheque, to examine the "apparent tenor" for its accord with the formal requirements of law, to be sure that there is no material alteration and that a paid cheque is not presented a second time. In large measure the existing requirements are designed for the protection of the drawer.
- 3.3.8. If a customer claims that the payment by his bank against a cheque was without proper mandate, the paying bank can rebut his claim only by producing the paid cheque (in original), and showing that it had discharged its obligation under law by verifying the signature and apparent tenor and that the payment was in due course. In the absence of such proof, the paying banker is bound in law to recredit the amount. In the U. K., banks have tried to reduce the risk by obtaining customer consent agreements to enable them to waive physical presentment of cheques. Section 76 of the NI Act in India, which deals with waiver of presentment, specifically recognises the drawers right to waive presentment<sup>1</sup>.

---

<sup>1</sup> In *Sumitra Baluja V. Bharat Chemical Industries* (1983) 53 Comp. Cas. 561, the Delhi High Court analysed the implication of waiver by the drawer.



## **Changes in law**

- 3.3.9. The requirement of physical presentment is a legal requirement. But this is meant for the benefit of the drawer. Courts in India have held that an individual can waive his legal right if there is no public policy behind the right conferred by law. On this basis also it should be possible for banks in India, like the banks in the U. K., to introduce the cheque truncation process on the basis of customer agreements. But in the long term, unless the law is changed, the process of truncation of cheques may not make much headway. The definition of "presentment" in Section 64 of NI Act may have to be suitably amended to permit electronic presentment of essential data or image of the cheque. This, however, involves a greater probe into the status of technology at the branch level and the extent of dishonour of cheques for alteration/forgery, etc.

## **EVIDENCE AND BURDEN OF PROOF**

- 3.3.10. The fundamental difference between a paper based payment system and a paperless payment system is the absence of any written record of the transactions in the later case. Our study of other systems shows that the evidence law in regard to transactions effected or carried out on electronic medium have developed considerably in most of the countries where the use of electronic technology has attained sufficient maturity. There are basically two issues in regard to proof of EFT:
1. Should there not be a legal obligation on any service provider to issue a print out or written record on completion of an electronically completed transaction?
  2. Whether and to what extent computer printouts should be admissible evidence?
- 3.3.11. In the paperbased 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 (normally this is provided by way of automatic and mechanical print out of the transactions). When EFT is introduced in India, especially EFTPoS and other card based transactions like ATMs, a provision requiring service providers to ensure furnishing of authenticated records of transactions needs to be made. Rules of evidence in

regard to computer based transactions have already developed in the UK, both in civil and criminal proceedings. It is time that we address ourselves to those problems. This is however, an issue of general nature applicable to all computer based transactions. To examine the existing provisions of Evidence Act, generally in its applicability to all electronically concluded transactions and particularly the definition of "document", to see the extent to which records kept in electronic media are admissible evidence, is outside the purview of this Committee. The Committee, however, went into greater details about the need for amending the Bankers Books Evidence Act to take care of special problems that may arise after the introduction of EFT system.

- 3.3.12. The United Nations Commission on International Trade Law had made a survey which showed that in most countries records kept in computers can be used as evidence in case of litigation subject to the proponent of the record establishing certain facts about the record and the 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.
- 3.3.13. In the UK, Section 5 of the Civil Evidence Act, 1968, provides that subject to certain conditions, a statement contained in a document produced by computer will be admissible as evidence in civil proceedings. The Criminal Evidence Act, 1965 was amended by the Police and Criminal Evidence Act, 1984 to provide that a document produced by a computer print out will be admissible as evidence in any proceedings if it is shown that the statement is reasonably accurate and that the computer was working properly at the relevant time.
- 3.3.14. In India, although the Evidence Act which generally governs the proof in civil and criminal proceedings, has not yet adapted itself to the computer age, some headway is made in the Customs and Excise Laws. Records kept in disc, microfilm and other electronic memory systems are made admissible. The Customs and Central Excise Laws (Amendment) Act, 1988 which introduced new Sections, 138C in the Customs Act 1962 and 36B in the Central Excise and Salt Act, 1944, has provided a lead in this regard<sup>1</sup>.
- 3.3.15. The issues relating to amending the Bankers Books Evidence Act so as to make computer print outs used in banking transactions, replacing the traditional

---

<sup>1</sup> Extract of the relevant Section of this Act is in *Appendix F*.

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. The proposal made by the Reserve Bank for amending the Bankers Books Evidence Act is stated to be under consideration of the Government of India<sup>1</sup>.

- 3.3.16. As an alternative to the draft amendment suggested in terms of Appendix E to the Bankers' Books Evidence Act, an amendment on the lines of Appendix F can also be considered.

## **PRESERVATION OF RECORDS**

- 3.3.17. Books, accounts and other documents as well as instruments handled by banks, apart from their evidentiary value, have special significance from supervisory angle. The BR Act provides a specific provision enabling the Central Government to make Rules for the preservation of records<sup>2</sup>. Pursuant to this, the Banking Companies (Period of Preservation of Records) Rules, 1985 [BC(PPR) Rules] have been promulgated by the Central Government, prescribing the period for which banking companies are required to preserve specified ledgers, registers and other records. A period of 5 to 8 years is prescribed as a period for which specified records are to be preserved.
- 3.3.18. Of the various records listed in the BC(PPR) Rules, the entries pertaining to Drafts, TTs and Mail Transfer Registers, Remittance Registers, despatch and receipt advice of remittances could be of special significance to EFT<sup>3</sup>.
- 3.3.19. As part of the technological upgradation and also to relieve the banks of the problem of space in preserving the records, certain measures like preserving these records on micro-films and computer floppies were considered in the past. In the absence of amendment to the concept of "primary evidence" in the Evidence Act, the move has not made much progress. In fact, one of the reasons for promoting an amendment to the Bankers Books Evidence Act was to accord to the records maintained on micro-films and other electronic

---

<sup>1</sup> Text of the amendment suggested in this regard is in *Appendix E*.

<sup>2</sup> The Banking Regulation Act, 1949, Section 45Y.

<sup>3</sup> The banks are required to preserve for 8 years, applications and vouchers relating to DDs, TTs, MTs and despatch & receipt advices in regard to these. See, the Banking Companies (Period of Preservation of Records) Rules, 1985.

retrieval devices, the status of "**prima facie evidence**", (if not primary evidence). In the case of EFT, although initially the system may work as a hybrid system (partly paperbased and substantially paperless), eventually, the aim should be to develop a completely paperless Funds Transfer System. As discussed in Chapter II, the regulatory and supervisory concerns in EFT arise on account of the high potential of EFT abuses for money laundering, evasion of tax and other unlawful fund transfers. The need for preservation of records of transactions in the normal course would be more, especially when EFT is made completely paperless.

- 3.3.20. The preservation of records may also have significance in regard to litigation. Although the BC (PPR) Rules are not driven by considerations of period of limitation for enforcement of claims, banks may, in their own interest, have to preserve records consistent with the law of limitation and evidence to take care of future litigation.
- 3.3.21. The question of amending the existing Rules for preservation of records in relation to EFT needs to be considered as a matter of policy by the Reserve Bank having regard to the supervisory and regulatory requirements. There is no specific entry pertaining to EFT in the existing Rules. A specific entry, therefore, would have to be considered and a suitable period and the method of preservation, after considering the supervisory policy and technological aspects of preservation of records has to be decided.

## CONFIDENTIALITY AND DATA PROTECTION

- 3.3.22. In the absence of specific statutory provision, the law relating to banker's secrecy law in India has, by and large, followed the English decisions. The Court of Appeal decision in the *Tournier Case*<sup>1</sup> had established that the secrecy obligation of bankers is a legal obligation arising by implied contract. The following formulation by Bankes LJ in the that case is still considered as the most accurate proposition of law in regard to banker's secrecy obligation:

"In my opinion it is necessary, in a case like the present, to direct the jury what are the limits and what are the qualifications of the contractual duty of secrecy implied in the relation of banker and customer. There appears to be no

---

<sup>1</sup> *Tournier V. National Provincial and Union Bank of England* [1924] 1. KB. 461

authority on the point. On principle I think that the qualifications can be classified under four heads:

- (a) where disclosure is under compulsion by law;
- (b) where there is a duty to the public to disclose;
- (c) where the interests of the bank require disclosure;
- (d) where the disclosure is made by the express or implied consent of the customer."

3.3.23. EFT, as we have seen is a method of funds transfer through an electronic network within the banking system. The existing obligation of secrecy attached to the banker-customer relation, unless altered by express contract, would extend to EFT transactions undertaken by the bankers. Do the banks or customers need any special protection, apart from the general obligation already existing under the law?

3.3.24. The special concern of the banker's secrecy obligation in EFT would arise *inter alia*, on account of the following:

- (i) EFT will create new records of transactions;
- (ii) EFT will result in an increase in the amount of information available in new records;
- (iii) because these are electronically readable, records will be more easily accessible;
- (iv) more institutions might gain access to an individual's financial records; and
- (v) the place where a person operates a terminal will be precisely located.

3.3.25. A clear understanding of the risk involved in transmission of payment data through a communication network and keeping records of transactions in computers and other electronic devices is necessary. The possibility of unauthorised access by third parties, of the vital data, may depend on the

design of the network system, its dependence on general communication facility etc. While a dedicated communication network may be less prone to unauthorised access, it may be different if the design of the system depends on general telecommunication facility.

- 3.3.26. The Council of Europe had adopted in 1981, a convention for the protection of individuals with regard to automatic processing of personal data. The Data Protection Act, 1984 enacted in the U. K. was pursuant to this convention. This Act basically provides that **personal data must not be disclosed in any way incompatible with the purpose for which the data is held.**
- 3.3.27. The Saraf Committee made a reference to the Data Protection Act, 1984 in the U.K.<sup>1</sup>. This Act, as discussed below, is aimed at protection of personal data of individuals stored or processed on electronic media against unauthorised disclosure and unauthorised use. The Act establishes a system of Registration of **Data Users and Computer Bureaux** and prohibits holding by any person of personal data on electronic media unless he is registered under the Act. The Act also confers specific rights on individuals who are **Data subjects**. These rights include right of access to the data, compensation for inaccuracy in the data, compensation for loss on account of unauthorised disclosure, etc. The Act exempts holding and use of personal data by certain specific categories of data users like statutory authorities<sup>2</sup>.
- 3.3.28. An analysis of the U. K. Data Protection Act would show that this Act is not specifically aimed at electronic banking or EFT. As such, the Act is a general legislation initiated for the purpose of dealing with the potential unauthorised access or abuse of personal data by computer network providers and others. Electronic banking records of a bank's customers are personal data under the Data Protection Act, and customers are 'data subjects'. Bank customers are entitled to compensation for unauthorised access to data collected by banks. Thus, in addition to the Common Law liability, bankers also incur liability for non-consensual access to EFT data under the Data Protection Act but the Act provides two defences to the bankers. These are, that the financial institutions are not liable if access to computer information is by a person in the registered entry, or if they can prove that they have taken reasonable care to prevent unauthorised access and consequential loss. It would seem that banker's

---

<sup>1</sup> *The Report of the Committee on Technology Issues, Reserve Bank of India, Bombay, 1994 Para 2.20.*

<sup>2</sup> *An extract of the scope and rationale of the principles under this Act is in Annexure 6.*

liability will ultimately depend on the precaution taken to prevent non-consensual access.

- 3.3.29. Although, the principles provided in the Data Protection Act cannot be considered as a necessary concomitant to introduction of EFT, as a long term perspective, the question, whether a similar legal framework may have to be provided in India to cope up with the pressure on the banker's secrecy obligations due to increasing computerisation of banking business, needs to be considered.

## **DISPUTE RESOLUTION**

- 3.3.30. One of the important issues considered in most of the countries where EFT has been in operation, is the provision for a separate investigation and dispute resolution mechanism. This is felt necessary especially in regard to high value funds transfers. In the U. S., in regard to EFT of all types, specific statutory provisions are made to provide for an effective mechanism for investigation and resolution of disputes. This assumes special significance in India, as EFT transactions are highly technical and need a clear understanding of the concepts and technological aspects in investigating and resolving disputes.
- 3.3.31. Under the existing framework of Indian law, the bank customers have the following remedies:
- (1) to approach civil courts by way of suit for damages, injunction or specific performance.
  - (2) to approach Consumer Foras established under the Consumer Protection Act.
  - (3) to avail Customer Grievances Redressal Machinery provided within the banking system. (Such as complaint to Banking Ombudsman, complaint to Reserve Bank's Grievance Cell, etc.).
- 3.3.32. Civil courts are bound by the technical rules of evidence and procedure and the process of dispute resolution by resort to litigation in courts could be extremely expensive and time consuming. Given the existing rules of evidence law and the general delay in the judicial system with hierarchical appeal systems, resolution of grievances through courts may not be suited to EFT disputes.

- 3.3.33. Consumer Foras established under the Consumer Protection Act 1986 are gaining popularity among the bank customers. All banking services come within the purview of Consumer Foras. EFT being a "service" would also come within the purview of the jurisdiction of Consumer Foras. Consumer Foras are designed to resolve disputes of general nature. These can not be considered as equipped with the expertise to handle and resolve disputes involving highly technical aspects. In fact, the National Consumer Disputes Redressal Commission has repeatedly held that even in disputes of general nature, if the case involves complicated questions of law or elaborate evidence, the consumer foras should decline to exercise jurisdiction<sup>1</sup>. In this view of the matter, to make EFT more user friendly, the question, whether a separate system of dispute resolution needs to be provided requires to be considered.
- 3.3.34. In the U.K., for resolving customer disputes in banking services, a system of Ombudsman has been introduced. There are both voluntary and statutory models of separate Ombudsman system in the U.K. The statutory Ombudsman system is applicable to Building Societies which engage in retail deposit mobilisation and certain retail banking services including consumer credit. The voluntary system is operated by agreement between participating banks.
- 3.3.35. In India, until 1995, customer grievances were handled at the branch level, at the controlling office level and at the Head Office level of banks<sup>2</sup>. With a view to improve customer services, the Reserve Bank also had set up separate Customers Grievances Cell to coordinate redressal of customer grievances. As the perception of customer grievances system gained more importance, the Reserve Bank introduced in 1995 a system of Banking Ombudsman. The Banking Ombudsman Scheme, 1995 was introduced as a directive dated 14th June 1995, issued under section 35A of the BR Act. The Ombudsman appointed under this system can give relief against banks by directing the banks to carry out specific obligations undertaken by them in regard to banking services. He can also award compensation up to an amount of Rupees ten lakhs.
- 3.3.36. The existing system of Ombudsman for banking sector in India is a mixture of principles of conciliation, mediation and adjudication. The remedy through

---

<sup>1</sup> *M/s. Special Machines, Karnal V. Punjab National Bank*, [1991] 1 CPR 52; [1991] 1 CPJ78; *Tressa V. Motor Superior* [1991] 2 CPR 53.

<sup>2</sup> For customer grievance redressal systems in banks, generally see, "The Report of the Committee on Customer Services in Banks (Goiporia Committee Report) IBA, Bombay 1991.



Ombudsman is an additional remedy and not exclusive. The Ombudsman award becomes enforceable only if the complainant accepts it.

- 3.3.37. The question whether a separate system of arbitration or other form of adjudication of disputes between banks and their customers, arising under the EFT would be necessary, can be better considered when a clear idea about the type of disputes commonly raised and the number of such disputes are known. Resolution of disputes between bank customers and banks may have to be treated differently. A separate mechanism for the investigation and resolution of claims between banks or between a bank and Reserve Bank, however needs to be considered on a priority basis.

