ELECTRONIC BANKING: EMERGING INTERNATIONAL LAW

DISSERTATION SUBMITTED TO JAWAHARLAL NEHRU UNIVERSITY
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR
THE AWARD OF THE DEGREE OF

MASTER OF PHILOSOPHY

PARITOSH KUMAR

INTERNATIONAL LEGAL STUDIES DIVISION
CENTER FOR STUDIES IN DIPLOMACY INTERNATIONAL
LAW AND ECONOMICS
SCHOOL OF INTERNATIONAL STUDIES
JAWAHARLAL NEHRU UNIVERSITY
NEW DELHI-110067
INDIA
2001

JAWAHARLAL NEHRU UNIVERSITY
SCHOOL OF INTERNATIONAL STUDIES

Telegram : JAYENU
Telex : 031-73167 JNU IN
Telephones : 667676/ 667557/ 418,408
Fax : 91-11-686-5886

Centre for Studies in Diplomacy
International Law & Economics

20th July 2001

Certificate

This is to certify that the dissertation entitled ***"Electronic Banking: Emerging Interantional Law"***, submitted by **Paritosh Kumar** is in partial fulfillment of requirement for the degree of **Master of Philosophy** of this University. It is his original work and may be placed before the examiners for evaluation. This dissertation has not been submitted for the award of any other degree of this University or any other University.

K D Kapoor
PROF. K.D. KAPOOR
Chairperson

B.S. Chimni
Prof. B.S.CHIMNI
Supervisor

ACKNOWLEDGEMENTS

Though I did manage to venture into a territory unknown, it was full of surprises and learning experiences on the whole. Firstly, I was struck by the extent of usage, penetrable powers and scope of e-banking. Then my advances were limited by the knowledge that the spread of e-banking has by far outpaced laws that are supposed to govern its transactions. And finally it was this very fact that made the work more worthwhile and rewarding.

I am extremely grateful to my professor and guide, Prof. B.S. Chimni, a literary barometer for his scholarly insights into this work and also for his patience with my ignorance.

I would also like to thank Prof. V.S. Mani, Mr. D.S. Mohil, Prof. Y.K. Tyagi, and Asso. Prof. Bharat Desai for their support and guidance.

I am also grateful to Prashant, Anil, Pallavi, Anand, Tanay, Sanjeev, Sanu and my classmates for all their help.

I extend very special thanks to Medha & Dobby, who took time from their work to see this humble beginning to its desired end. They did a magnificent and speedy job, I am grateful to them for making this dissertation possible.

And finally to my parents, brothers and sisters, to whom nothing I have written or could write could express what I owe. It is to them that I dedicate this work.

Paritosh Kumar

J.N.U. 20th July

CONTENTS

ABBREVIATIONS

ABA-American Bar Association.

ACH-Automated Clearing House.

BIPS-Bank Internet Payment System.

BIS- Bank for International Settlements.

BSA-Banking Secrecy Act.

CBDT – Central Board of Direct Taxes.

CFAA- Computer Fraud and Abuse Act.

CPSS- Committee on Payment and Settlement System.

DOT – Department of Telecommunications

EC-European commission.

ECPS-Electronic Communications Privacy Act.

ECS-Electronic Clearing Services.

EDI-Electronic Data Interchange.

EDIFACT- Electronic Data Interchange for Administration Communication and Transport.

EFT- Electronic Fund Transfer.

EU- European Union.

FATF-Financial Action Task Force.

FCBA- Fair Credit billing Act.

FCRA-Fair Credit Reporting Act.

FinCen-Financial Crimes Enforcement Network.

FSTC-Financial Services Technology Consortium.

GUIDEC-General Usage of Internationally Digitally Ensured Commerce.

HTTP- Hyper Text Transfer Protocol.

ICC-International Chamber of Commerce.

IT- Information technology.

OECD-Organization for Economic Co-Operation and Development.

RBI- Reserve Bank of India.

SET-Secure Electronic Transaction.

S-HTTP-Secure Hyper Text Transfer Protocol.

SSL-Secure Socket Layer.

SWIFT-Society for Worldwide Interbank Financial Telecommunications.

TILA-Truth in Lending Act.

UCC-Uniform Commercial Code.

UCITA-Uniform Computer Information Act.

UCTA-Uniform Electronic Transactions Act.

UKDPA-United Kingdom Data Protection Act.

UNCITRAL-United Nations Commission on International Trade Law.

Chapter - I

Introduction

CHAPTER I

INTRODUCTION

Technological developments, particularly in the area of telecommunication and information technology, are revolutionizing the way business is done. Electronic commerce is now thought to hold the promise of a new commercial revolution by offering an inexpensive and direct way to exchange information and to sell or buy products and services. This revolution in the market place has set in motion a revolution in the banking sector for the provision of a payment system that is compatible with the demands of the electronic market place.

Electronic banking, also known as Electronic Fund Transfer (EFT), uses computer and electronic technology as a substitute for checks and other paper transactions. EFT is initiated through devices such as cards or codes that one uses to gain access to one's account. A number of electronic payment systems, sometimes referred to as "electronic money", are under development for simplifying purchases online.

The two fundamental aspects of electronic banking are the nature of the delivery channels through with activities are pursued, and the means of computer to gain access to those channels.[1] Currently, widely used access devices through which electronic banking products and services can be provided to customers include point of sale terminals, automated teller machines, telephones, personal computers, smart cards and other devices.

[1] Risk Management for Electronic Banking and Electronic Money Activities, Basle Committee on Banking Supervision, Basle, 1998, available at http://www.bis.org/publ/bess.35.pdf.

The electronic payment system can be segmented into three broad categories:[2]

1) Banking and financial payments

- Large-scale or wholesale payments (e.g. bank-to-bank transfer)
- Small-scale or retail payments (e.g. automated teller machines and cash dispensers).
- Home banking (e.g. bill payment).
- Mobile banking

2. *Retailing payments*

- Credit cards (e.g. Visa or Master Card)
- Private label credit/debit cards (e.g. J.C. Penney card)
- Charge Cards (e.g. American Express)

3. *On-line electronic commerce payments*

- Token-based payment systems
- Electronic cash (e.g. DigiCash)
- Electronic checks (e.g. NetCheque)
- Smart cards or debit cards (e.g. Mondex Electronic Currency Card)
- Credit card-based payment systems.
- Encrypted credit cards (e.g. world wide web form-based encryption].
- Third-party authorization numbers (e.g. First Virtual)

[2] Ravi KalaKota and Andrew. B. Whinston, *Frontiers of Electronic Commerce*, (Massachusetts, 2000), p. 298.

In line with global trends, banking business in India too has been undergoing tremendous changes. The first step in the evolutionary process has been the gradual deregulation of the financial sector, which commenced in the 1990's. After that the use of "Information Technology" in banking has grown up tremendously. The development and use of communication networks has also helped the banking industry to gain in terms of improved bank services. It started with BANKNET network, a leased line terrestrial network connecting seven major cities. Then came the Shared Payment Network System (SPNS) of ATMs of Indian Banks Association in Mumbai. A landmark development came with the setting up of the INFINET (Indian Financial Network) - a Wide Area Satellite based network using VSAT technology in June, 1999 at the Institute for Development and Research in Banking Technology, Hyderabad. Electronic payment products such as electronic clearing service (credit and debit) are becoming increasingly popular with corporates and general public. The Reserve Bank and other banks, responding to the needs of business entities, have been offering electronic clearing service products.

Although it is evident that the electronic revolution has commenced in India, widespread electronic banking may be several years away. At present there are four major banking laws in India governing the banking business. These are: The Reserve Bank of India Act 1934, the Banking Regulation Act 1949, the Bankers Book Evidence Act 1891, and the Negotiable Instrument Act 1881. These are supported by other basic legislations like the Contract Act 1872, the Partnership Act 1932, the Sales of Goods Act 1930, the Consumer Protection Act 1986, Income Tax Act 1961, and the MRTP Act 1969. It would be necessary and worthwhile to reform the existing Indian banking law regime in the light of concerns raised by electronic banking. Recently there have been some reforms in Indian law. The Information Technology Act, 2000 is a step in this direction. It recognizes e-commerce, digital signature and electronic records. Some provisions of the Indian Evidence Act, the Indian Penal Code, the Banker's Book Evidence Act and the Reserve Bank of India Act have also been amended. But these are only e-commerce specific. So far as electronic banking is concerned one has to look beyond the Information Technology Act 2000. However various committees[3] have been constituted to look into different issues and many of them have submitted their report. So in near future legislation on these issues are expected.

CURRENT STATE OF INTERNATIONAL LAW

The big issue facing electronic banking is the absence of a clear-cut regulatory framework; both nation-wide and worldwide. This is the major reason why many business houses and consumers lack confidence in electronic banking. Since many issues like digital signature, security measures, criminal laws, money laundering etc. has a global impact, the issues to be solved require a global perspective and a global effort. There are international bodies and for a pondering over these issues to reach a universal solution.

The United Nations Commission on International Trade Law (UNCITRAL) prepared the *Legal Guide on Electronic Funds Transfer 1986*[4]. It explored the legal issues that would have to be faced in moving from a paper based to an electronic funds transfer system. Subsequently, it came up with M*odel Law on International Credit*

[3] Like Saraf Committtee Report on Technology Issues, Shere Committee on Electronic Fund Transfer (EFT) to propose legislation, Narasimhan Committee – II onBanking Sector Reforms has in its report dealth with, the issues in technology up-gradation, Vasudevan Committee Report on Technology Upgradation and Dandekar Committee on Legal Issues in Electronic Banking.

[4] A/CN. 9/SER.. B/1, Sales No. E.87. V. 9.

Transfer 1992.[5] As indicated by its title, and in contrast to the Legal Guide, the Model Law applies to credit transfers. It does not apply to debit transfers, even when made in electronic form. Some of the issues related to electronic banking have also been covered in the *UNCITRAL Model Law on Electronic Commerce (1996).*[6] The *Model Law* provides, among other things, that where the law requires a signature, that requirement could be met electronically if the electronic signature provides a link between the signer and the record (called the 'data message' in the *Model Law*) and evidence of intent to be associated with the record, both to be sufficiently reliable for the purpose of the record in the circumstances.

Since the adoption of the *Model Law*, the *UNCITRAL* has constituted a Working Group to frame guidelines for legislation on these issues. To name a few, *OECD* regarding certification processes, digital authentication and certification technology, the applicability of the certification process, allocation of risk and liabilities in the use of certification techniques and certification through registries and incorporation by reference and it on enactment stage.[7]

The Organization for Economic Co-operation and Development (OECD) has come up with a number of guidelines on different aspects and has thus provided a framework for nations. These include: *Guidelines on the Protection of Privacy and Trans -border Flows of Personal Data (1980)*[8], *Guidelines for Cryptography Policy,*[9]*(1997) Guidelines for the Security of Information System.*[10] *Inventory of*

[5] UN Commission on International Trade law, Year Book, Vol. XXIII: 1992 (New York, 1994). Pp. 413-17.