## **PREVENTION OF FRAUDS**

- 3.3.38. Fraud in an EFT involves an unauthorised instruction, alteration of the amount or alteration of the name of the beneficiary. In paragraph 3.2.42 to 3.2.47, the issues relating to allocation of loss arising on account of fraud, including interloper fraud, has been discussed. Prevention of fraud is a different issue. The former deals with the consequence where as the later with the cause. Allocation deals with the incidence of loss on the parties to an EFT when it is caused by fraud. Prevention is the elimination of the cause itself, by directing the incidence on the person who causes it. There are basically two issues here :

1. What should be the responsibility of the service providers and users in regard to design of the system?
2. Whether fraud in EFT should be made a punishable offence and if so what elements should constitute the offence?

## **Nature of the Problem**

- 3.3.39. Fraud is not unique only in EFT. Bank frauds involving paper based payment instruments in recent years, has been a matter of grave concern. But misuse of computers and other electronic devices through unauthorised access is not the problem of EFT only; rather, it is common to all computer based transactions. What makes such misuse or unauthorised access a matter of special significance for EFT, is the high potential and intensity, given the sums involved, especially in high value transfers, and the ease with which it can be perpetrated. To understand the problem, we may usefully turn to some of the usual sources of frauds in EFT, experienced in the countries where EFT has developed.

The common sources of EFT fraud inter alia, are :

1. Dishonest employees of customers.
2. Fraudulent use of customer activated terminals.
3. Dishonest bank employees.
4. Tapping telecommunication transmission.

3.3.40. All the above sources are existing in paper based funds transfer system also. Most of the bank frauds originate in customer's employees dishonestly drawing unauthorised cheques, altering cheques or collecting cheques. Similarly, in many cases of fraudulent withdrawals from customers' account, connivance of bank-employees is observed. Interception in postal transmission of cheques and other payment instruments and unauthorised collection by unscrupulous persons has become a menace in recent years. Despite these frauds continuing for decades in regard to paper based fund transfer instruments, no satisfactory legal solution has yet been found in any country.

### **Responsibility of system providers**

3.3.41. One way of minimising these frauds would be at the design stage of the system. Proper system of regulation and monitoring of the commissioning and operations of the systems and subjecting the service providers to adhere to certain internationally prevalent technical standards in the designs and use of the system, like dedicated communication systems instead of common telecommunications carriers, may help in minimising, if not completely eliminating, interloper frauds of **hacking and tapping**.

### **Criminal liability for Fraud and other computer crimes**

3.3.42. Fraud by itself is not an offence under the Indian Penal Code (IPC) and as such, "Fraud" is not defined in criminal law in India. However, certain acts when done "fraudulently", are made offences. "Mischiefs", "Theft", "Cheating" are some of the offences which have elements of fraud. But these offences require some additional ingredients, like "moving a movable property out of the possession of another" as in the case of "theft" (Section 378 of IPC);

"intentionally causing wrongful loss or destruction of property" as in the case of mischief (Section 435, IPC); and "dishonestly or fraudulently removing, concealing etc. of property" as in the case of "cheating" (Section 421, IPC) . In most of these cases the definition of offences are directed against **"property"**. An EFT being a message in electronic media may not fall within the description of "property". It also does not fall in the definition of "document" in regard to the category of **offences against documents**.

3.3.43. In the law of Torts, fraud means deceit. It requires intention to deceive and actual deceit. Indian Contract Act, 1872, defines fraud in relation to a contract as, commission of any of the specified acts with intent to deceive. The acts specified are, "a suggestion which is not true, made by a person who does not believe it to be true; the concealment of a fact; a promise made without any intention of performing it; any other act or omission as the law specifically declares to be fraudulent"<sup>1</sup>.

3.3.44. In a recent publication on computer crimes<sup>2</sup> the following acts are described as constituting Computer Crime :

- Unauthorised attempt to access, alter, add, delete or hide data.
- Unauthorised attempt to access, alter, add, delete or hide program or system.
- Stealing of data or programs in any manner.
- Unauthorised (physical and/or logical) entry into computer work environment.
- Change or alteration of the defined systems.

On the basis of the above description, computer crimes are classified into three broad categories :

- Data related crimes

---

<sup>1</sup> For full definition of "fraud", see the Indian Contract Act, 1872, Section 17.

<sup>2</sup> Rakesh M. Goyal & Manohar S. Pawar, *Computer Crimes-concept, Control And Prevention*, SCPL, Bombay [1994]

- Software related crimes
- Physical crimes

3.3.45. In EFT, it is the data related crimes which are the most common. And if that is so, the existing provisions of the IPC or the definition of 'fraud' in the law of Torts or Contract Act may not be helpful in fixing criminal liability as an effective way of preventing EFT frauds.

3.3.46. In the UK, computer crimes are dealt with under two recent enactments. The UK Counterfeiting Act of 1981, contains a special section defining forged "instrument" as including **"any disc, tape, sound track or other device on or in which information is recorded or stored by mechanical electronic or other means"**. All crimes against documents are thus extended to electronic data. Further, the U.K. Computer Misuse Act, 1990, for the first time defined three distinct computer crimes and provided for punishment varying from six months to five years imprisonment<sup>1</sup>. The offences defined under this Act are:

- (i) Unauthorised access to computer material
- (ii) Unauthorised access with intent to commit or facilitate commission of further offence.
- (iii) Unauthorised modification of computer material.

In all the above offences an element of "intent" is required.

3.3.47. The United States provides a much more comprehensive criminal law in regard to computer crimes. The Counterfeit Access Device and Computer Fraud and Abuse Act, 1984, is a complete code. But most of the offences under this Act are directed against computer systems operated for or on behalf of the Government.

3.3.48. The Committee understands that in the wake of increasing economic offences and bank frauds, the Government of India and the Reserve Bank are exploring possibility of a new criminal law to deal with these special crimes. Criminal jurisprudence, both substantive (elements of liability) as well as procedural

---

<sup>1</sup> An extract of the UK Computer Misuse Act, 1990 is in Annexure 7.

(investigation and prosecution) needs to be given a fresh look in the computer age. Since EFT frauds form a homogeneous subject to those offences and frauds, it may be more appropriately considered in such a legislation along with other computer frauds.

- 3.3.49. One possible way of defining the offence and fixing liability for EFT frauds could be to identify the specific acts like **issuing or causing to issue an unauthorised payment instruction, making or causing an unauthorised alteration in a payment order and stipulating a presumption that the person issuing or causing to issue such unauthorised payment instruction or a person making or causing to make an unauthorised alteration in a payment order, shall be presumed to have done so with a dishonest intention unless he proves otherwise.** This is shifting the burden of proof.
- 3.3.50. Traditionally, criminal liability required the proof of both **actus reus** (commission of an act prohibited by law) and **mens rea** (the mental culpability) and criminal jurisprudence rested on the principle that a man is presumed to be innocent until the prosecution proves his guilt beyond reasonable doubt. Instances of departure from these traditional concepts either by dispensing with requirement of mens rea or by shifting the burden of proof on the accused in areas where such departure is justified on larger social benefits, are quite large in what are today called statutory offences. But criminal law is normally a legal response to an existing or growing public wrong. Number of factors and statistics to justify departure from the normal rule would be required. In view of this, it may be too early for this Committee to recommend any specific definition of fraud as an offence or the method of imposing criminal liability on frauds in EFT. A new criminal law dealing with the computer crimes on the lines of the U.K. Computer Misuse Act 1990 may be a welcome move in the long term.

## **SETTLEMENT OF INTER-BANK PAYMENT OBLIGATION**

- 3.3.51. There are different methods in the banking system of each country for settlement of inter-bank payment obligations arising out of clearing of collection items. Two banks may bilaterally establish a correspondent arrangement in which case normally payment obligations are settled by appropriate book-keeping entries in the account maintained by one of them. Alternatively, two or more banks may maintain account with a third bank for settlement of payment obligation between them. In such cases, settlement for individual

items or batches of items are made by a debit and corresponding credit entry made in the respective accounts maintained with the third bank.

- 3.3.52. In most of the cases banks establish clearing houses which also serve as settlement agency. The amounts transferred to and received by each of the participating banks, at predetermined intervals, are totalled and settled by banks with a net debit position in favour of those with a net credit position. The concept of netting has several variations.
- 3.3.53. In most of the systems, the Central Bank or in the absence of the Central Bank, the biggest bank, functions as the settlement bank in the clearing system. The time gap between clearing and settlement is the zone of risk of failure of a bank to settle its position to which the entire banking system is exposed and which normally triggers the systemic risk. It is mainly for this reason apart from the reason of lending moral and credit support to the settlement system by virtue of its position, that a country's Central Banking authority is concerned with the efficient functioning of the settlement mechanism.
- 3.3.54. In an EFT environment, the following specific aspects need special mention:
1. The frequency with which the transactions are netted;
  2. The period of time after netting, within which settlement of net balance is made;
  3. Whether netting and settlement is by pairs of banks or for the clearing as a whole; and
  4. The means of settlement.
- 3.3.55. In an EFT credit transfer system, depending on the settlement system, the beneficiary's bank may assume an irrevocable obligation to the beneficiary by crediting the amount to his account before it has received value (before inter-bank settlement takes place). It may so happen that since the creation of a debit balance arises out of the sending and receiving of payment instructions, no bank in the network may know until the end of the day, whether it will finish the day with a net debit or credit balance. In general, EFT in low value's are settled in batches on a net or net-net basis, while high value EFTs are settled individually on gross basis. Exceptions to this are CHIPS system in U. S. and CHAPS system in the U. K.

- 3.3.56. The UNCITRAL Legal Guide lists the following means available for reducing systemic risk:
- Limiting the participation in net or net-net settlement networks.
  - Prescribing intra-day bilateral net debit limits or net-credit limits.
  - Minimising the period of execution and settlement.
  - Not making the funds available to the credit party until settlement.
  - Appropriate collateral or guarantee of acceptable financial institutions or insurance to cover debit balance.
- 3.3.57. In designing the settlement system, the need for integrity as well as efficiency of the funds transfer system as a whole may have to be given priority, especially in the initial stages of developing the EFT system.

## **PART - IV**

### **COMMITTEE'S FINDINGS AND CHOICE OF LEGAL FRAME WORK**

#### **Summary of Findings**

- 3.4.1. For sustained growth and efficient functioning of any system of EFT, a close co-ordination between technology and legal rules is essential. The design of the system determines whether funds transfer can be made promptly, accurately and securely. The law must correspondingly provide precise rules to define and determine rights and obligations arising out of EFT, so that quick and predictable resolution of disputes about loss, could be possible. [3.0.1 - 3.0.2]
- 3.4.2. Electronic technology has already spread its roots in our banking industry and is presently in the process of growing to its adulthood. However, corresponding development in the general legal rules, and procedures, have not kept pace with the fast changing business environment. [3.1.3 - 3.1.12]
- 3.4.3. Since the EFT System is in nascent stage, the existing framework for monetary

and banking regulations could be considered to be adequate in the short term to deal with various regulatory and supervisory issues. When more and more consumer oriented EFT systems like EFTPoS take shape and if multiple systems of credit transfers are organised, there would be a need for regulations and monitoring of not only the design of the system but also the operations of the service providers and users. For this purpose, specific empowerment of the Reserve Bank, being the monetary and banking authority, would be required. [3.2.3 - 3.2.9]

- 3.4.4. EFT of all types would bring in a fresh crop of consumer issues. Most of these can however be adequately regulated under the existing provisions of law under the Consumer Protection Act (with the pending proposal for amendment) and the Banking Regulation Act. It would be too early to anticipate problem of future for formulating legal response for the consumer problems that arise when consumer oriented EFT systems attain maturity. [3.2.10 - 3.2.15]
- 3.4.5. Under the existing laws, banks in India are competent to undertake, subject to compliance with regulatory instructions wherever applicable, EFT business, whether by way of credit transfers or debit transfers. Similarly, customer activated funds transfer systems like ATMs and other card systems can also be organised by banks, subject to Reserve Bank's regulatory instructions. [3.2.16 - 3.2.18]
- 3.4.6. The Income Tax Act Provision requiring payment in excess of Rs. 10,000/- to be only by a crossed cheque or draft and in some cases "A/c. Payee" cheques or drafts may come in the way of implementation of EFT System, unless appropriate correction in the Tax Laws is made to clarify that the restriction on method of payment would not apply when payment is made by electronic transfer of funds between two accounts maintained with banks. [3.2.19]
- 3.4.7. The underlying funds transfer procedure changes to a large extent, and accordingly the legal consequences, when medium of communication changes from paper to electronics. Existing paper based funds transfer law in India is designed to operate as debit transfer. Since most EFTs are made by credit transfers, there are no statutory rules which are directly applicable to EFTs. EFT will also eliminate the elements of "negotiability", which is common in the paper based funds transfers. [3.2.20 - 3.2.23].
- 3.4.8. Default rule regarding finality of payment : Although it may be possible to determine finality of payment by analogy of existing laws or contract between



the parties, considerable confusion and uncertainty would arise depending on how the courts would view the relationship between various persons under an EFT transaction. Unlike paper-based payment for which a clearly pronounced finality rule is available, there is, at present, no finality rule that would specifically apply to EFTs. [3.2.24 -3.2.32].

- 3.4.9. There is no specific default rule under the existing law for determining the point of time up to which a payment order issued for execution in an EFT system is revocable. In the absence of contract, the problem may have to be resolved by courts by reference to the general provisions of contract and agency law. Unlike paper-based funds transfers where principles are well established by judicial decisions, in EFT there could be considerable confusion, till the position is settled by judicial pronouncements. [3.2.33 - 3.2.34]
- 3.4.10. There are no statutory provisions under the existing law which specifically provide for verification of authenticity of a paperless instruction. Although a legally binding security procedure can be established by agreement for determining authenticity of payment instructions, the question is whether, in the absence of statutory law governing the validity of such procedures, the reasonableness of such procedure may be open to judicial determination? In such cases the basis on which commercial reasonability or otherwise of such procedure can be decided by courts assumes significance. [3.2.35 - 3.2.37].
- 3.4.11. The security and confidentiality aspects of the design of the system may bring pressure on the secrecy obligation of banks. The existing provisions of banker's obligation of confidentiality needs a review for protection of both bankers and customers against unauthorised access to personal data. [3.2.38 - 3.2.41 & 3.3.22 - 3.3.29].
- 3.4.12. The existing laws contain only the general principles of awarding damages and the measure of damages. Ceiling on the liabilities of participants can be provided by specific terms in contract. If ceiling on customers liability in case of loss by interloper fraud etc. are required to be provided, separate statutory provisions would be required. [3.4 - 3.2.47].
- 3.4.13. The incidence of fraud and errors as well as malfunctioning or failure of communication network, including computer hardware and software failures, are matters governed by the Law of Contract and Torts. Given the tendency of inequality in the bargaining powers, in the absence of special statutory

provisions, there could be inequitable allocation of loss arising on account of frauds, errors and system failures. [3.2.42 -3.2.45].

- 3.4.14. Though the issue of systemic risk arising out of bank failures and insolvencies is a common issue for both paper-based and paperless funds transfers, the high intensity of the EFTs may call for special rules for interbank settlement procedure. [3.2.48 - 3.2.53].
- 3.4.15. Under the existing law, physical presentation of the cheque at the branch of the drawee bank is a legal requirement designed for the benefit of the drawer. The law permit waiver of this right by the drawer. A probe into the status of technology at the branch level to be adaptable for electronic presentation of cheque, as also the extent of alterations or forgeries discovered in the present system of physical presentation, is required for considering any change in the existing law. [3.3.1 -3.3.9].
- 3.4.16. The advent of EFT may aggravate the already unsatisfactory Indian law of evidence and also on rules relating to preservation of bank's records. This is an area where contractual framework may afford little assistance. [3.3.10 - 3.3.21].
- 3.4.17. The advent of EFT may open up new issues in bank frauds. Special statutory provisions to provide for criminal liability for unauthorised access and fraud, without requiring proof of the elements of mens rea as in the traditional criminal liability principle, may have to be provided. [3.3.38 - 3.3.50].