[6] General Assembly Resolution 51/162 of 16th Dec. 1996.

[7] Draft Guide to Enactment of the UNCITRAL Model Law on Electronic Signature, A/CN. 9/WG.IV/wp.88, March 2001.

[8] Guideline is available at, http://www.oecd.org/dsti/sti/it/ec/act/paris-ec/pdf/progrep-e.pdf.

[9] Guideline is available at, http://www.oecd.org/

[10] C (92) 188/Final, Nov. 1992.

Controls on *cryptography Technology,*[11] and *Inventory of Approaches to Authentication and Certification in a Global Networked Society.*[12] Apart form this it has worked in the field of taxation too.[13] However, it may be noted, that OECD guidelines are not binding.

In the field of money laundering problem the *Financial Action Task Force* has done a commendable job.[14]

The European Commission (EC) has also worked on different issues relating to electronic banking. In 1998, EC came up with draft *EC Directive on a Common Framework for Electronic Signature.*[15] Other relevant directives are: *Transparency Directive (1998)*[16] *Distance contract Directive (1996),*[17] *Database Directive (1996),*[19] *Data Protection Directive*[20]and draft *Directive on Electronic Money.*[21]Then there is *European Electronic Data Interchange (EDI) Agreement,*[22]which *United Nations Economic Commission for Europe* adopted in 1995. All these legislations have helped in regulating electronic banking and have prevented utter confusion.

Apart from these organizations, *the Bank for International Settlement (BIS)* [23]has prepared various reports with the help of *Committee on Payment and Settlement system* and the *Basle Committee on Banking Supervision.* These reports have examined

[11] DSTI / ICCP/REG (98) 4/Final, Jan 1999.

[12] Dsti/iccp/reg [98] rev3,SEP 1998.

[13] Electronic Commerce:The Challenges to Tax Authorities and Taxpayers,1997,available at, http:// www.

[14] FATF Annual Report [1999-2000]is available at , http:// www.oecd.org/fatf.

[15] O.J. 98/C325/04(23/10/98)

[16] Directive 98/34/EC, June 98, OJL 204, 1998 as amended by the Directive 98/48/EC, July 1998, OJL 217.

[17] Directive 97/7EC, May 1997, OJL 144, 1997.

[19] Directive 96/9/EC, March 1996,OJL77,1996.

[20]Directive 95 /46/EC, October 1995, OJ23. 11.19.95 nol.281

[21] European Commission Proposal for a Directive on the taking-up, the pursuit and the prudential supervision of the business of electronic money institution of July 1998. available at, http://europa.eu.int/ISPO/e-commerce /legal/document/52000 ag 0008-em.pdf

[22] 1994 OJL338/98

[23] BIS various reports are available at,http://www.bis.org/publ

various legal, policy and technical issues and have provided suggestions.

The International Chamber of Commerce has come up with *Uniform Rules for Interchange of Trade Data by Tele-transmission*[24]. It has also drafted the *General Usage of International Digitally Ensured Commerce (GUIDEC)*[25]. All these works have had a major impact on the development of electronic banking specific laws.

STATEMENT OF THE PROBLEM

There are a variety of legal and policy issues that are involved with electronic banking. International organizations and states are seeking to address these. One of the areas is that of criminal laws. The most critical issues in considering the application of criminal law is whether computer related conduct should be regarded as requiring technology specific legislation or whether it might be regulated through the application of more general criminal law provisions. Another area is that of money laundering for perhaps the highest hurdle facing an anonymous e-cash system is the potential to facilitate illegal money laundering.[26] A third area is that of tax evasion. E-cash makes it quite easy for individuals to store vast sums of money in offshore accounts- that is, on computers located outside the concerned States and thus hiding income to avoid paying income taxes. A fourth area is that of the law of evidence. Here the problem is of admissibility of computer-generated records, which are capable of being tampered easily. A fifth area relates to security issues, which are a major source of concern for every one both inside and outside the banking industry. The issues are authentication and non-

[24] ICC Publication No.452 ofJan,1998.

[25].FullPublication is available at, http://www.iccwbo.org/cust/html/guidec./.20./.20 living./.20 documents.htm

[26] Money laundering means hindering attempts to trace illegally acquired cash by passing through ostensibly legitimate commercial transactions, Eric Huges, Address before the seminar in law, Internet, and Society at Harvard Law School (Apr. 1.1996).

repudiation, integrity and privacy. In fact security is required at all phases of information cycle i.e. gathering, creating, processing, storing transmitting and deleting.[27] Next, there is the problem of appropriate banking and financial regulations. Here the question is whether existing banking or other regulations apply to e-money arrangements? What is the status of e-money? Who should issue e-money? Whose law will apply in case of dispute? Other such issues are related with clearing and settlement as well as liquidity and stability. Apart from this there is whole lot of risk associated with electronic payment system, i.e. operational risk, reputation risk and legal risk. There is also problem attached with consumer protection,[28] as to how law should develop to provide consumers effective protection or should it be left to the industry or whether alternative dispute resolution mechanisms should be developed to tackle consumer issues, finally, there are issues related to contract terms and enforceability in the new on line environment.

SCOPE OF THE STUDY

The study mainly examines legal and policy issues attached to electronic banking and work done by international organizations and states. The second chapter provides a brief introduction to the evolution of electronic banking. The third chapter focuses on the legal issues related to electronic banking. The fourth chapter deals with observations, declarations and model legislations of international organizations such as UNICITRAL, EC, ECE, OECD, BIS, Group of Ten Countries, FATF. It also contains a comparative study of U.S.A., U.K., and India. The fifth chapter contains the conclusions of the study.

[27] The G-10 Deputies Report on Electronic Money – Consumer Protection, Law Enforcement, Supervisory and Cross – border Issues, (Basle, April 1997), available at http://www.bis.org/publ/ gten 01.pdf.

[28] Security of Electronic Money, Committee on Payment and Settlement System , available at http://www.bis.org/publ/cpss18.pdf.

Chapter - II
Electronic Banking an Overview

CHAPTER II

ELECTRONIC BANKING AN OVERVIEW

In this chapter we are going to discuss about the evolution of electronic banking and electronic money, how it functions, how it is different from traditional banking and the different types of electronic payment systems. Electronic banking refers to the provision of retail and small value banking products and services through electronic channels. Such products and services can include deposit taking, lending, account management, the provision of financial advice, electronic bill payment and the provision of other electronic payment products and services such as electronic money.[1]

DIFFERENT ASPECTS OF ELECTRONIC BANKING

Two fundamental aspect of electronic banking are the nature of the delivery channels through which activities are pursued, and the means for computer to gain access to those channels. Common delivery channels include "closed" and "open" networks. "Closed networks" restrict access to participants (financial institutions, consumers, merchants, and third party service providers) bound by agreements on the terms of membership. "Open networks" have no such membership requirements. Currently, widely used access devices through which electronic banking products and services can be provided to customers include point of sale terminals, automatic teller machines, telephones, personal computers, smart cards and other devices.

[1] Risk Management for Electronic Banking and Electronic money Activities, Basle Committee on Banking Supervision, (Basle, March 1998) , p-3, available at, http://www.bis.org/publ/bcbs35.pdf.

E banking can be separated into two streams: one is e-money products, mainly in the form of stored value product, the other is electronic delivery channel products or access products. The latter are products that allow consumers to use electronic means of communication to access conventional payment services, for example, use of a standard personal computer and a computer network such as the Internet to make a credit card payment or to transmit instructions to make funds transfers between bank accounts.

Electronic money refers to "stored value" or prepaid payment mechanisms for executing payments via point of sale terminals direct transfers between two devices or over open computer networks such as the Internet.[2] Here record of the funds or "value" available to a consumer is stored on an electronic device in the consumer's possession. The electronic value is purchased by the consumer (for example, in the way that other prepaid instruments such as traveler's check might be purchased and is reduced whenever the consumer uses the device to make purchase. Stored value products include "hardware" or "card-based" mechanisms (also called "electronic purses"), and "software" or "network-based" mechanisms (also called "digital cash"). Stored value card can be "single-purpose" or "multi-purpose"[3]. Single-purpose cards (e.g., telephone cards) are used to purchase

[2] Several official bodies have each issued their own definition of electronic money. But a precise definition of electronic money is difficult to provide, in part because technological innovations continue to blur distinction between forms of prepaid electronic mechanism, see, The G-10-Deputies Report on Electronic Money - Consumer Protection, Law enforcement, Supervisory and Cross Border Issues, (Basle, April ,1997) , available at http://www.bis.org/publ/gten01.pdf.

[3] Stored value card may be characterized by the use of a magnetic stripe or a computer chip embedded in the card. A plastic card with an embedded computer chip (known as a 'smart card') may perform stored value applications, in addition to other functions such as debit and credit applications. Ibid.

one type of good or service, or products from one vendor; multi-purpose cards can be used for a variety of purchases from several vendors.[4]

Bank may participate in electronic money schemes as issuers, but they may also perform other functions. These include distributing electronic money issued by other entities; redeeming the proceeds of electronic money transactions for merchants; handling the processing, clearing and settlement of electronic money transactions; and maintaining records of transactions.

The advent of electronic payment can be traced back to 1918, when the Federal Reserve banks of the USA first moved currency via telegraph.[5] Electronic payment systems exist in a variety of forms, which can be divided into two groups.[6]

1. Wholesale payment systems and 2. Retail payment systems.

Wholesale payment system exists for non-consumer transactions. High-value wholesale payments flow through the three major interbank funds transfer systems: CHIPS, SWIFT and Fedwire. *Retail electronic payment systems* encompass those transactions involving consumers. These transactions involve the use of such payment mechanisms as credit cards, automated teller machines (ATMs), debit cards, point-of-sale (POS) terminals, home banking, and telephone-bill-paying services. Payment for these mechanisms are conducted online and flow through the check truncation system and the

[4] .Increasingly, the terms multi-purpose or multi-function are also used to convey the idea that the card or device can function as several types of payment instrument (e.g. credit card, debit card, stored value card), and/or that the card can be used for purposes besides financial transactions (e.g. identification card, repository of personal medical information). The lack of standarisation of terminology is perhaps a reflection of rapid technological innovations. Risk Management for Electronic Banking and Electronic Money Activities, supra note 1, pp.6

[5] Electronic money and its Legal Impact, available at, http://www.loasbridge.533.net/e-money-html.

[6] Ibid.

Automated Clearing House (ACH) System. A number of innovations are taking place in the area of retail electronic payments known as electronic money. These innovations, which are still at a relatively early state of development, have the potential to challenge the predominant role of cash for making small-value payments and could make retail transaction easier and cheaper for consumers and merchants.