## **THE CHOICE OF LEGAL FRAMEWORK**

- 3.4.18. An important aspect that can be noticed in the findings of the Committee is that while the existing legal framework on most of the regulatory and consumer interest issues may be considered as adequate, atleast in the short term, these would be inadequate in regard to evidence and investigation issues. Most of the transactional issues could be covered by contractual framework. A contractual model has the advantage of maximum flexibility. But, when unregulated, it may lead to exploitation, especially when there is an inherent inequality in the bargaining power. Further, the growth of sound legal principles may be hampered if uniformity in the rights and obligations are not brought in. Choice by contract may lead to divergent incidence leading to considerable confusion and lack of uniformity. This leaves us to examine

the issue whether at this stage it is necessary in India to go in for a comprehensive legislation to consider all the issues where legal position is not very clear.

- 3.4.19. A legislative model has the advantage of maximum **certainty, uniformity and predictability**. But in considering the formulation of a detailed and comprehensive legislation one has to bear in mind the rigidity that will be brought in by a legislation. Legislation making is a slow process. Changing the legislation once made, is much slower. In an area where the technology is growing and fast changing, a comprehensive legislation may hamper the development. The experience in other countries does show that without a detailed legislation EFTs can successfully function on contract basis. EFT is an evolving field. By its very nature, maximum flexibility is needed to allow the system to grow in a market responsive environment. At the same time, the substantial issues do indicate that some form of basic regulatory framework and statutory rules to define the trigger events may have to be provided to ensure certainty and predictability of transactions. Even assuming that EFT can function under a contract regime, unless there is a statutory regulation to regulate the terms of such contracts, the development of law and legal principles may be hampered and there would be a complete confusion about the incidences of EFT operations. The experience in other countries shows that statutory rules were called in at some stage to prevent system providers from excluding by contract every conceivable source of their liability. **While a comprehensive legislation may hamper the development of evolving technology, leaving it completely to an unregulated contract regime may create chaos.**
- 3.4.20. That leaves us to the third alternative, namely, a combination of regulatory and contractual model. **A regulatory model, properly moulded, provides the certainty and predictability associated with statute law and at the same time leaves enough flexibility allowing growth and development of technology.** The question then is how much should we legislate and how much is to be left to be regulated by a flexible subordinate legislation technique? The UNCITRAL Legal Guide provides a clue for this. It says: **"if the number of special rules is too large it may be preferable for special law to be adopted, as there currently are for debit transfers".**
- 3.4.21. An instructive passage from the Jack Committee Report is noteworthy in considering the question of whether we should go for, and what type of, legal framework for EFTs. That Committee had observed :

"The need for some measure of EFT regulation is, in our judgement, urgent enough to override the cautionary argument for delay until EFT systems have developed further. But the caution should be kept firmly in mind: it will be of prime importance to limit any proposals to what is seen as absolutely necessary, and to frame them in such a way as will not hamper the design and development of future EFT systems. A 'two-tier' approach that restricts statute law to a few key issues common to EFT systems, reserving for standards of best practice those more detailed issues that bear on specific systems or technologies, should help to preserve flexibility."

## **CHAPTER IV**

### **EFT SYSTEM PROPOSED BY THE RESERVE BANK**

- 4.1. The Saraf Committee which went into the technological issues, has outlined an EFT System which would facilitate inter-bank and intra-bank funds transfer. When it materialises, banks and banks' customers should be able to transfer funds from any branch of the same bank or other bank in any corner of the country. That Committee has recommended setting up of a nation-wide EFT System under the leadership of the Reserve Bank. Having regard to the existing ground realities, it was recommended that initially the EFT System may cover the metro centres, and thereafter gradually extended to other centres, in a time-bound manner.
- 4.2. The EFT System as envisaged, would facilitate both low value-high volume funds transfers as well as high value low volume funds transfers. While the ultimate aim is to achieve funds transfer on Real Time basis to the beneficiary for high value funds transfers, an optimistic target of giving credit to the account of the beneficiary at least a day next to the date a funds transfer is initiated by the originator, is set out. It was felt that initially, making the funds available to a beneficiary on the day next to the date on which a payment order is initiated would be a major improvement in our existing payment system.
- 4.3. Considering the urgency of introducing an EFT System, especially for low value funds transfers, it was proposed by the Saraf Committee that the existing organizational set-up for MICR cheque processing would be adequate. It was also proposed by that committee that the computer and communication infrastructure being created as a part of technology upgradation of service branches of banks at centres where MICR Clearing is in place, would adequately meet the technology requirements of the proposed EFT in the initial stages.

#### **The Process Flow for the Proposed Low Value Funds Transfer**

- 4.4. Customers of branches of banks in a centre, where EFT facility is available, can request for remittance of funds to a designated beneficiary by furnishing

to that bank the identity of the account, the name and place of the beneficiary's bank and other required particulars. All such requests received by each branch will be accumulated upto a specified cut-off time on a working day and thereafter bunched and sent to a designated service branch of that bank either by electronic communication or through paper, depending on the level of computerisation of the branch.

- 4.5. The service branches of all banks in a centre to which the EFT system is extended would consolidate the payment instructions received by them from different branches upto a cut-off time specified for this purpose; then the service branches would transmit the electronic data file to the National Clearing Cell (NCC) of the Reserve Bank in accordance with the procedure specified in this behalf. The NCC and where there is no NCC, the agency appointed for this purpose, would function as an EFT Service Centre.
- 4.6. The EFT Service Centre in each place where EFT facility is extended, would sort out the payment instructions centre-wise and transmit EFT data file consolidated centre-wise to outstation EFT centres in the specified manner, retaining the local payment instructions. The local payment instructions will be sorted out bank-wise and consolidated data file for each bank would be transmitted to the service branches.
- 4.7. The outstation EFT Centres which receive EFT data file from other EFT centres would in turn, process the data file after complying with the specified security procedure and sort out payment instructions bank-wise and transmit the consolidated data files to respective service branches of banks in that centre. The service branches, after complying with the security procedure, in turn would process the data file branchwise and communicate the payment instruction to the respective branches which will credit the beneficiary's account after complying with the specified security procedure. The entire process from the time a payment instruction is received from the originator, till the beneficiary's account is credited, is expected to be completed in two days.

## **High Value Funds Transfers**

- 4.8. Any payment of the value of Rs.one crore and above would be treated as high value payment. For high value payments, a faster method of processing and funds availability to the beneficiary on the same day by batching the messages for more than once a day, is proposed.

## **Security procedures and integrity of the system**

- 4.9. The Saraf Committee seems to have realised that it may not be practical to assume a completely automated EFT System in the initial stages. When the system starts, it may have to be necessarily a hybrid system of message transmission. The Committee, however, appears to have considered that at least at the stage of consolidation at the service branch of a bank in a centre, the paper should get converted into electronic media and data can flow electronically with adequate security system. At each stage, a security procedure conforming to accepted standards would have to be put in place to ensure maximum safety, security and integrity of the funds transfer system.

## **Inter-bank Funds Settlement**

- 4.10. In the proposed EFT System, settlement service would be provided by the Reserve Bank. The Reserve Bank will debit the remitting bank's account at the originating centre and credit the beneficiary's account at the destination centre. An appropriate clearing and settlement system would be put in place to minimise risk and ensure efficiency.

## **EFT- THE FUTURE DIRECTION (AS ADVISED TO THE COMMITTEE)**

### **Communication backbone**

- 4.11. The most important pre-requisite for establishment of an EFT is the existence of a very reliable communication network. The quality of terrestrial communication network in India leaves much to be desired. The only reliable communication infrastructure seems to be the one based on satellite communication using VSAT network. The VSAT networks provide rapid, reliable satellite transmission of data, voice and video between unlimited number of geographically dispersed sites. The Committee understands that the Reserve Bank or a designated agency is planning to set up a satellite based VSAT network to cater to the needs of banking industry as a whole. The proposed network is to cover all the State capitals, district head quarters, major commercial centres and currency chest centres, in a phased manner. Bank offices, financial institutions, Government departments form the main target group. Starting with about 50 VSATs, progressively, the number of VSATs may go upto 5000. The network infrastructure will have redundancy in terms of HUBs, servers, etc. A Network Management System will monitor

the performance of the traffic, configure remote nodes, diagnose, isolate and report faults and allocate bandwidth among different nodes.

## **Upgradation of proposed Small-value high-volume EFT**

- 4.12. When the above communication infrastructure is ready, the existing EFT solution will be upgraded to work in the new infrastructure. This solution as well as the High-value EFT solution, described below, is to use the same backbone.

## **Proposed Model of large-value EFT Network**

- 4.13. The above infrastructure will take care of both high-value institutional funds transfer as well as retail transactions. The solution will support transfer of funds on Real Time Gross Settlement (RTGS) basis as well as on a batch basis, at periodical intervals. The solution will have all the security features of International standard, to ensure data integrity. After the settlement is done in the Reserve Bank, the necessary settlement reports will travel to the desired destination. The solution will provide for audit trail and log file to keep track of activities in the network. Facilities to monitor current account balance position of participating institutions will be provided. The solution will be a high availability one with redundancy in respect of critical components.

## **LEGAL ASPECTS OF THE PROPOSED EFT SYSTEM**

### **The terminology**

- 4.14. There is no generally accepted terminology in use to describe the parties or the activities involved in funds transfer. In each country, terms have developed which have reflected the realities of funds transfer system in use, in that country<sup>1</sup>. But at the same time, efforts to harmonize EFT rules and terminology used in EFT transactions by developing international standards is made by various International Agencies<sup>2</sup>. Keeping in mind the needs for harmonization of terminology and at the same time giving to the terminology closest

---

<sup>1</sup> See, generally *UNCITRAL LEGAL GUIDE ON ELECTRONIC FUNDS TRANSFERS*, United Nations, New York(1987).

<sup>2</sup> see, para 2 of *UNCITRAL Guide* *ibid*.



functional meaning as obtained in present banking practices in India, the Committee decided to adopt specific terminology to identify, analyse and define the parties and activities in EFT. A Glossary of terms adopted by the Committee as also a select collection of Glossary in other systems is in **Appendix A**.

- 4.15. The EFT System outlined above is basically a credit transfer system. The principal parties in this system are the "originator" who initiates a payment instruction by issuing a "payment order" to his bank which is called a sending bank. Sending bank accumulates the payment orders received by it in a day upto a cut-off time ("specified time") and sends the bunch of orders to its "service branch". The service branch prepares "EFT data file" by consolidating payment orders received from the branches it serves. The NCC or other agency specified in each centre as "EFT service centre" receives EFT data file from service branches and after processing transmits the EFT data file consolidated by it to respective outstation EFT centres. Depending on whether a service branch or EFT is sending an EFT data file or receiving an EFT data file, it is called "Sending Service Branch" and "Sending EFT Service Centre" or as the case may be, "Receiving Service Branch" or "Receiving EFT Service Centre". The person to whom the funds are transferred is called the "Beneficiary" and his bank the "Beneficiary Bank".

## **Scope of the Proposed EFT System**

- 4.16. The legal implications of the proposed system in terms of nature of the funds transfer, territorial limits for the transfer, monetary unit, and limitation for participation and the conditions subject to which the facility could be extended need to be clearly spelt out. For this purpose, the main issues that need to be considered are discussed below.

### **1. Nature of the funds transfer**

- 4.17. The procedure required to be followed and the rules of finality as well as rights and obligations of participants would considerably differ in respect of credit transfers and debit transfers. While most of the existing rules of Negotiable Instruments Act may be applied to EFT debit transfers, separate rules for credit transfers would be required. Both, credit transfers as well as debit transfers may not be governed by the same set of rules. It would also be necessary to explore in terms of system compatibility and operational

efficiency whether both type of funds transfer can be operated in the proposed EFT system. Similarly, taking into account the risk and time critical elements in the high value funds transfers, separate procedure for processing, executing and settling these transfers may be required to be provided for.

## **2. Territorial limits**

- 4.18. In an EFT system both sending bank and receiving bank need to be bound by certain basic rules for payment and settlement. The existing provisions of the RBI Act in regard to extending overdraft (without collateral) to banks will have to be taken into account in streamlining the settlement procedure. Further, having regard to the existing exchange control regulations, it is to be considered, whether the funds transfer system should eventually be only a domestic funds transfer system in which funds can be transferred only within the territorial limits of India.

## **3. Monetary Unit**

- 4.19. The existing exchange control regulations would have to be kept in view in deciding whether only funds expressed in Indian rupees should be permitted for transfer in the system.

## **4. Participation**

- 4.20. Who can use the system for funds transfer in the proposed system? If the Reserve Bank or its agencies have to act as EFT Service Centres and provide settlement service, only banks and institutions considered as eligible to open and maintain account with the Reserve Bank would become settlement participants. Having regard to the need for ensuring safety, soundness and integrity of the system and the need to minimise the systemic risk, certain prudential criteria may have to be adopted to put in place an objective procedure of admitting settlement participants in the system. Further, inter-bank and intra-bank funds transfer facility may have to be restricted to settlement participants only.

## **5. General Conditions**

- Having regard to the possible abuse of the system for evasion of tax and other unlawful remittances, it is for consideration whether

transfer of funds should only be required to be routed between two identifiable accounts.

To ensure operational efficiency and to minimise errors, it may be necessary to require the payment order to be in a specified format.

## **Legal Framework**

- 4.21. If the proposed EFT system is to be operated by the Reserve Bank, binding rules for the operation of the system and mutual rights and obligations of the participants could be provided by the Reserve Bank under its regulation making powers. However, these Regulations should not be extended to govern the banker-customer relationship between participating banks and their customers who may initiate the payment orders. The banker-customer relationship is contractual in nature and it should be possible to define precisely the transactional rules by contract, between banks and their customer.
- 4.22. There are two issues in designing combination of regulations and contract and their contents:
- How to ensure uniformity in the terms of contract made with customers by various banks?
  - How to eliminate inconsistency between RBI Regulations and banks' contract?
- 4.23. To ensure uniformity of terms leading to proper growth of legal principles and to ensure consistency between the Regulations and contract, it is for consideration whether a proper blend could be achieved by requiring the banks as a condition of their participation in the system, to adhere/adopt a Model Contract with their customers. In this process, EFT facility would be made available only to those customers who agree to be bound by the Regulations and terms of Model Contract.
- 4.24. As to the contents of Regulations and Model Contract, it may be necessary to adopt rules which would make the EFT facility more user friendly and thereby attractive. The advantages of attraction of speed and economy may be lost unless these are matched by equitable principles of loss allocation and safety of the funds transfer mechanism.

- 4.25. A rule of finality of payment needs to be formulated consistent with present banking practices as to credits to an account and issue of credit advice by bankers. The Committee understands that there is no uniformity in the banking practice in India in regard to sending to the customers, written advice of credits received to their accounts<sup>1</sup>. While some bigger banks with mass banking branch networks have not been following such a practice, some foreign banks and some of the Indian banks, both in public and private sector, have been following the written credit advice system. By international standards, this is a much desirable practice. Similarly, sending periodical statement of accounts to the customers also needs to be looked into when EFT systems are introduced. In the U. S. and the U. K. and many other advanced and developing countries, by law or bankers' implied contract, these have been made mandatory for banks.
- 4.26. In determining the irrevocability rules, the design of the system and its compatibility to effectively stop payment, needs to be considered. Security procedure would have to be of international standard. To ensure timely completion of payments, specific obligations of participants in regard to various acts in the system need to be specified and every participant be made accountable for loss caused by his default. To simplify investigation and resolution of disputes, it may be necessary to fix responsibility at one point so that bank customers need not engage in multi-party litigation.
- 4.27. While essential rules governing transactional issues need to be provided by Regulations and Contract, operational details could be supplemented by issue of circulars from time to time.