The following figure compares attributes of current conventional payment systems and electronic payment systems.[7]

Current Payment Systems	Electronic Payment Systems
High degree of central bank control	Various national views about control
Highly structured supervision/regulation	Highly technical, yet to be designed
Large legal and policy literature	Little current literature
Body of examining and Customs mechanisms	Monitoring technology unavailable
Physical means of payment-checks, currency	Intangible electronic analogs
Huge infrastructure established world-wide	Downsized, computer-based

[7] Electronic Commerce: The Challenges to Tax Authorities and Taxpayers, An Informal Round Table Discussion between Business and Government, Turku, Finland, 18th Nov. 1997, OECD, available at http://www.oecd.org/daf/fa/e-com/turku_e.pdf.

Relatively labour intensive	Relatively capital intensive
High value infrastructure-brick and mortar	Low cost decentralized facilities
Bank-dominated wire transfers	Personal computer transfers
Clearing mechanism required	Clearing requirement reduced
Transportation - courier, land, sea, air	Telecommunications
World-wide use of US currency	Easy currency exchange/one currency
Serial numbers and banks records	Enciphered messages
Significant statistical data collection	No methodology for statistics
Economic national borders	No borders, effectively
Defined jurisdictions	Overlapping, unknown jurisdictions
Generally non-refutable, standard methods of validation	Evolving methods of transaction verification
Authentication, established structure to verify authenticity	Undetermined, system specific may involve third party.

TYPES OF ELECTRONIC PAYMENT SYSTEM

Electronic payment system can be segmented into three broad categories:

I. BANKING AND FINANCIAL PAYMENTS: This category covers electronic data interchange (EDI) for inter organizational commerce. Using EDI, Banks and other organizations exchange trading information electronically. The spectrum of EDI covers large-scale bank-to-bank transfers and wholesale payments as well small-scale or retail payments via automated teller machines (ATMs) and cash dispensers. And it also includes home banking (example, bill payment).

High-value wholesale payments flow through the three major interbank funds transfers systems: the *Clearing House Interbank Payment Systems (CHIPS),*[8]*the Society for Worldwide Interbank Financial Telecommunications (SWIFT),*[9] *and Fedwire*[10]

Although cash payments represent the direct converse of electronic forms of payment, cash delivery is itself increasingly based on the huge base of Automated Teller Machines (ATMs), which are being networked together to permit customers to collect cash from different banks as well as in other

[8] CHIPS is a private sector system owned and operated by the New York Clearing House Association, an organization of banks in New York City. CHIPS is an online, real-time electronic payment system that transfers and settles transactions, Electronic Commerce and the NII: Draft for Public Comments, available at http://iitfcat.nist.gov:94/doc/electronic_commerce.html>.

[9] SWIFT which headquarter in Brussels, is actually a financial messaging system rather than a payment system. The system facilitates interbank transfer of information but presupposes a separate system for effecting the payment. SWIFT has been criticized for relying on hub and spoke technology. SWIFT is now focusing its attention on the requirements for global settlement of large value payments. Its existing proprietary network and charging structure is simply not cost effective when making lower value payments. Ibid. pp,55-57.

[10] Fedwire is a real time payment system operated by the Fedral Reserve for financial institutions that have either reserves or clearing accounts at Federal Reserve Bank, Ibid, pp. 45-47.

countries. ATM and credit card networks are linked in that. Visa and MasterCard holders have long enjoyed the facility to draw cash from ATMs. A number of companies including NatWest in the UK, are developing smart card technologies, which may ultimately bridge the gap between ATM networks for delivering cash and the requirement to make electronic payments.[11]

Banks are introducing new ways for consumer to access their account balances, transfer funds, pay bills, and buy goods and services without using cash, mailing a check, or leaving home. The four major categories of home banking (in historical order) are:[12]

i. *Proprietary bank dial-up services*: A home banking service, in combination with a PC and modem, lets the bank become an electronic gateway to customers' accounts, enabling them to transfer funds or pay bills directly to creditors' accounts.

ii. *Off-the –shelf home finance software*: This category is attracting the interest of banks as it has steady revenue streams by way of upgrades and the sale of related products and services. Examples include Intuit's Quicken and Microsoft Money.

iii. *Online services-based banking:* This category allows banks to setup retail branches on subscriber-based online services such as Prodigy, Compuserve, and America Online.

[11] Andreas Crede, *Electronic Commerce and the Banking Industry: The Requirement and Opportunities for New Payment Systems Using the Internet*, p-10, available at http://www.ascuse.org/jemc/vol1/issue3/crede.html.

[12] Ravi Kalakota and Andrew Whinston, *Electronic Commerce: A Manager's Guide*, (Massachusetts, 1997), pp, 189-190.

iv. *World Wide Web-based banking*: This category of home banking allows banks to bypass subscriber-based online services and reach the customers' browser directly through the World Wide Web.

And the next to come up is "mobile banking". It will give customer full autonomy and self-service via electronic channels. WAP (Wireless Application Protocol) is expected to become a key delivery channel for the secure execution of transactions on the move and the retrieval of ever-changing information, such as bank account details. Eventually, as more services are offered via the channel, the mobile will become a "bank in your pocket", the perfect personal transaction device.[13]

Electronic Data Interchange (EDI)

EDI is used to electronically transmit documents such as purchase orders and invoices. EDI can also be used to transmit financial information and payments in electronic form.[14] When used for effecting payments, EDI is called Financial EDI. FEDI is typically set up between banks and their corporate customers to allow the banks to receive payment authorizations from payers, and make payment settlements to payees. Fund transfers between banks are handled using the typical bank networks, such as the CHIPS and SWIFT automated clearinghouses. Some banks even provide Van-like services [15] with their FEDI payment services, allowing their corporate customers to submit remittance information with payment

[13] Paul Scarrott, "Banking in a Mobile World", *The Banker Supplement*, April 2000, p. 16, See also, *The Banker*, vol. 151, no. 899, Jan. 2001, pp-42-43.

[14] Kamlesh K Bajaj and Debjani Nag, *E-Commerce: The Cutting Edge of Business*, (New Delhi, 1999), pp. 13-14.

[15] VANs are private networks; so far, they are more secure because and reliable then the Internet. The EDI service provider maintains the VAN and transfer the data between participants, David Kosiur, *Understanding Electronic Commerce*, (Washington, 1997), pp.56-59.

instructions, instead of requiring the customer to use the bank for payments, and a separate EDI Van for remittances.

II. RETAILING PAYMENTS: This group of payment solutions describes a wide area of *credit card (e.g. Visa, Master-Card) debit cards (e.g. J.C. Penney Card) and Charge Card (e.g., American Express)*

The few large credit card company-Visa, MasterCard -operate worldwide systems for electronic authorization and settlement of card-best payments. With the emergence of electronic commerce, both the technology used in the electronic clearing and the global clearing network infrastructure provided by these card system operators have evolved as valuable assets for extending the business into OP (Online Payment) Solutions.

In a *credit card* transaction, the consumer presents preliminary proof of his ability to pay by presenting his credit card number to the merchant. The merchant can verify this with the bank, and create a purchase slip for the consumer to endorse. The merchant then uses this purchase slip to collect funds from the bank, and on the next billing cycle, the consumer receives a statements from the bank with a record of the transaction. Both MasterCard and Visa have established their own network, which are used for verifying transactions world wide.[16]

However, credit cards only work with signed-up merchants, and do not generally support individual-to-individual or direct business-to-business payment transactions.[17] Credit cards are distinguished from debit cards by

[16] Andreas Crede, supra note 11, p.10.

[17] Ravi kalakota and Andrew Whinston, supra note 12, p. 157.

having access to a line of credit made available to the cardholder by the card issuer.

A *debit card* transaction works much like a credit card transaction. For example, a customer gives an ATM to the merchant for the purchase. The merchant Swipes the card through a transaction terminal, which reads the information; the customers enters his personal identification number (PIN); and the terminal routes the transaction through the ATM network back to the customer bank for authorization against the customer's demand deposit account. The funds, once approved, are transferred from the customer's bank to the merchant's bank.

Credit card-issuing banks make money, in part, by charging merchants a processing fee ranging from 1.5 to 3% of the value of transaction.[18] Merchants impose a minimum purchase amount because the fees for small purchase amounts would erode their profits enormously. The usual distinction between a credit card and a charge card is that the balance on a charge card must be paid in full each month, whereas a credit card may carry a balance from month to month, albeit with interest accrued. Charge card such as American Express carries no present spending limit. It does not involve lines of credit and do not accumulate interest charges.

III. ONLINE ELECTRONIC COMMERCE PAYMENTS

The last category includes all different payment solutions designed for electronic commerce transactions. OPs (Online Payment Systems) can be

[18] Gary P. Schneider and James T. Perry, *Electronic Commerce*, (Cambridge, 2000), p. 213.

split into[19] (1) *credit or postpaid, (2) debit or prepaid and (3) token-based payments.*

Credit cards have become the most common means for consumers to pay for gods and services on the Internet. From the technical point of view, it is much easier to create a system for processing credit card purchases than to invent a new payment technology.[20] However, credit-card based online payments raise some problems,[21] i.e. the problem of card authorization (is the user also the owner?), data protection (how to protect the card number and expiration date?), and integrity of the amount charged. The solution of the problems include: (1) encryption of credit card and transaction data, and (2) use of trusted intermediaries who will not pass credit card details to the payee.

In the first option, the payer has to trust the payee on two counts. *First,* that the mutually agreed upon amount has been charged. *Second,* data are properly protected in the payee's database. As the payer has no written evidence of the transaction, it may be difficult to monitor and protest an online transaction. Secure online credit card payments of this kind are usually based on secure protocols such as Secure Hyper Text Transfer Protocol (SHTTP) and Secure Socket Layer (SSL).

For many credit card applications, strong cryptography using a protocol such as SSL provides a high degree of communication security. [22]

[19] Michael Shaw, Robert Blanning and Andrew Whinston (ed.), *Handbook on Electronic Commerce*, (New York, 2000), p. 275.

[20] G.Winfield Treese, Lawrence C.Stewart, *Designing Systems for Internet Commerce*, (Massachusetts, April 1998), pp.284-286.

[21] Gary P. Schneider and James T. Perry, supra note 18 p. 279.

[22] However, security afforded by export-grade cryptography in general-purpose communication software may not be sufficient for financial applications.

The second option requires a standard to assure the interoperability of intermediaries as well as an infrastructure for verification and settlement. To that end, a standard has been established recently in the form of the secure Electronic Transaction Standard (SET)[23]. SET increases security and privacy for all parties involved. However, since SET involves numerous encryption and decryption cycles, plus some intermediaries (e.g. trust centers and payment gateway operators), it is too expensive for micro-payment applications on the Web. The protocol includes strong encryption and authentication of all of the parties in a credit card transaction: the buyer (or cardholder), the merchant, and the merchant's bank. Although it is still in the early stages of deployment SET is the emerging standard for handling credit transactions on the Internet.