## Regulatory Issues

- 4.28. The lead proposed to be taken by the Reserve Bank may be necessary in the initial stages. However, in the proposed EFT system, unless proper firewalls are put in place in the long run, there could be a mix up of roles. EFT operations are basically banking services. The issues in it need to be seen from three angles - the regulator's angle, the system provider's angle and the user's angle. It may be possible to treat the Reserve Bank in the proposed system as

---

<sup>1</sup> For a detailed analysis of banking practice in India on bankers' obligation to send credit advice, see generally, the Report of the Committee on Customer Service in Banks (Goiporia Committee), IBA (1991).

a system provider apart from settlement bank. It would be natural to assume that design and security of the system would be the responsibility of the system provider. The question of technical standards of the design and certification by appropriate technical experts assumes significance from the point of view of liability for system failures, unauthorised third party access and interloper fraud. It may have to be considered as a matter of policy, whether the activities relating to EFT, even in the short term, should be separately and exclusively administered by a nodal department so that the identity of the regulatory role of the Reserve Bank is kept distinct from these activities as far as possible. Central bank is providing similar service in U. S. but the service is limited only to large value funds transfers. Reserve Bank may have to determine a policy as to whether in the long term, a national network of retail funds transfer services could be continued through some other agency or a subsidiary, retaining with the Reserve Bank only the large value inter-bank/inter-corporate payments. This may greatly help in avoiding any conflict of interest in the essential role of the Reserve Bank as bank regulator and monetary authority.

## **CHAPTER V**

### **RECOMMENDATIONS**

- 5.1. Having made a comparative study of the legal framework existing in some other countries and analysed the EFT issues in the light of present status of technology and legal provisions in India, and having recorded its findings thereon, the Committee unanimously makes the following

#### **GENERAL RECOMMENDATIONS :**

##### **5.2. Short Term Measures**

- 5.2.1. A judicious combination of regulatory and contractual models at this stage of development of technology in the country is ideal for introducing by the Reserve Bank, a country-wide EFT system for inter-bank and intra-bank credit transfers.
- 5.2.2. To start with, a single national level inter-bank and intra-bank funds transfer system may be introduced immediately through the Regulations to be made by the Central Board of the Reserve Bank under Section 58 of the Reserve Bank of India Act, 1934, on the lines of the draft placed in **Appendix B**.
- 5.2.3. A Model Customer Contract, as per the draft placed in **Appendix C**, which will govern the banker-customer relationship in regard to EFT, should be adopted by banks participating in the EFT System.
- 5.2.4. The administration and co-ordination of the EFT System operations should be assigned to a Nodal Department with requisite manpower having technical know how of the design and operations of the system. This will ensure security aspects and efficient functioning of the system.

## Long Term Measures

- 5.3.1. In the long term, banks may be encouraged to promote and establish consumer EFT systems like EFTPoS and other card based EFT systems. Promotion of a few more EFT systems for inter-bank transfer networks may also be encouraged.
- 5.3.2. The Reserve Bank may consider operating the EFT System through an agency or subsidiary so that a clear demarcation of its regulatory and supervisory role would be possible. Bulk transfers (low value high volume) may also be allowed to be managed by a group of large banks with country-wide branch network and technical capability, with settlement assistance by the Reserve Bank. The Reserve Bank may restrict its EFT System for high value inter-bank/inter-corporate funds transfers on "Real Time - Gross Settlement" basis.
- 5.3.3. When the Reserve Bank considers that multiple EFT Systems should be developed and regulated and yet a stage has not been reached where a full-fledged legislation can be enacted, it would be sufficient if the Reserve Bank of India Act is amended by introduction of a separate chapter dealing with EFT Systems and power is conferred on the Bank to draft Regulations necessary therefor.
- 5.3.4. When multiple EFT systems develop, for the purpose of regulating, defining and determining rights and obligations of the system providers and system users, a flexible statutory model empowering a central regulatory authority, preferably the Reserve Bank, be promoted for administration of the statute with enough rule making powers. An outline of such legislation is in **Appendix G**. The Parliament has got the legislative competence to enact the proposed EFT Act as it is covered by entries 38, 45, 46 and 48 of List-I of Union List under Schedule-VII of the Constitution of India. The draft of the EFT Legislation would not contravene any of the express provisions of the Constitution of India and it is not inconsistent or repugnant to any other existing law.

5.4. On the terms of reference, the Committee unanimously makes the following

## **SPECIFIC RECOMMENDATIONS :**

### **Reference No.1**

5.5. *Defining the scope of "Electronic Funds Transfer" and liabilities of the participants arising out of contractual obligations.*

### **5.6. Recommendations for short-term measures**

#### **5.6.1. Scope of EFT**

- (1) The EFT System to be established by the Reserve Bank should extend to any credit transfer within the country by any person, whether for high value or low value, if :
  - (a) the funds are transferred from an account of the originator maintained with the sending bank to a designated bank account of a designated beneficiary with a receiving bank.
  - (b) the sending bank and the receiving bank are admitted participants in the EFT System.
  - (c) the funds are expressed in Indian Rupees.
- (2) All commercial banks in public and private sector and cooperative banks satisfying certain criteria referring to prudential norms of capital adequacy, level of computerisation and willingness to abide by the regulations should be eligible to be admitted in the EFT System as a participant.
- (3) Financial institutions, Government departments and agencies of the Government and any other institutions approved by the



Reserve Bank to open a settlement account with it may also be eligible to be admitted as direct participant in the EFT System.

- (4) Account holders can avail the EFT facilities only through their banks.

#### **5.6.2. Responsibilities and liabilities of the participants and bank customers:**

The responsibilities and liabilities of the participants shall be determined by Regulations made by the Reserve Bank under Section 58 of the Reserve Bank of India Act. The rights and liabilities between a bank and its customers in regard to EFT shall be determined in terms of a Model Customer Contract. To achieve consistency and uniformity, the banks participating in the EFT System should be required to adhere to and adopt the model contract for determining the rights and liabilities between them and their customers.

### **5.7. Recommendations for Long-Term Measures**

- 5.7.1. Banks may be encouraged to organise and promote consumer oriented EFT Systems like EFTPoS, ATMs, and other card based payment systems. Alternative funds transfer systems in high volume and low value category should be encouraged to be promoted by selected banks. It would then be necessary to amend the Reserve Bank of India Act, by insertion of a chapter dealing with Multiple EFT Systems and empowering the Reserve Bank to draft Regulations for multiple payment system, by amending Section 58 of that Act on the lines of **Appendix D** to this report.
- 5.7.2. Eventually, the Reserve Bank may concentrate on high value inter-bank inter-corporate funds transfers so that bulk transfers or low value high volume transfers could be operated by other EFT Systems. A legislation on the lines of **Appendix G** placed with this report may be promoted for determining the responsibilities and liabilities of participants. The

Reserve Bank may be empowered by this statute to formulate and administer Regulations in regard to the design and operation of all EFT Systems.

## **Reference No.2**

5.8. *Defining the trigger events that determine the finality and irrevocability of the transfer of funds at different stages like sender finality, settlement finality receiver finality etc., including the scope for countermanding and money-back guarantees.*

## **5.9. Recommendations for Short-Term Measures**

### **5.9.1. Finality of payment**

Payment made under EFT shall be final when the receiving bank credits the funds to the account of the beneficiary whether or not the beneficiary is advised of the credit.

### **5.9.2. Irrevocability**

The payment order shall become irrevocable when it is executed by the sending bank. A payment order is treated as executed when the sending bank communicates the payment order to its service branch for further processing of the order.

### **5.9.3. Settlement finality**

A suitable procedure compatible with the system be worked out by the Reserve Bank by way of settlement procedure for inter-bank payment obligations. The Committee recommends that initially every bank should be required to ensure that it maintains adequate balance in its settlement account to meet the payment obligations arising on each day.

#### **5.9.4. Money back guarantee**

A customer suffering a loss due to non-completion of funds transfer shall be entitled to refund of the amount debited to his account by the sending bank for execution of that payment order, alongwith interest at the Bank Rate, beyond the third day from the date the payment order was initiated. No damages for special circumstances would be admissible for any loss on account of non-execution of the payment order. For the purpose of determining liabilities of the participants, the "fault principle" shall be followed so that the party on account of whose conduct loss had arisen and could be attributed to him, shall bear the loss.

#### **5.9.5. Disputes Resolution**

- (i) The bank customers should not be required to engage in multi-party litigations. The sending bank alone should be made answerable to the customers. The sending bank may however seek reimbursement from the participant at fault. As between banks and bank or bank and the Reserve Bank, panel of expert Arbitrators may be constituted by the Reserve Bank to resolve any claims.
- (ii) For resolution of complaints and claims by customers, the Reserve Bank may consider whether qualified Ombudsmen should be appointed or existing Ombudsman Scheme should be extended for resolution of EFT disputes.

#### **5.10. Recommendation for Long-Term Measures**

In the long term, when multiple systems of EFT and consumer oriented EFT Systems are developed, it would be necessary to formulate and define through statutory provisions, specific default rules to define the trigger events. The provisions in this behalf will have to be formulated after gaining experience in the short term. Accordingly, when the long term legislation is promoted, either the regulatory authority may be empowered to formulate

and administer regulations for trigger events or if found necessary, provision may be included in the statute itself.

## **Reference No. 3 & 4**

- 5.11. *Operational security & determination of liability in the event of operational failure at any stage. Defining measures to ensure security, integrity and efficiency of communication network linkages (eg. checksum, encryption, firewall, etc.)*

## **Recommendations**

### **5.12. Operational security**

5.12.1. Security procedure involving electronic authentication conforming to accepted technical standards should be adopted. Since consumer education in this regard is yet to start, initially security procedure may be specified by the Reserve Bank for participants and by banks for their customers. But in the long run, these will have to be established by contract.

5.12.2. Before starting the EFT operations, to ensure that the design of the system is in conformity with accepted technical standards, proper certification should be obtained. This is necessary to ensure safety and security as well as to avoid any possible claim against the system provider in respect of failure to provide a system with accepted standards.

### **5.13. Liability for computer hardware or software failure**

#### **Recommendation for Short-Term Measure**

5.13.1. Having regard to the dependence on available infrastructure facilities and the ground realities of possible interruptions, any liability on account of the system failure (computer hardware and software failures) should be excluded. Unless negligence of the parties is proved, a

participant or system provider should not be made liable for loss on account of system failure.

### **Recommendation for Long-Term Measure**

5.13.2. In the long term, when the legislation is promoted, specific provision empowering the regulator to ensure standards in the system design and operations of the system providers should be included.

#### **Reference No.5**

5.14      *Definition of "fraud" in electronic environment.*

### **Recommendation**

5.15.      In the long term, offences in regard to computer misuse and penalty may be defined on the lines of the UK Computer Misuse Act.

#### **Referene No.6**

5.16.      *The extent to which paper documents are mandatory vis-a-vis the contractual obligations.*

### **Recommendation for Short-Term Measure**

5.17.      In the EFT System to be introduced by the Reserve Bank, banks should be required to furnish to the customers on request, duly authenticated written confirmation of the completion of funds transfer.

### **Recommendations for Long-Term Measures**

5.18.1. In the long term, provision for automatic print-outs in all consumer oriented EFT Systems should be made mandatory. Banks should also adopt the internationally observed practice of sending written communication of receipt of credit to the accounts of customers.

- 5.18.2. The existing provisions of the Banking Companies (Preservation of Records) Rules, 1985, should be reviewed in relation to EFTs and specific provisions compatible with regulatory concerns should be provided.

#### **Reference No.7**

- 5.19. *Consequences of bank failures and other systemic events - procedures to follow.*

#### **Recommendation for Short-Term Measure**

- 5.20. Initially, in the EFT System to be introduced by the Reserve Bank, the settlement procedure should be self-insuring by eliminating overdraft. Gradually, the time-gap between the point of time at which the party's account is credited and the point of time of settlement between banks should be minimised.

#### **Recommendation for Long-Term Measure**

- 5.21. In the long term, in the proposed EFT Legislation, provisions should be included for establishment of a Contingency Fund. A part of the fee/charges recovered from the participants should be contributed to build up a corpus for this contingency fund which can be used to arrest any systemic risk of bank failures in settlement of EFT transactions.

#### **Reference No.8**

- 5.22. *Admissibility of electronic media for the purpose of evidence, preservation of period of electronic media etc.*

#### **Recommendations**

- 5.23.1. An amendment to Bankers' Books Evidence Act on the lines of Appendix E placed with this report may be promoted to make the records in any electronic data retrieval system and computer print-outs, admissible evidence and accord to it, the status of 'primary evidence'.

- 5.23.2. The Reserve Bank may review the existing rules under the Banking Companies (Period of Preservation of Records) Rules, 1985 and formulate specific rules for the preservation of records stored in disc, floppy, micro-film and any other computer or electronic data retrieval system.

## **Reference No.9**

- 5.24. *Cheque truncation*

## **Recommendation**

- 5.25. The Committee is not in favour of recommending amendment to the Negotiable Instruments Act immediately to dispense with the requirement of physical presentment of cheques, especially in the light of the status of the present technology at branch level. As and when the banks are able to upgrade technology for transmission of cheque images, a cheque truncation procedure based on customer consent could be evolved. The extent of cases of alteration and fraudulent encashment should be studied thereafter, and if such study shows that advantages of cheque truncation outweigh the risk involved in cheque truncation, steps may be taken for promoting an amendment to Section 64 of NI Act to provide for presentation by electronic transmission of image.

## **Reference No.10 & 11**

- 5.26. *Any other matter relating to Electronic Funds Transfer such as securities transfer and other cash/credit/ debit transactions through Electronic Funds Transfer at Point of Sale (EFTPoS) devices and computer/communication net-works. A comprehensive fresh legislation to deal not only with EFT, but also for bringing changes required in the existing Acts such as Negotiable Instruments Act, Bankers' Book Evidence Act, Securities (Contract Regulation) Act (SCRA) etc.*

- 5.27. **Recommendations for Short-Term**

- 5.27.1. The draft of the Regulations that may be made by the Central Board

of the Reserve Bank for establishing a country-wide EFT System by the Reserve Bank is in **Appendix B**. The draft of the Model Customer Agreement, to be adopted by banks is in **Appendix C**.

5.27.2. Following amendments to existing laws are recommended:


- (a) An amendment to Reserve Bank of India Act, 1934 on the lines of **Appendix D** to this Report.
- (b) An amendment to Bankers' Books Evidence Act, 1891 on the lines of the draft in **Appendix E** placed in this Report or alternatively on the lines of Section 138 C introduced in 1988 in the Customs Act, 1962, should be pursued immediately.
- (c) The Reserve Bank should take up with the Central Board of Direct Taxes (CBDT) the question of clarifying and if required, amending the relative provisions of the Direct Tax Laws, for recognising and according to the funds, transferred under the Reserve Bank EFT System, the same status as that of a payment by account payee cheque.

## 5.28. **Recommendations for Long-Term Measures**

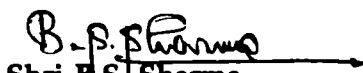
- (a) An EFT Legislation in the long run, should be promoted to establish a central regulatory authority, preferably the Reserve Bank, for the purpose of regulating establishment and operations of EFT Systems. This legislation should also provide for default rules in regard to various trigger events like finality of payment, irrevocability and settlement. A draft of the outline for such legislation is placed in **Appendix G** of this Report. The Parliament has got the legislative competence to enact the proposed EFT Act as it is covered by entries 38, 45, 46 and 48 of List-I of Union List under Schedule-VII of the Constitution of India. The proposed Act would not contravene any fundamental rights or any other express provisions of the Constitution of India and is not inconsistent or repugnant to any other existing law.