In addition to credit card payments, SET is conceived to be employed for debit and smart card solutions[24]

Third-Party Processors and Credit Cards

In third-party processing, consumers register with a third party on the Internet to verify electronic micro-transactions. Verification mechanisms can be designed with many of the attribute of electronic token, including anonymity. They differ from electronic token systems in that (1) they depend on existing financial instruments and (2) they require the on-line involvement of at least one additional party and, in some cases, multiple parties to ensure extra security. However, requiring an on-line third-party

[23] Justin Stephenson and laura Bennett, Chapter 4, "E-Payments", In Stephen York and ken Chia (ed). *E-Commerce: A Guide to the Law of Electronic Business*, (London, 1999), pp. 69-71.

[24] For further detail see, "SET information home page", at http://www.setco.com.

connection for each transaction to different banks could lead to processing bottlenecks that could undermine the goal of reliable use.

Examples of companies that are already providing third-party payment services on the Internet are *First Virtual* and *Cyber Cash.*[25]

First Virtual has developed a system for linking credit card, bänks and processing agents with the Internet. It has developed a closed loop payment system which involves First Virtual's providing a mailbox from which instructions to make the payment and to credit the seller's account are made. The system depends on the "off-line" network provided by EDS which is used to transfer creditcard/bank account information, with First Virtual effectively acting as a message clearing house. In effect the buyer sends a message to First Virtual, which passes this on to EDS. EDS is turn acts under instruction from First Virtual to pass on the account details to the seller. When the transaction is confirmed, First Virtual sends a message to buyer to confirm that the transaction should still go ahead, at which point payment is effected.[26]

The debit card works in a similar manner as electronic cheks and credit cards, except that settlement "the actual payment" takes place immediately and online. In general, with debit OP solutions, the payer has already deposited money before the payment transaction is initiated. Two subtypes have to be considered, the debit card, with the option of direct debit payments and the value storage card.

[25] First virtual is different from CyberCash in a way because it uses the SET Protocol to transfer information to the acquiring bank. CyberCash uses their own software to process credit card information before setting accounts with the bank. David Kosiur, *Understanding Electronic Commerce*, (Washington, 1997), pp. 45-46.

[26] Andres Crede, supra note 11, pp 14-15, also see http://www.fv.com.

The debit card is another typical access product. The debit card carries the bank account address of the payer. Usually, the card works with a PIN, which identifies the card user as the legal proprietor of the card. The use of debit cards in the electronic commerce environment works much like conventional "Electronic Fund Transfer at Point of Sale" (EFTPOS) systems. Once debit card data and PIN are transmitted, the payees asks the card emitting institutions to authorize the payment online. The emitting institution checks the availability of funds and credits the payee while debiting the payer immediately. These transactions are fully atomic and do not involved credit or liquidity risk.[27]

An example of a debit cards is the *EC-card,* which is very popular in Germany and other European countries. Deutsche Bank is currently testing a direct online fund transfers solution with PIN verification and based on SET.

Another prepaid instrument is *the value storage card.* Traditionally, such cards have been used in closed systems. Thus, the issuer of the card is the only one to accept payment with the card. Originally, cards were not rechargeable and the value of the card was paid at the time of purchase (pre-payment). Typical examples of such value storage cards are telephone cards. When it comes to electronic commerce, value storage cards can function as wallets for electronic cash.

The other type of *debit card is smart card.* Cards carrying electronic cash are called smart card. The term "smart" refers to chip-embedded software, placed on the card. Smart card based system are token rather than prepaid access products. Due to an unmatched service versatility and very

[27] Michael Shaw, Robert Blanning and Andrew Whinston (ed.), supra note 19, p. 280.

lucrative bundling, co-branding, and cross-marketing opportunities and therefore ease of diffusion, smart cards might evolve as a major mid-term OP solution.

Smart cards use magnetic stripe technology or integrated circuit chips to store customer-specific information, including electronic money. [28] With a smart card, credit theft is practically impossible because a key to unlock the encrypted information is required, and there is no external number that a thief can identify and no physical signature that a thief can forge. A typical example of smart card is *Mondex.*[29]

The *Mondex card* acts as a form of "Virtual Cash". The card is programmed to reflect an amount of money which is prepaid by the card holder to the *Mondex* issuer and the card holder is than able to present the card by way of payment at any outlet which accepts the payment system.[30] Payments are made by debiting the *Mondex* card and crediting the seller's *Mondex* card. The card system is very secure because any interference with the chips usually destroys them entirely, leaving the card useless.

Other example is *Visa Cash.*[31] It comes in two varieties, disposable and reusable. The reusable cards are charged up using specialized terminals and Automated Teller Machines. The disposable cards are loaded with a predetermined value.

[28] Ravi Kalakota and Andrew Whinston, supra note 12, pp. 176-177. See also Gary P. Schneider and James T. Perry, supra note 2, pp. 231-234. Also see Debbie McElory and Efraim Turban, Chapter-14, "Smart Cards", in Michael Shaw, Robert Blanning and Andrew Whinston (ed.), *Handbook on Electronic Commerce*, (New York, 2000), pp. 289-302.

[29] For a detail see Mondex Web Site at, http://www.mondex.com.

[30] Justin Stephenson and Laura Bennett, supra note 23, pp. 72-73.

[31] G. Winfield Treese, Lawrence C. Stewart, supra note 20, p. 287.

Token-based payment systems include *electronic cash (e.g. DigiCash) and electronic checks (e.g. NetCheck)*

An electronic check[32] has all the same features as a paper check, except that they are initiated electronically, use digital signature for signing and endorsing, and requires the use of digital certificates to authenticate, the payer's bank, and bank account. The security/authentication aspects of digital checks are supported via digital signatures using public-key cryptography. Ideally, electronic checks will facilitate new online services by: enhancing security at each step of transaction through automatic validation of the electronic signature by each party. (payee and banks); and facilitating payment integration with widely used EDI-based electronic ordering and billing processes.