- (b) For protection of personal data, a legislation on the lines of the UK Data Protection Act may be promoted as a long term measure.
- (c) A comprehensive legislation on the lines of Computer Misuse Act of the United Kingdom may be promoted.



**Smt. K.S. Shere**  
Chairperson



**Shri B.S. Sharma**  
Member



**Shri A.S. Khan**  
Member



**Smt. Rama Ananthakrishnan**  
Member



**Shri K. Samdani**  
Member



**Shri. S. Venkatachalam**  
Member



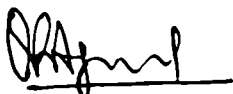
**Shri Arjun Goswami**  
Member




**Shri K.R. Ganapathy**  
Member



**Shri. V.K. Shah**  
Member



**Shri O.P. Agarwal**  
Member



**Shri N.V. Deshpande**  
Member-Secretary

Bombay,  
January 18, 1996.

## **APPENDICES**

	<b>Page</b>
<b>APPENDIX A</b>	Glossary of terms 91
<b>APPENDIX B</b>	(Draft) RBI (EFT) Regulations, 1996 99
<b>APPENDIX C</b>	(Draft) Model Customer Agreement 114
<b>APPENDIX D</b>	(Draft) Amendment to RBI Act 119
<b>APPENDIX E</b>	(Draft) Amendment to Bankers Books Evidence Act 121
<b>APPENDIX F</b>	Extract of the Customs and Central Excise Laws (Amendment) Act, 1988 123
<b>APPENDIX G</b>	Outline of the Proposed EFT Act 126

## GLOSSARY OF TERMS

---

### I. TERMS ADOPTED BY THE COMMITTEE

---

**"Acceptance"** means execution of a payment order.

**"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.

**"Beneficiary"** means the person designated as such, and to whose account payment is directed to be made, in a payment order.

**"Beneficiary bank"** means the branch of the bank identified in a payment order in which the account of the beneficiary is to be credited.

**"EFT"** means Electronic Funds Transfer.

**"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.

**"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.

**"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.

**"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.

**"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.

**"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.

**"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.

**"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.

**"Notified"** means communicated electronically or in writing.

**"Originator"** means the person who issues a payment order to the sending bank.

**"Participating Bank or Institution"** means a bank or as the case may be, an institution admitted for participating in the EFT System.

**"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.

**"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.

**"Reserve Bank"** means the Reserve Bank of India established under the Reserve Bank of India Act, 1934 (2 of 1934).

**"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 issued; and
- (ii) for detecting error in the transmission or the content of a payment order, a communication and an EFT Data File.

A security procedure may require the use of algorithms or other codes, identifying words or numbers, encryptions, callback procedures, authentication key or similar security devices specified from time to time.

**"Sending bank"** means the branch of a bank, maintaining an account of and to which payment order is issued by the originator.

**"Settlement Account"** means an account opened and maintained for the purpose of settlement of payment obligations under EFT System.

**"Specified"** means specified by procedural guidelines issued from time to time by the Nodal Department pursuant to these Regulations.

---

## **II. EXTRACT FROM THE GLOSSRY OF TERMS ADOPTED BY JACK COMITTEE (U.K.)**

**SOURCE : Réport of the Review Committee on Banking Services : Law and Practice, HMSO, London (1989)**

---

**ATM (Automated Teller Machine) :** Computerised self-service cash dispenser operated by inserting a magnetic stripe card followed by the appropriate PIN. Services available apart from cash withdrawals may include deposits, balance enquiries, mini-statements etc.

**AUTHENTICATION :** Means of ensuring that a message or instruction in an EFT context comes from an authorised source; the most common example is the PIN.

**BIOMETRIC IDENTIFICATION TECHNIQUE :** Means of personal identification based on the recognition of a physical characteristic unique to each individual. Techniques currently being developed include fingerprint, palmprint and voice recognition and vein and retina scan.

**BUDGET CARD :** Type of credit card with a credit limit based on a multiple of the sum paid by the cardholder into his account each month.

**CASH CARD :** Payment card used in conjunction with an ATM.

**CHARGE CARD :** Also known as "travel and entertainment card". Similar to a credit card, it enables the holder to make retail payments normally of unlimited value, but unlike a credit card, the balance must be settled in full on receipt of a monthly statement. An annual fee is normally payable. The most common examples are American Express and Diners Cards.

**CHEQUE GUARANTEE CARD :** Card issued by a bank or building society for the purpose of guaranteeing the payment, or supporting the encashment of a cheque upto a value of (normally) 50. Some credit cards may also function as a cheque guarantee card.

**CLEARING :** Transmission of instructions and settlement of payments between accounts held at different banks or different branches of the same bank.

**CREDIT CARD :** Card which enables the holder to pay for goods and services on credit, and to obtain cash advances. On receipt of a monthly statement, the customer

may settle the outstanding balance in full, or in part, with any balance carried over being charged interest. The most common examples are Access and Visa.

**CREDIT TRANSFER** : Process by which a debtor sends (pushes) funds through the banking system to his creditor (this contrasts with transfer by cheque where the creditor draws funds from the debtor's account to his own). See also **BANK GIRO CREDIT**.

**DEBIT CARD** : Card which may be used to pay for goods and services at a point-of-sale terminal, automatically debiting the customer's account (it may also normally be used as a cash card).

**DIRECT DEBIT** : Direct claim made (initiated) by a creditor on his debtor's bank account. His debtor must approve the arrangement in advance and give his bank, signed authority to transfer funds periodically as instructed by the payee.

**EFT** : (Electronic Funds Transfer) Funds transfer effected through the banking system by electronic techniques with input and output methods being largely or completely in electronic form.

**EFT-POS** : (Electronic Funds Transfer at Point of Sale). Payment system allowing retail payments to be made by transferring funds electronically from the customer's account to the retailer's account without the use of cash or cheques. The customer passes his payment card through a terminal at the sales point and authorises the transaction by entering his PIN or signing a receipt slip. If card and PIN/signature are valid, the terminal accepts the transaction and transmits details of it to a central processor, from which the retailer's bank account is credited and the customer's account debited automatically.

**ENCRYPTION** : Cyphering or scrambling of an electronically transmitted message to conceal its meaning and prevent unauthorised access or alteration.

**HACKING** : Unauthorised access to information held on a computer.

**HOME AND OFFICE BANKING SYSTEM** : System which allows a customer to call up account information, transfer funds between accounts held in the same name, and make bill payments to specified third parties from his home or office, using a personal computer or television with special keyboard or adapted telephone, linked to the bank's central computer.

**LASER CARD** : Payment card whose store of data relating to the holder and to his account may be accessed and updated by a reader terminal using laser technology.

**MAGNETIC STRIP(E)** : On payment cards, holding encoded machine-readable information for identification, authorisation and transmission purposes.

**OFFLINE** : Describes payment system which is not linked to a central computer where data must be physically transmitted at the end of the day by tape, disc etc. Hence **ONLINE**, which describes payment systems directly linked to a central computer and so capable of immediate updating.

**PAYMENT CARD** : Generic term for any plastic card (credit, debit, charge, storecard etc.) which may be used on its own to pay for goods and services or to withdraw cash.

**PIN** : (Personal Identification Number). Set of characters (usually a four digit sequence) to authenticate funds transfer instructions initiated through a customer activated terminal such as ATM.

**SMART CARD** : Payment card incorporating microprocessors (with very large data storage capacity) accessible by electronic terminal readers whereby, for example, details of transactions may be recorded and the available balance stored on the card updated. Also known as **MEMORY** or **CHIP CARD**.

**STORECARD** : Payment card (with functions equivalent to a credit or budget card) for use at the retail outlets of the issuer or the trader on whose behalf it is issued.

**TRUNCATION** : Method of processing a cheque whereby it is not returned (presented) to the drawer's bank, but rather is retained by the collecting bank. The drawer's account is debited on the basis of the payment information, incorporated in the cheque, that is electronically transmitted from a collecting bank to the paying bank.

---

### **III. EXTRACT FROM THE GLOSSARY OF UNCITRAL**

**SOURCE** : UNICITRAL Legal Guide on EFT, United Nations, New York (1987)

---

**CLOSED-USER NETWORK (FOR FUNDS TRANSFERS)** : A paper-based or electronic clearing house, a communications service or a switch which is restricted to the banks or their customers who agree to adhere to particular technical standards and banking procedures.



**COMMUNICATIONS SERVICE** : A service that moves messages, including funds transfer instructions, among subscribers but which does not perform the accounting to enable settlement. (Similar to definition of "communication service" in DIS 7982) .

**CREDIT TRANSFER** : A funds transfer where the account of the originating bank or its customer is to be debited and the account of the destination bank or its customer is to be credited.

**DEBIT TRANSFER** : A funds transfer where the account of the originating bank or its customer is to be credited and the account of the destination bank or its customer is to be debited. (Compare to definition of "debit transfer" in DIS 7982.)

**ELECTRONIC CLEARING HOUSE** : A clearing house for funds transfer instructions in electronic form. An electronic clearing house may be either on-line or off-line. An electronic clearing house operating in batch mode is also referred to as an automated clearing house.

**FUNDS TRANSFER** : Movement of funds between the transferor and the transferee. (Almost identical to first sentence of DIS 7982. Compare definitions of "funds transfer transaction" and of "payment" in DIS 7982.)

**INTERMEDIARY BANK(S)** : Bank(s) between the originating bank and the destination bank through which a funds transfer passes. (Compare to definition in DIS 7982.)

**SETTLEMENT** : A transfer of funds from a bank with a debit position to a bank with a credit position or an agreed accounting entry between them to cover one or more prior funds transfer transactions. (Based on DIS 7982.)

---

#### **IV. EXTRACT FROM ARTICLE 4A OF UCC (1991) U.S.A.**

**SOURCE : 12 CFR, appendix B to subpart B.**

---

**"Payment order"** means an instruction of a sender to a receiving bank, transmitted orally, electronically or in writing, to pay, or to cause another bank to pay, a fixed or determinable amount of money to a beneficiary if:

- i) the instruction does not state a condition to payment to the beneficiary other than time of payment.
- ii) the receiving bank is to be reimbursed by debiting an account of, or otherwise receiving payment from, the sender, and

- iii) the instruction is transmitted by the sender directly to the receiving bank or to an agent, funds-transfer system, or communication system for transmittal to the receiving bank.

**"Funds Transfer"** means the series of transactions, beginning with the originator's payment order, made for the purpose of making payment to the beneficiary of the order. The term includes any payment order issued by the originator's bank or an intermediary bank intended to carry out the originator's payment order. A funds transfer is completed by acceptance by the beneficiary's bank of a payment order for the benefit of the beneficiary of the originator's payment order.

**"Funds-transfer system"** means a wire transfer network, automated clearing house, or other communication system of a clearing house or other association of banks through which a payment order by a bank may be transmitted to the bank to which the order is addressed.

**Security procedure"** means a procedure established by agreement of a customer and a receiving bank for the purpose of (i) verifying that a payment order or communication amending or cancelling a payment order is that of the customer, or (ii) detecting error in the transmission or the content of the payment order or communication. A security procedure may require the use of algorithms or other codes, identifying words or numbers, encryption, callback procedures, or similar security devices. Comparison of a signature on a payment order or communication with an authorised specimen signature of the customer is not by itself a security procedure.

---

**(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.

- (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 algorithms 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.

## **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 is liable to be kept under suspension for such period as may be specified in the order of suspension.

- (2) Every order of suspension shall be notified immediately to all the participating banks and institutions including a bank or institution against which the order of suspension is passed.
- (3) An order of suspension may be reviewed and may be revoked at any time by the Governor upon representation received from the concerned bank or institution or on his own. Every revocation shall be notified immediately to all participating banks and institutions.
- (4) A participating bank or an institution shall not, while any order of suspension is in force against it, be entitled to send or receive any EFT data file or otherwise to effect any funds transfer in the EFT System.

Provided that a suspension shall not affect the obligations of the suspended 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 writing, and before the expiry of one month from the date of receipt of notice by the Nodal Department.
- (3) Notwithstanding its withdrawal, a bank or institution shall discharge all its payment obligations arising out of fund transfers attributable to it, whether effected before or after the withdrawal became effective.
- (4) The withdrawal of any participating bank or institution shall be notified to all 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 by the Governor on his being satisfied that such bank or institution has

- (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**

#### **11. 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 separate 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 respect 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 separate unit.

- (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

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 account 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 guidelines**

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.

---

## **(DRAFT) MODEL CUSTOMER AGREEMENT**

---

**(Name of the bank, branch and address)**

- Name of the Customer
- Address for communication in regard to EFT
- Particulars of Account/s designated for EFT

### **TERMS AND CONDITIONS OF EFT EXECUTED IN THE RBI EFT SYSTEM**

I/We am/are desirous of availing the Electronic Funds Transfer Facility through the RBI EFT System. In consideration of the bank agreeing to extend to me/us the said EFT facility, I/we hereby agree to and undertake the following terms and conditions :

#### **1. Definitions**

- (i) "Customer" means the person named hereinabove who has executed this Agreement.
- (ii) "Bank" means .....
- (iii) "EFT Facility" means the Electronic Funds Transfer Facility through the RBI EFT System
- (iv) "Security Procedure" means a procedure established by agreement between the bank and the customer for the purpose of verifying that the payment order or communication amending or cancelling a payment order transmitted electronically is that of the customer or for detecting error in the transmission for the content of the payment order or communication. A security procedure

may require the use of algorithms or other codes, identifying words or numbers, encryption, callback procedures, or similar security devices.

- (v) Words or expressions used in this Agreement, but not specifically defined herein shall have the respective meanings assigned to them in the RBI EFT Regulations, 1996.

## **2. Scope of the Agreement**

- (1) This Agreement shall govern every payment order issued by the customer during the period of validity of the Agreement.
- (2) This Agreement shall be in addition to and not in derogation of the RBI EFT Regulations, 1996. The customer has gone through and understood the RBI (EFT Systems) Regulations, 1996 and agrees that the rights and obligations provided therein in so far as it relates to the originator shall be binding on him/it in regard to every payment order issued by him/it for execution in the EFT System.
- (3) The customer understands and agrees that nothing in this Agreement shall be construed as creating any contractual or other rights against the Reserve Bank or any participant in the EFT System, other than the bank.

## **3. Commencement and termination**

- (1) This Agreement shall come into force as soon as a security procedure is established by mutual agreement between the bank and the customer.
- (2) The Agreement shall remain valid until it is replaced by another agreement or terminated by either party or the account is closed, whichever is earlier.
- (3) Either party to this Agreement may terminate this Agreement by giving one month's notice in writing to the other party. Notwithstanding the termination of the Agreement the parties to the Agreement shall be bound by all transactions between them in regard to EFT Facility availed of by the customer, before the termination of the Agreement.

#### **4. Security procedure**

- (1) For the purpose of agreement for security procedure, the bank may offer one or more or a combination of one or more security devices.
- (2) A security procedure once established by Agreement shall remain valid until it is changed by mutual agreement.

#### **5. Rights and obligations of customer**

- (1) The customer shall be entitled, subject to other terms and conditions in the Regulations and this Agreement, to issue payment orders for execution by the bank.
- (2) Payment order shall be issued by the customer in the form annexed hereto, complete in all particulars. The customer shall be responsible for the accuracy of the particulars given in the payment order issued by him and shall be liable to compensate the bank for any loss arising on account of any error in his payment order.
- (3) The customer shall be bound by any payment order executed by the bank if the bank had executed the payment order in good faith and in compliance with the security procedure. Provided that the customer shall not be bound by any payment order executed by the bank if he proves that the payment order was not issued by him and that it was caused either by negligence or a fraudulent act of any employee of the bank.
- (4) The customer shall ensure availability of funds in his account properly applicable to the payment order before the execution of the payment order by the bank. Where however, the bank executes the payment order without properly applicable funds being available in the customer's account, the customer shall be bound to pay to the bank the amount debited to his account for which an EFT was executed by the bank pursuant to his payment order, together with the charges including interest payable to the bank.
- (5) The customer hereby authorises the bank to debit to his account any liability incurred by him to the bank for execution by the bank of any payment order issued by him.
- (6) Customer agrees that the payment order shall become irrevocable when it is executed by the bank.

- (7) Customer agrees that the bank is not bound by any notice of revocation unless it is in compliance with the security procedure.
- (8) Customer agrees that he shall not be entitled to make any claim against any party in the RBI EFT System except the bank.
- (9) Customer agrees that in the event of any delay in the completion of the Funds Transfer or any loss on account of error in the execution of the Funds Transfer pursuant to a payment order, the bank's liability shall be limited to the extent of payment of interest at the Bank Rate for any period of delay in the case of delayed payment and refund of the amount together with interest at the Bank Rate upto the date of refund, in the event of loss on account of error, negligence or fraud on the part of any employee of the bank.
- (10) Customer agrees that no special circumstances shall attach to any payment order executed under the EFT Facility under this Agreement and under no circumstances customer shall be entitled to claim any compensation in excess of that which is provided in clause (9) above, for any breach of contract or otherwise.

## **6. Rights and obligations of the bank**

- (1) The bank shall execute a payment order issued by the customer duly authenticated by him as verified by the security procedure, unless :
  - (a) the funds available in the account of the customer are not adequate or properly applicable to comply with the payment order and the customer has not made any other arrangement to meet the payment obligation.
  - (b) the payment order is incomplete or it is not issued in the agreed form.
  - (c) the payment order is attached with notice of any special circumstances.
  - (d) the bank has reason to believe that the payment order is issued to carry out an unlawful transaction.
  - (e) the payment order cannot be executed under the RBI EFT System.
- (2) No payment order issued by the customer shall be binding on the bank until the bank has accepted it.

- (3) The bank shall, upon execution of every payment order executed by it, be entitled to debit the designated account of the customer, the amount of the funds transferred together with charges payable thereon, whether or not the account has sufficient balance.
- (4) If the funds transfer is not complete before the close of business of the third following EFT business day the bank shall advise the customer.
- (5) The bank shall issue to him a duly authenticated record of the transaction after completion of the funds transfer and also issue at the end of each month, a statement of account. The customer shall, within a period of two days from the date of receipt of the record of transaction or as the case may be, within the period of ten days from the date of receipt of the monthly statement report to the bank any discrepancy in the execution of the payment order. The customer agrees that he shall not be entitled to dispute the correctness of the execution of the payment order or the amount debited to his account if he fails to report the discrepancy within the said period days.

Date:

Signature of the Customer

---

**(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.

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 .....

- 2. 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.'



---

**(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.

# **THE BANKER'S BOOKS EVIDENCE AMENDMENT BILL, 1994 (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)".

---

**Extracts from  
THE CUSTOMS AND CENTRAL  
EXCISES LAWS (AMENDMENT) ACT, 1988**

---

(The following text was inserted by way of Section 138C in the Customs Act, 1962 and Section 36B in the Central Excise and Salt Act, 1944)

**Admissibility of micro films, facsimile copies of documents and computer print outs as documents and as evidence**

- (1) Notwithstanding anything contained in any other law for the time being in force,
- (a) a micro film of a document or the reproduction of the image or images embodies in such micro film (whether enlarged or not); or
  - (b) a facsimile copy of a document; or
  - (c) a statement contained in a document and included in a printed material produced by a computer (hereinafter referred to a "computer print out"), if the conditions mentioned in sub-section (2) and the other provisions contained in this section are satisfied in relation to the statement and the computer in question,

shall be deemed to be also a document for the purposes of this Act and the rules made thereunder and shall be admissible in any proceedings thereunder, without further proof or production of the original, as evidence of any contents of the original or of any fact stated therein of which direct evidence would be admissible.

- (2) The conditions referred to in sub-section (1) in respect of a computer print out shall be the following, namely :-
- (a) the computer print out containing the statement was produced by the computer during the period over which the computer was used regularly to store or process information for the purposes of any activities regularly

carried on over that period by the person having lawful control over the use of the computer;

- (b) during the said period, there was regularly supplied to the computer in the ordinary course of the said activities, information of the kind contained in the statement or of the kind from which the information so contained is derived;
  - (c) throughout the material part of the said period, the computer was operating properly or, if not, then any respect in which it was not operating properly or was out of operation during that part of that period was not such as to affect the production of the document or the accuracy of the contents; and
  - (d) the information contained in the statement reproduces or is derived from information supplied to the computer in the ordinary course of the said activities.
- (3) Where over any period, the function of storing or processing information for the purposes of any activities regularly carried on over that period as mentioned in clause (a) of sub-section (2) was regularly performed by computers, whether --
- (a) by combination of computers operating over that period; or
  - (b) by different computers operating in succession over that period; or
  - (c) by different combinations of computers operating in succession over that period; or
  - (d) in any other manner involving the successive operation over that period, in whatever order, of one or more computers and one or more combinations of computers,

all the computers used for that purpose during that period shall be treated for the purposes of this section as constituting a single computer; and references in this section to a computer shall be construed accordingly.

- (4) In any proceedings under this Act and the rules made thereunder where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say, --
- (a) identifying the document containing the statement and describing the manner in which it was produced;

- (b) giving such particulars of any device involved in the production of that document as may be appropriate for the purpose of showing that the document was produced by a computer;
- (c) dealing with any of the matters to which the conditions mentioned in sub-section (2) relate

and purporting to be signed by a person occupying a reasonable official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate; and for the purposes of this sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.

(5) For the purposes of this section, –

- (a) information shall be taken to be supplied to a computer if it is supplied thereto in any appropriate form and whether it is so supplied directly or (with or without human intervention) by means of any appropriate equipment ;
- (b) whether in the course of activities carried on by any official, information is supplied with a view to its being stored or processed for the purposes of those activities by a computer operated otherwise than in the course of those activities, that information, if duly supplied to that computer, shall be taken to be supplied to in the course of those activities;
- (c) a document shall be taken to have been produced by a computer whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment.

Explanation : - For the purposes of this section, –

- (a) "computer" means any device that receives, stores and processes data, applying stipulated process to the information and supplying results of these process; and
- (b) any reference to information being derived from other information shall be a reference to its being derived therefrom by calculation, comparison or any other process.

---

# 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/issurer/ 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 international 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 forming messages relating to credit transfers transmitted over computer to computer telecommunications network<sup>1</sup>.]

**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

---

<sup>1</sup> See, *UNCITRAL LEGAL GUIDE ON ELECTRONIC FUNDS TRANSFERS*, United Nations, New York (1987).

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 easily 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.

## **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 committing 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.

- (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**

## **ANNEXURES**

		<b>Page</b>
<b>ANNEXURE 1</b>	<b>Governor's memorandum dated August 1, 1995 Constitution and Terms of Reference of the Committee.</b>	<b>133</b>
<b>ANNEXURE 2</b>	<b>Composition of Sub-Committees</b>	<b>136</b>
<b>ANNEXURE 3</b>	<b>Extract from the Code of Good Practice issued by the office of Fair Trading (U.K.)</b>	<b>138</b>
<b>ANNEXURE 4</b>	<b>Extract from the Code of Good banking Practice (1991) (UK)</b>	<b>147</b>
<b>ANNEXURE 5</b>	<b>Extract from the European Commission Recommendation on payment cards.</b>	<b>153</b>
<b>ANNEXURE 6</b>	<b>Extract of the Policies and Views of the U.K. Data Protection Registrar.</b>	<b>158</b>
<b>ANNEXURE 7</b>	<b>Extract from the U.K. Computer Misuse Act, 1990.</b>	<b>161</b>

गवर्नर  
GOVERNOR



भारतीय रिजर्व बैंक  
केन्द्रीय कार्यालय  
बंबई  
RESERVE BANK OF INDIA  
CENTRAL OFFICE  
BOMBAY

## MEMORANDUM

### Committee for proposing Legislation on Electronic Funds Transfer and other Electronic Payments

An efficient Payments System is crucial for growth and productivity in a developing economy. Electronic Communications system enables fast funds movement between two places, by way of message transmissions as against the conventional way of transferring funds through paper-based instruments like cheques, drafts etc. The Saraf Committee on Technology Issues relating to Payments System has, inter alia, recommended instituting Electronic Funds Transfer (EFT) System in India. The EFT system will require framing of regulations to decide on the finality of funds transfer at each stage. A Committee has, therefore, been set up to study all aspects relating to Electronic Funds Transfer and propose appropriate legislation. The members of the Committee will be :

1. Smt. K.S. Shere, Chairperson  
Principal Legal Adviser,  
Reserve Bank of India,  
Bombay.
2. Shri B.S. Sharma, Member  
Chief General Manager,  
Department of Government &  
Bank Accounts,  
Reserve Bank of India,  
Central Office,  
Bombay.

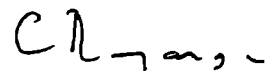
- |     |  |                  |
|-----|--|------------------|
| 3.  | Smt. Rama Ananthakrishnan,<br>Chief General Manager,<br>Department of Information Technology,<br>Reserve Bank of India,<br>Bombay. | Member           |
| 4.  | Shri K.R. Ganapathy,<br>General Manager,<br>Department of Information Technology,<br>Reserve Bank of India,<br>Bombay.             | Member           |
| 5.  | Shri O.P. Agarwal,<br>General manager,<br>Department of Banking Operations &<br>Development,<br>Reserve Bank of India,<br>Bombay.  | Member           |
| 6.  | Shri S. Venkatachalam,<br>Vice President,<br>Regulatory and Compliance Division,<br>Citibank,<br>Bombay.                           | Member           |
| 7.  | Shri K. Samdhani,<br>Deputy General Manager (Law),<br>Local Head Office,<br>State Bank of India,<br>Bombay.                        | Member           |
| 8.  | Shri Arjun Goswami,<br>Senior Legal Manager,<br>Standard Chartered Bank,<br>Bombay.  | Member           |
| 9.  | Shri V.K. Shah,<br>Law Officer,<br>Indian Banks' Association,<br>Bombay.   | Member           |
| 10. | Shri N.V. Deshpande<br>Additional Legal Adviser<br>Reserve Bank of India<br>Bombay.  | Member-Secretary |

The Terms of Reference of the Committee will be as under :

- (i) Defining the scope of "Electronic Funds Transfer" and determining the responsibilities and liabilities of the participants arising out of contractual obligations.
- (ii) Defining the trigger events that determine the finality and irrevocability of the transfer of funds at different stages like sender finality, settlement finality, receiver finality etc., including the scope for countermanding and money-back guarantees.
- (iii) Operational security; determination of liability in the event of operational failure at any stage.
- (iv) Defining measures to ensure security, integrity and efficiency of communication network linkages (eg. checksum, encryption, firewall etc.)
- (v) Definition of "Fraud" in electronic environment.
- (vi) The extent to which paper documents are mandatory vis-a-vis the contractual obligations.
- (vii) Consequences of bank failures and other systemic events - procedures to follow.
- (viii) admissibility of electronic media for the purpose of evidence, preservation period of electronic media etc.
- (ix) Cheque truncation.
- (x) Any other matter relating to Electronic Funds transfer such as securities transfer and other cash/credit/debit transactions through Electronic Funds Transfer at Point of Sale (EFTPOS) devices and computer/communication networks;
- (xi) A comprehensive fresh legislation to deal not only with EFT, but also for bringing changes required in the existing Acts such as Negotiable Instruments Act, Bankers' Book of Evidence Act, Securities and Contract Regulation Act (SCRA) etc.

The Committee will have a period of five months to prepare the draft Electronic Funds Transfer Act and also make recommendations on modification in existing legislative provisions.

August 1, 1995



(C. Rangarajan)  
Governor



---

## COMPOSITION OF SUB-COMMITTEES

---

### **I. The Sub-Committee for Short-Term Measures**

This Sub-Committee was formed to identify and consider the provisions of existing statutes, Regulations and Rules in which amendments would be required. The Sub-Committee will consist of :

- |    |   |           |
|----|---|-----------|
| 1. | Mr. V.K. Shah,<br>Law Officer, IBA                    | Chairman, |
| 2. | Mr. S. Venkatachalam,<br>Vice-President, Citibank, NA | Member    |
| 3. | Mr. K.R. Ganapathy,<br>GM, DIT, RBI                   | Member    |
| 4. | Mr. O.P. Agrawal,<br>GM, DBOD, RBI                    | Member    |

### **II. Sub-Committee for Long Term Measures,**

This Sub-Committee will go into the question whether there is any need for a separate comprehensive legislation. The Sub-Committee will undertake a study of comparative models of legal framework for EFT in some of the leading countries where electronic banking and EFT have already made some advancement. This Sub-Committee would consist of:

- |    |  |          |
|----|--|----------|
| 1. | Mr. Arjun Goswami<br>Head, Legal & Compliance,<br>Standard Chartered Bank. | Chairman |
| 2. | Mr. K.Samdhani,<br>DGM, Law, SBI.  | Member   |

- |    |  |        |
|----|--|--------|
| 3. | Smt. Rama Ananthakrishnan,<br>CGM, DIT, RBI.                                       | Member |
| 4. | Mr. B.S.Sharma,<br>CGM, DGBA, RBI.   | Member |
| 5. | Shri A.S.Khan,<br>Addl. Legal Adviser,<br>Ministry of Law,<br>Government of India. | Member |

The Member Secretary, Shri N.V.Deshpande will be associated with both the Sub-Committees and will co-ordinate the work of each of the Sub-Committees.

**EXTRACT FROM  
THE CODE OF GOOD PRACTICE ISSUED  
BY THE OFFICE OF FAIR TRADING (U.K.)  
SOURCE : Report of the Review Committee on Banking  
Services : law and Practice HMSO London (1989)**

---

**Electronic Funds Transfer (including Automatic Teller Machines)**

**Availability and disclosure of terms and conditions of use applicable to EFT transactions**

1. Card issuers should issue clear and unambiguous terms and conditions of use; in particular, the clauses which deal with the card holder's liabilities and responsibilities should be clearly and simply stated and highlighted in the text.
2. Card issuers should encourage their card holders to read and to be aware of the terms and conditions; copies should be readily available at all their branches, particularly when applications for EFT facilities are made by prospective card holders. Card issuers should provide a copy of the terms and conditions:
  - (a) on request; and
  - (b) with the notice of acceptance of the application for a card, or with the card/PIN, whichever is sooner.
3. Card issuers should advise their card holders to keep EFT receipts, check them against the appropriate entries in their periodic statements, and report any possible errors or unauthorised transactions promptly.
4. Card issuers should advise their card holders to report promptly any loss, theft or unauthorised use of a card. Card issuers should provide written acknowledgement of any such report.
5. Card issuers should allow customers to choose their own PIN. Customers should however be warned not to choose numbers which others might be aware of such as the day and month of their birthday.

6. Card issuers should warn card holders about the safeguarding of their PINS.
7. Before an EFT card is first used the card holder should have received documentation on:
  - (a) any charges for the issue or use of an EFT card and PIN, separate from activity or other charges applying to the account generally;
  - (b) the time taken for amounts to be debited from or credited to the card holder's account;
  - (c) the nature of any restrictions imposed by the card issuer on the use of the EFT card (including withdrawal and transaction limits) and an indication that merchants or other institutions may impose additional restrictions;
  - (d) a description of the types of transactions that may be made, and of the accounts that may be accessed, with the EFT card;
  - (e) a description of any credit facility which may be accessed by the card holder through an electronic terminal;
  - (f) the card holder's liability for unauthorised transactions;
  - (g) the procedure for reporting the loss or theft of an EFT card (including, in particular, the telephone number for reporting lost or stolen EFT cards outside of normal business hours); customers should be told whether or not a card issuer will accept notification of a lost or stolen card from a bank card notification and registration organisation;
  - (h) the means to activate error or dispute resolution processes (including the procedure for querying entries on a periodic statement);
    - (i) frequency of receipt of periodic statements;
  - (j) the card issuer's liability to the card holder in the event of the card issuer's failure to carry out a transaction with an EFT card because of machine malfunction or other cause; and
  - (k) the general nature of the written documentation received by the card holder recording a transaction through an electronic terminal.

## **Changing the terms and conditions of use**

8. Card issuers wishing to vary or modify the EFT terms and conditions to:
  - (a) impose or increase charges relating solely to the use of an EFT card and PIN, or the use of an additional or replacement card,
  - (b) increase a card holder's liability for losses relating to EFT transactions (subject to the liability limits established elsewhere under the Office's proposals), or
  - (c) adjust the periodic transaction limits applying to the use of an EFT card, should provide written notification to the card holder, and allow a period of notice of at least 30 days before the change takes effect.
9. Card issuers should advise other changes in advance through:
  - (a) notices on, or with, periodic account statements;
  - (b) notices on bank premises; and
  - (c) press advertisements.
10. Advance notice need not be given when changes are necessitated by an immediate need to restore or maintain the security of the system or individual accounts.
11. Card issuers should issue, if there have been a given number of changes in a 12 month period, a single document providing a consolidation of variations made to the terms and conditions over that period or a complete reprint of the existing terms and conditions.

## **Paper records of EFT transactions: receipts at electronic terminals**

12. A receipt should contain the following information:
  - (a) the amount of the transaction;
  - (b) the date of the transaction, and where possible, the time of the transaction;
  - (c) the type of transaction eg, "deposit", "withdrawal", "transfer", (codes may be used only if they are explained on the receipt);

- (d) an indication of the account(s) being debited or credited;
- (e) data that enable the card issuer to identify the customer and the transactions;
- (f) the general location of the terminal used to make the transactions or a number or code that enables that terminal to be identified;
- (g) in the case of EFTPOS terminal receipt, the name of the merchant to whom payment was made; and
- (h) in the case of accounts accessed at an ATM, the balance of the account where possible.

### **Paper records of EFT transactions: periodic statements**

- 13. Periodic statements should be provided at least every three months, provided that at least one transaction has taken place during that three months period. Card holders should also be offered the option of receiving more frequent periodic statements. That option should be given appropriate publicity at the time the account is opened. Statements should be available, at any time, at the request of the card holder.
- 14. The statement should show:
  - (a) in respect of each EFT transaction occurring since the previous statement -
    - the amount of the transaction;
    - the date the transaction was debited or credited to the account;
    - the type of transaction;
    - the receipt number, or other means, which will enable the account entry to be reconciled with a transaction receipt; and
    - in the case of an EFTPOS transaction, the name of the merchant to whom payment was made;
  - (b) any charges relating solely to the use of an EFT card and PIN (identified as a separate item);
  - (c) balance at the start and end of the period; and

- (d) the address or telephone number to be used for enquiries concerning the account or to report any errors in the statement.
15. Card issuers should be required to remind card holders by means of a notice on each statement, that all entries on statements be checked and that any apparent error or possible unauthorised transaction be promptly reported to the institution.

### **Liability for unauthorised transactions**

16. The liability of an EFT card holder for unauthorised use of his or her card should be limited to \$50 until the card issuer is notified of any loss, theft or other unauthorised possession of the card, after which the card holder should normally be under no further liability. However, the card holder may be made liable for any loss arising, before notice is given, from the use of his or her card by a person who obtained possession of it with his or her consent.
17. The card holder should not be liable if the card issuer did not provide him or her with a summary of his or her maximum liability for unauthorised transactions, before the card was first used.
18. The card holder should not be under a liability unless there are contained in the terms and conditions which were sent to him or her before the card was first used, the name, address and telephone number to whom notice, oral or in writing, of any loss, theft or other unauthorised possession can be notified.
19. The card issuer should provide an adequately manned facility for reporting the loss, theft or unauthorised use of a card by telephone at all times.
20. Subject to paragraph 21 below, it should be notice by telephone, and not any confirmatory notice in writing, which should be the effective notice for the purposes of reporting any liability relating to the loss, theft or unauthorised use of a card.
21. Notice to the card issuer should take effect when received but where it is given orally, and the agreement so requires, it should be treated as not taking effect if not confirmed in writing within seven days.
22. Card holders should not be responsible for losses that are caused by the fraudulent or negligent conduct of employees and agents of card issuers or merchants who are linked to the EFT system.
23. Card holders should not be responsible for losses relating to cards that are faulty, expired, or cancelled.

24. Card holders should not be responsible for losses occurring before they have received their card and/or PIN. In any dispute about the receipt of a card and/or PIN which was sent to a card holder by mail, the card issuer should not rely only on proof of delivery to the card holder's correct address as proof that the card was received by that person. Nor should the card issuer have any terms or conditions of use which deem a card or PIN sent to the card holder at that person's correct address to have been received by the card holder within a certain time after posting. [This paragraph stands only if the Office's proposal that cards and PINs should not be posted to customers, unless at their express request, is not adopted.]

## **Error and Dispute Resolution Procedures**

25. Card issuers should establish appropriate procedures to investigate transactions which are disputed by their card holders. They should establish arrangements to ensure that disputed transactions are recorded at a central location. Data should be available on the type and frequency of disputed transactions.
26. Card issuers should provide advice in their documentation on the means to activate the card issuer's dispute resolution processes.
27. If the card holder formally requests the activation of the dispute resolution processes they should be informed of all major stages in these processes and the length of time each stage is likely to take (preferably in writing). The card issuer should, within 30 days of receipt of a written complaint, notify the customer, in writing of the outcome of the investigation, including a summary of the reasons for the conclusion reached. Where it is not possible for the card issuer to complete its investigations within 30 days, the customer should be notified and given an indication of the likely delay in investigating the matter, and the reasons for that delay.
28. Where, as a result of the investigation of a complaint, a card issuer discovers that an error has been made (whether it was the error complained of or not), the card issuer should forthwith correct that error (including appropriate adjustments for interest and or charges) and notify the cardholder of the amount with which his or her account has been debited or credited as a result.
29. Where, as a result of an investigation of a complaint, a card issuer concludes that no error has occurred, it should promptly advise the card holder accordingly and should supply, at the request of the card holder, copies of any material on which the finding was based respecting, as necessary, security considerations and the confidentiality of other records.
30. Where a card holder who complains of an error is not satisfied with the results of the card issuer's investigation of the matter, that card holder should be advised that further external



avenues of dispute resolution exist, including, as appropriate, the Banking Ombudsman and Building Societies Ombudsman.

### **Deposits at electronic terminals**

31. Where, in relation to a deposit of funds at an electronic terminal, there is a discrepancy between the amount recorded as having been deposited and the amount recorded as having been received, the card holder should be notified of the difference as soon as possible and should be advised of the actual amount which has been credited to the nominated account.
32. The security of deposits received at electronic terminals should be the responsibility of the financial institution receiving the deposit from the time the transaction at the electronic terminal is completed (subject to verification of amount(s) deposited).

### **Networking Arrangements**

33. Card issuers should not be able to avoid any obligations owed to their card holders by reason only of the fact that they are party to a shared EFT system, and the another party to the system has actually caused the failure to meet the obligations.

### **Audit-trials**

34. Card issuers should ensure that their EFT systems generate sufficient records to enable transactions to be traced, checked and where an error has occurred, to be identified and corrected.

### **Privacy**

35. The following principles should be applied:
  - (a) the duties of confidentiality that apply to banks in respect of customer records should apply to all card issuers;
  - (b) no person other than an employee or agent of the card issuer which maintains the account, and the customer or any person authorised by the customer should have access through any electronic terminal to information concerning the customer's account;
  - (c) except where it is being operated by an employee or agent of the card issuer concerned, no electronic terminal should be capable of providing any information concerning a customer's account unless the request for information is preceded by the entry of the correct card/PIN combination for that account;

- (d) except where it is provided pursuant to a legal duty or responsibility, no information concerning the use of EFT services by a customer should be provided by any card issuer, except with the consent of that customer; and
  - (e) in particular, retailers should have no access to information about a customer's bank account other than a simple statement as to the availability or non-availability of funds for payment.
36. These principles should not nevertheless prevent a card issuer from giving information about the credit-worthiness of a card holder to a credit reference agency with the consent of that card holder.

### **Machine failure**

37. Card issuers should not seek to avoid liability, by means of exclusion clauses in their terms and conditions, for any reasonably foreseeable losses caused by the malfunctioning of any EFT system. (Exceptions to this rule are shown at paragraph 42 of the main paper.)

### **Provisions relating to the involvement of retailers etc.**

38. Since EFTPOS will involve parties other than banks and other card issuers (principally retailers, equipment suppliers, telecommunication companies and settlement and clearing bodies) it will be necessary for the proposed code to require the banks and the other card issuers to use all reasonable endeavours (principally by contractual means) to require retailers etc. to play their part in protecting customers' interests. The following matters will need to be covered as part of this protection.
39. There should be safeguards for retailers and others for the security and confidentiality of personal accounts.
40. Customers should be able to discreetly ascertain the level of funds in their accounts so as to avoid embarrassment at the till.
41. Wording on screens of refusals to accept payment by card should be as neutral as possible to avoid embarrassment to the card holder.
42. There should be adequate controls (essentially by card issuers, but also retailers and others) to avoid error and fraud.
43. Comprehensive information should be given to the customer about differing charges (if any) made by retailers for the various methods of payment.

44. Where a refund is made by the retailer for defective goods, the refund should be made by EFT, if the original purchase price was paid by EFT, unless the retailer and the customer agree that the refund should be made by another means.
45. Customers using an EFTPOS terminal should be given a paper receipt, the information in which is detailed at paragraph 29 of this Annex.

---

**EXTRACT FROM  
THE CODE OF GOOD BANKING PRACTICE (U.K.)  
SOURCE : Butterworths BANKING LAW Handbook,  
2nd Edn., London (1993)**

---

**Code of banking practice**

**I Introduction**

(1) The Code has been prepared by the British Bankers' Association (BBA). The Building Societies Association (BSA), and the Association for Payment Clearing Services (APACS).

(2) The Code is written to promote good banking practice. Specific services may have their own terms and conditions which will comply with the principles contained in the Code.

.....

.....

(4) The governing principles of the Code are:

- (a) to set out the standards of good banking practice which banks, building societies and card issuers will follow in their dealings with their customers;
- (b) that banks, building societies and card issuers will act fairly and reasonably in all their dealings with their customers;
- (c) that banks, building societies and card issuers will help customers to understand how their accounts operate and will seek to give them a good understanding of banking services;
- (d) to maintain confidence in the security and integrity of banking and card payment systems. Banks, building societies and card issuers recognise that their systems and technology need to be reliable to protect their customers and themselves.

- (5) The Code requires banks, building societies and card issuers to provide certain information to customers. This will usually be at the time when an account is opened. Information will also be available to customers from branches, if any, of the bank, building society or card issuer. Banks, building societies and card issuers will provide additional information and guidance about specific services at any time on request.
- .....

## **Customers and their cards**

### **Opening an account**

- (1) Card issuers will satisfy themselves about the identity of a person seeking to open an account or to obtain a card to assist in protecting their customers, members of the public and themselves against fraud and other misuse of the banking and card processing systems.
- (2) Card issuers will provide to prospective customers details of the identification needed.

### **Terms and conditions**

- (1) The written terms and conditions of a card service will be expressed in plain language and will provide a fair and balanced view of the relationship between the customer and the card issuer.
- (2) Card issuers will tell customers how any variation of the terms and conditions will be notified. Card issuers will give customers reasonable notice before any variation takes effect.
- (3) Card issuers should issue to their customers, if there are sufficient changes in a 12 month period to warrant it, a single document providing a consolidation of the variations made to their terms and conditions over that period.
- (4) Card issuers will publish changes to their interest rates in their branches or their stores or in the press or in the statement of account sent to card holders, or by all those methods when such changes are made with immediate effect.
- (5) Card issuers will tell customers the time it normally takes for a transaction to appear on their account and how frequently they can expect a statement.

## **Issue of cards**

- (1) Card issuers will issue cards to customers only when they have been requested in writing or to replace or renew cards that have already been issued.
- (2) Card issuers will tell customers if a card issued by them has more than one function. Card issuers will comply with requests from customers not to issue personal Identification Numbers (PINs) where customers do not wish to use the functions operated by a PIN.

## **Security of cards**

- (1) Card issuers will issue PINs separately from cards and will advise the PIN only to the customer.
- (2) Card issuers will tell customers of their responsibility to take care of their cards and PINs in order to prevent fraud. Card issuers will emphasise to customers that:
  - (a) they should not allow anyone else to use their card and PIN;
  - (b) they should take all reasonable steps to keep the card safe and the PIN secret at all times;
  - (c) they should never write the PIN on the card or on anything usually kept with it;
  - (d) they should never write the PIN down without making a reasonable attempt to disguise it.

## **Lost cards**

- (1) Card issuers will inform customers that they must tell their card issuers as soon as reasonably practicable after they find that:
  - (a) their card has been lost or stolen;
  - (b) someone else knows their PIN;
  - (c) their account includes an item which seems to be wrong.
- (2) Card issuers will tell customers, and will remind them at regular intervals on their statement or by other means, of the place and the telephone

number where they can give the details of a lost or stolen card at any time of the day or night. Card issuers will arrange for that telephone number to be included in British Telecom Phone Books.

- (3) Card issuers will act on telephone notification but may ask customers also to confirm in writing any details given by telephone.
- (4) Card issuers, on request, will inform customers whether they accept notification of loss or theft of a card from card notification organisations.
- (5) Card issuers on being advised of a loss, theft or possible misuse of a card or that the PIN has become known to someone else will take action to prevent further use of the card.

### **Liability for loss**

- (1) Card issuers will bear the full loss incurred;
  - (a) in the event of misuse when the card has not been received by the customer;
  - (b) for all transactions not authorised by the customer after the card issuer has been told that the card has been lost or stolen or that someone else knows the PIN (subject to (4) below);
  - (c) if faults have occurred in the machines, or other systems used, which cause customers to suffer direct loss unless the fault was obvious or advised by a message or notice on display.
- (2) Card issuers' liability will be limited to those amounts wrongly charged to customers' accounts and any interest on those amounts.
- (3) Customers' liability for transactions not authorised by them will be limited to a maximum of 50 in the event of misuse before the card issuer has been notified that a card has been lost or stolen or that someone else knows the PIN (subject to (4) below).
- (4) Customers will be held liable for all losses if they have acted fraudulently. They may be held liable for all losses if they have acted with gross negligence.
- (5) In cases of disputed transactions the burden of proving fraud or gross negligence or that a card has been received by a customer will lie with the card issuer. In such cases

card issuers will expect customers to co-operate with them in their investigations.

## **Records**

- (1) Card issuers will provide customers with a written record on their statement of account of all payments and withdrawals made. In addition, in many cases customers will be provided with an immediate written record.

## **Handling customers' complaints**

- (1) Each card issuer will have its own internal procedures for the proper handling of customers' complaints.
- (2) Card issuers will tell their customers that they have a complaints procedure. Customers who wish to make a complaint will be told how to do so and what further steps are available to them if they believe that the complaint has not been dealt with satisfactorily by the card issuer.
- (3) Card issuers subscribing to the Code should belong to one or other of the Banking and Building Societies Ombudsman Schemes, the Finance Houses Conciliation and Arbitration Scheme, the Consumer Credit Trade Association Arbitration Scheme or the Retail Credit Group Mediation and Arbitration Scheme. Card issuers will provide details of the applicable scheme to customers using such methods as leaflets or notices or in appropriate literature.

## **Glossary of terms**

This Glossary explains the meaning of words and phrases. They are not precise legal or technical definitions.

.....

### **PAYMENT CARDS**

A general term for any plastic card which may be used to pay for goods and services or to withdraw cash. A card may be used for more than one function.

### **COMMON EXAMPLES ARE:**

**Credit Card** - a card which allows customers to buy on credit and to obtain cash advances. Customers receive regular statements and may pay the balance in full, or in part usually subject to a certain minimum. Interest is payable on outstanding balances.



**Charge Card** - Similar to a credit card. It enables customers to pay for purchases, and in some cases to obtain cash advances. When the monthly statement is received the balance must be paid in full.

**Debit Card** - a card, operating as a substitute for a cheque, that can be used to obtain cash or make a payment at a point of sale. The customer's account is subsequently debited for such a transaction without deferment of payment.

**Budget Card** - Similar to a credit card but customers agree to pay a fixed amount into their card account each month.

**Store Card** - Similar to a budget card or charge card, but issued by particular companies or retail groups for use at their own outlets.

**Cash Card** - a card used to obtain cash and other services from an ATM (Automated Teller Machine/Cash Machine).

**Cheque Guarantee Card** - a card issued by a bank or building society which guarantees the payment of a cheque up to the amount shown on the card provided its conditions of use are followed.

**Eurocheque Card** - a specific cheque guarantee card which can be used either with special eurocheques to pay for goods or services, or by itself to withdraw cash from machines, in the UK and other countries.

**EXTRACT FROM  
THE EUROPEAN COMMISSION  
RECOMMENDATION ON PAYMENT CARDS**

**Source : Report of the Review Committee on Banking Services : Law  
and Practice HMSO London (1989)**

---

1. This Annex applies to the following operations:

- electronic payment involving the use of a card, in particular at point of sale;
- The withdrawing of banknotes, the depositing of banknotes and cheques, and connected operations, at electronic devices such as cash dispensing machines and automated teller machines;
- Non-electronic payment by card, including processes for which a signature is required and a voucher is produced, but not including cards whose sole function is to guarantee payment made by cheque;
- electronic payment effected by a member of the public without the use of a card, such as home banking.

2. For the purposes of this Annex the following definitions apply;

"Payment Device": a card or some other means enabling its user to effect operations of the kind specified in paragraph 1.

"Issuer": a person who, in the course of his business, makes available to a member of the public a payment device pursuant to a contract concluded with him.

"System provider": a person who makes available a financial product under a specific trade name, and usually with a network, thus enabling payment devices to be used for the operations aforesaid.

"Contracting holder": a person who pursuant to a contract concluded between him and an issuer holds a payment device.

"Company-specific card": a card issued by a retailer to his client, or by a group of retailers to their clients, in order to allow or facilitate, without giving access to a bank account, payment for purchases of goods or services exclusively from the issuing retailer or retailers, or from retailers who under contract accept the card.

3. (1) Each issuer shall draw up full and fair terms of contract, in writing, to govern the issuing and use of the payment devices he issues.
  - (2) Those terms of contract shall be expressed.
    - in easily understandable words and in so clear a form that they are easy to read;
    - in the language or languages which are ordinarily used for such or similar purposes in the regions where the terms of contract are offered.
  - (3) The terms of contract shall specify the basis of calculation of the amount of the charges (including interest), if any, which the contracting holder must pay to the issuer.
  - (4) The terms of contract shall specify:
    - Whether the debiting or crediting operations will be instantaneous and, if not, the period of time within which this will be done;
    - for those operations which lead to invoicing of contracting card-holder, the period of time within which this will be done.
  - (5) The terms of contract shall not be altered except by agreement between the parties; however, such agreement shall be deemed to exist where the issuer proposes an amendment to the contract terms and the contracting holder, having received notice thereof, continues to make use of the payment device.
4. (1) The terms of contract shall put the contracting holder under obligation vis-a-vis the issuer:
    - (a) to take all reasonable steps to keep safe the payment device and the means (such as a personal identification number or code) which enable it to be used;
    - (b) to notify the issuer or a central agency without undue delay after becoming aware;

- of the loss or theft or copying of the payment device or of the means which enable it to be used;
  - of the recording on the contracting holder's account of any unauthorised transaction;
  - of any error or other irregularity in the maintaining of the account by the issuer;
- (c) not to record on the payment device the contracting holder's personal identification number or code , if any, nor to record those things on anything they are likely to be lost or stolen or copied together;
- (d) not to countermand an order which he has given by means of his payment device.
- (2) The terms of contract shall state that provided the contracting holder complies with the obligations imposed upon him pursuant to subparagraphs (a), (b) first indent, and (c) of paragraph 4(1), and otherwise does not act with extreme negligence, or fraudulently, in the circumstances in which he uses his payment device he shall not, after notification, be liable for damage arising from such use.
- (3) The terms of contract shall put the issuer under obligation vis-a-vis the contracting holder not to disclose the contracting holder's personal identification number or code or similar confidential data, if any, except to the contracting holder himself.
5. No payment device shall be despatched to a member of the public except in response to an application from such person' and the contract between the issuer and the contracting holder shall be regarded as having been concluded at the time when the applicant receives the payment device and a copy of the terms of contract accepted by him.
6. (1) In relation to the operations referred to in paragraph 1, issuers shall kept, or cause to be kept, internal records which are sufficiently substantial to enable operations to be traced and errors to be rectified. To this end, issuers shall make the requisite arrangements with the system providers, as necessary.
- (2) In any dispute with a contracting holder concerning an operation referred to in the first, second and fourth indents of paragraph 1 and relating to liability for an unauthorised electronic fund transfer, the burden of proof shall be upon the issuer to

show that the operation was accurately recorded and accurately entered into accounts and was not affected by technical breakdown or other deficiency.

- (3) The contracting holder, if he so requests, shall be supplied with a record of each of his operations, instantaneously or shortly after he has completed it' however, in the case of payment at point of sale the till receipt supplied by the retailer at the time of purchase and containing the references to the payment device shall satisfy the requirements of this provision.
7.
  - (1) Vis-a-Vis a contracting holder the issuer shall be liable, subject to paragraphs 4 and 8:
    - for the non-execution or defective execution of the contracting holder's operations as referred to in paragraph 1, even if an operation is initiated at electronic devices which are not under the issuer's direct or exclusive control;
    - for operations not authorised by the contracting holder.
  - (2) Save as stated in paragraph 7(3) the liability indicated in paragraph 7(1) shall be limited as follows:
    - in the case of non-execution or defective execution of an operation, the amount of the liability shall be limited to the amount of the unexecuted or defectively executed operation;
    - in the case of an unauthorised operation, the amount of the liability shall extend to the sum required to restore the contracting holder to the position he was in before the unauthorised operation took place.
  - (3) Any further financial consequences, and, in particular, questions concerning the extent of the damage for which compensation is to be paid, shall be governed by the law applicable to the contract concluded between the issuer and the contracting holder.
8.
  - (1) Each issuer shall provide means whereby his customers may at any time of the day or night notify the loss, theft or copying of their payment devices; but in the case of company specific cards these means of notification need only be made available during the issuer's hours of business.

- (2) Once the contracting holder has notified the issuer or a central agency, as required by paragraph 4(1)(b), the contracting holder shall not thereafter be liable; but this provision shall not apply if the contracting holder acted with extreme negligence or fraudulently.
- (3) The contracting holder shall bear the loss sustained, up to the time of notification, in consequence of the loss, theft or copying of the payment device, but only up to the equivalent of 150 ECUS for each event, except where he acted with extreme negligence or fraudulently.
- (4) The issuer, upon receipt of notification, shall be under obligation, even if the contracting holder acted with extreme negligence or fraudulently, to take all action open to him to stop any further use of the payment device.

---

**EXTRACT OF  
THE POLICIES AND VIEWS OF  
THE UK DATA PROTECTION REGISTRAR  
SOURCE : Report of the Review Committee on Banking  
Services : Law and Practice HMSO, London (1989).**

---

This statement of policy was released for publication on 3 December 1986.

The Data Protection Act received Royal Assent on 12 July 1984. It is the first piece of legislation in the United Kingdom to address the use of computers.

The Act is designed to allow the United Kingdom to ratify the Council of Europe "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data".

The Convention has two objectives:

- to protect individuals in circumstances where information about them is processed automatically;
- to facilitate a common international standard of protection for individuals, such that the free flow of information across international boundaries can proceed properly.

The Data Protection Act is therefore concerned with information about individuals which is processed by computer (personal data). It introduces significant new rights for individuals to whom that information relates (Data Subjects). Such an individual generally has the right to:

- claim compensation for damage any asy associated distress arising from the loss or unauthorised destruction or disclosure of persosnal data relating to him or her, or arising from the inaccuracy of such data:
- have a copy of the information about him or

her which is held in computers (the "subject access" right) ;

- challenge the information if he or she believes it to be wrong and, and where appropriate, have it corrected or erased.

The Act places obligations on those who use personal data in computers (Data Users). They must be open about that use (through the Data Protection Register) and follow sound and proper practices (the Data Protection Principles). Computer Bureaux have more limited obligations mainly concerned with maintaining appropriate security around personal data.

The Act establishes the Data Protection Registrar in a position of independence reporting directly to Parliament. The Registrar is charged with administering the Act and supervising its operation. His decisions are subject to the supervision of the Courts and the Data Protection Tribunal, which is also established by the Act.

To achieve the objectives of the act, the Registrar will:

- (a) Underpin the rights given to individuals and resolve the problems of aggrieved individuals, by providing an effective ombudsman service;
- (b) promote the good practice contained in the Data Protection Principles, by encouraging and supporting the development and adopting of appropriate codes of practice, procedures and techniques by Data Users and their representative organisations;
- (c) establish openness in the use of personal data by developing and promulgating a Registrar of Data User activities as prescribed by the Act;
- (d) seek to obtain the proper implementation of the Act at minimum complexity and cost to Data Subjects and Data Users.

The Registrar will:

- (a) Liaise with organisations representing individuals and computer users so as to obtain the best understanding of the requirements and attitudes of those affected by the Act;
- (b) positively inform and guide Data Subjects and Data Users on the rights and requirements of the Act;
- (c) resolve complaints by;
  - using a mediated solution where this achieves a result properly supportive of the Act and satisfactory to all parties;
  - using the enforcement provisions of the Act where a mediated solution is not appropriate or attainable.



- (d) obtain compliance by Data Users with the requirements of the Act through:
  - guidance where there is a genuine lack of knowledge or confusion;
  - using the offence provisions where the Act is being ignored or flouted;
- (e) maintain a watching brief on matters pertinent to data protection in the United Kingdom and internationally, in particular those matters relating to the Council of Europe Convention;
- (f) monitor the operation of the Act and report to Parliament on this.

The positive nature of the Act is apparent. There is wide agreement with the news rights the Act confers on individuals. Ethical, practical Data Users would not argue against the good practice generally stated in the Data Protection Principles.

The Act causes change - improved rights, more open attitudes, sounder practices - change throughout the United Kingdom. It would be foolish to expect such change to be achieved quickly or without cost, or for the achievement to be consistently even in effect across the national community.

The Act breaks new ground. It is also concerned with computing, an all-pervasive and rapidly changing technology. In such circumstances the Act may not work precisely as foreseen. As experience is gained of the operation of the Act in practice, this will be reported to Parliament. Such reports may, at times, suggest that modifications to the Act may be appropriate.

The Data Protection Act should raise public confidence in computing and improve practice in computing installations. Both these factors will benefit all of us as individuals. They will not prejudice the sound and ethical use of computers. On the contrary, there should be a more favourable climate for computer use and a more effective operation of computer systems. Data Users should benefit from this Act as well as individuals.

---

**EXTRACTS FROM  
THE U.K. COMPUTER MISUSE ACT 1990  
(SECTIONS 1, 2, 3 AND 12)**

---

**Section 1**

1. Unauthorised access to computer material-- 1) A person is guilty of an offence if -
  - a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer;
  - b) the access he intends to secure is unauthorised; and
  - c) he knows at the time when he causes the computer to perform the function that the is the case.
2. The intent a person has to have to commit an offence under this section need not be directed at -
  - a) any particular program or data;
  - b) a program or data of any particular kind; or
  - c) a program or data held in any particular computer.
- 3) A person guilty of an offence under this section shall be liable on summary conviction to imprisonment for a term not exceeding six months or to a fine not exceeding level 5 on the standard scale or to both.

**Section 2**

Unauthorised access with intent to commit or facilitate commission of further offences, --

- 1) A person is guilty of an offence under this section if he commits an offence under Section 1 above ("the unauthorised access offence") within intent --

- a) to commit an offence to which this section applies; or
  - b) to facilitate the commission of such an offence (whether by himself or by any other person); and the offence he intends to commit or facilitate is referred to below in this section as the further offence.
- 2) This section applies to offences--
- a) for which the sentence is fixed by law; or
  - b) for which a person of twenty-one years of age or over (not previously convicted) may be sentenced to imprisonment for a term of five years (or, in England and Wales, might be so sentenced but for the restrictions imposed by section 33 of the Magistrates' Courts Act 1980).
- 3) It is immaterial for the purposes of this Section whether the further offence is to be committed on the same occasion as the unauthorised access offence or on any future occasion.
- 4) A person may be guilty of an offence under this section even though the facts are such that the commission of the further offence is impossible.
- 5) A person guilty of an offence under this section shall be liable (a)--
- a) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both; and
  - b) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.

### **Section 3**

#### **Unauthorised modification of computer material -**

- 1) A person is guilty of an offence if --
- a) he does any act which causes an unauthorised modification of the contents of any computer; and
  - b) at the time when he does the act he has the requisite intent and the requisite knowledge.
- 2) For the purposes of subsection (1)(b) above the requisite intent is an intent to cause a modification of the contents of any computer and by so doing -

- a) to impair the operation of any computer;
  - b) to prevent or hinder access to any program or data held in any computer; or
  - c) to impair the operation of any such program or the reliability of any such data.
- 3) The intent need not be directed –
- a) any particular computer;
  - b) any particular program or data or a program or data of any particular kind; or
  - c) any particular modification or a modification of any particular kind.
- 4) For the purposes of subsection (1)(b) above the requisite knowledge is knowledge that any modification he intends to cause is unauthorised.
- 5) It is immaterial for the purposes of this section whether an unauthorised modification or any intended effect of it of a kind mentioned in subsection (2) above is, or is intended to be, permanent or merely temporary.
- 6) For the purposes of the Criminal Damage Act 1971 a modification of the contents of a computer shall not be regarded as damaging any computer or computer storage medium unless its effect on that computer or computer storage medium impairs its physical condition.
- 7) A person guilty of an offence under this section shall be liable (a) –
- a) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both; and
  - b) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.

## Section 12

Conviction of an offence under Section 1 in proceedings for an offence under Section 2 or 3 –

1) If on the trial on indictment of a person charged with –

- a) an offence under section 2 above; or
- b) an offence under section 3 above or any attempt to commit such an offence; the jury find him not guilty of the offence charged, they may find him guilty of an offence

under Section 1 above if on the facts shown he could have been found guilty of that offence in proceedings for that offence brought before the expiry of any time limit under section 11 above applicable to such proceedings.

- 2) The Crown Court shall have the same powers and duties in relation to a person who is by virtue of this section convicted before it of an offence under section 1 above as magistrates' court would have on convicting him of the offence.
- 3) This section is without prejudice to section 6(3) of the Criminal Law Act 1967 (conviction of alternative indicatable offence on trial on indictment).
- 4) This section does not extend to Scotland.