Electronic checks are delivered either by direct transmission using telephones line, or by public networks such as the Internet. Electronic check payments (deposits) are gathered by banks and cleared through existing banking channels, such as Automated Clearing Houses (ACH) networks.

A prototype of electronic check system called "*NetCheck*"[33] has been developed. NetCheck provides "accounting server" software that allows organizations to set up their own in-house, online "banks", which would accept paper checks or credit card payments in exchange for crediting a customer's NetCheck account. NetCheck works in the following manner: When the payee receives an electronic check, the payee presents it to the accounting server for verification and payment. The accounting server

[32] Ravi Kalakota and Andrew Whinston supra note, 12, pp. 163-166. Also see, David Kosiur, supra note 15, pp. 49-51.

[33] For further detail see, NetCheck website at, http://www.netchex.com/index.html.

verifies the digital signature on the check. The payer's digital "signature" is used to create an order to a bank computer that authorizes fund transfer to the payee's bank and not to debit money from the payer's account.

An interesting aspect of the NetCheck system is that it can be used as a resource management tool on Internet, a form of internal cash. The Financial Services Technology Consortium (FSTC) is also developing a prototype electronic check system.[34]

Electronic Cash is nothing but a string of digits. It combines computerized convenience with security and privacy that improve on paper cash. A "digital cash or digital coin" is a message issued by a bank and encrypted with its private key.[35] The message will contain the following information: the serial number of the coin, the identity of the bank and its Internet address, the amount of the coin, and an expiry date. Because the "coin" is encoded with the bank's secret key it may only be read by using the bank's public key. It cannot be altered without destroying it. The bank keeps a record of the serial number of the "coins",

When a customer wishes to be issued with "coins" he or she sends a request to the bank. The request must be encoded with the customers' secret key. The bank may then decode the message with the customer's public key and have confidence that the request is what it appears to be and that it originated with the customer.

[34] Ravi Kalakota and Andrew Whinston, supra note 12 p. 167.

[35] Alan L Tyree, "Virtual cash – Payments on the Internet – part I", *Journal of Banking and Finance Law and Practice*, Vol. 7, 1996, pp. 35-38, available at http://www.law.usyd.edu.au/~alant/netplay.html. Also see, David C. Stewart, *The Future of Digital Cash on the Internet*, available at, http://www.global.concepts.com.

The "coins" are "issued" to a particular customer by encoding the coin with the customer's public key. This message is then sent to the customer who decodes it using his or her private key. Even if the message is intercepted it would be worthless since only the customer to whom the "coins" are issued can read the message. The "coins" thus received are stored on the customer's private system.[36] A customer who wishes to purchase something on the Internet may send the "coin" to the merchant. The "coin" should be encrypted with the merchant's public key to prevent interception. The merchant decodes using his or her private key and then does two things with the received message: first, the message is decoded using the bank's public key to verify that it is a "coin" for the appropriate amount of the payment. Secondly, the merchant must ascertain that the "coin" has not already been spent. This is done by asking the bank to verify that the serial number of the coin is still current.

Assuming the "coin" is valid, the simplest scenario is that the bank credits the merchant's account and then cancels the serial number so that the "coin" may not be spent again. Alternatively, the bank cancels the serial number and issues a new "coin" to the merchant that is identical in all respects save the serial number.

The payment process may be classified into online and offline transactions:[37]

If an online payment takes place the coins will be checked immediately for authenticity. This implies that a digital coin is used only

[36] The user's software stores these electronic coins on the hard drive of the computer. Once receiving the coins, the computer stores these note until the user desires to make a purchase.

[37] Juergen Seitz and Eberhard Stickel, *Internet Banking – An overview*, pp. 4-12, available at, www.arraydev.com/commerce/JIBC/9801-8/htm.,

once. The financial institution needs to check the authenticity by using a list of all coins that have been issued or a list of all coins that have been sent in for credit.

In case of offline payments the coins may be used more than once. To avoid double spending it is necessary to store information about the user or the users on the coin in order to be able to perform checks later. Anonymity may be guaranteed by so-called secret sharing. Then the financial institutions only gets information in case of double spending.

Since the issuer's digital signature authenticates the serial number on each electronic coin,[38] the coin's redemption links its original holder to the transaction. However, consumers can avoid this by using blinded coins. Using the "blinding" technique,[39] the bank can validate the coins without knowing the payer's identity. Therefore, this prevents the bank from recognizing the coins as having come from the payer's account.

To create a blinded coin, a bank customer must first make a request for electronic currency. The bank will then withdraw this pre-set denomination from the customer's account in the form of digital coins.[40] The customer's software then generates a 100-digit random serial number for each coin. Since the length of the randomly generated serial number is large, it guarantees with high probability that the serial numbers of any two coins

[38] To avoid erosion of privacy, systems such as anonymous electronic transactions are not only needed, but also considered essential, see, *Digital Cash, an overview*, at http://mrmac-jr.scs.unr.edu/

[39] David Chaum, the founder of DigiCash, created a blind signature system. Using this system, the electronic money in the "wallet' is double-encrypted-once to imprint it with an authorization tag so that its validity as tender can be verified by the merchant's computer, and a second time to protect the customer's identity from prying eyes, See Brain Connolly, *Digital Commerce Gaining Currency, INTELLECTUAL CAPITOL* at, http://www.intellectualcapitol.com/.

[40] See, J. Orlin Grabbe, *Internet Payment Schemes: part 3*, at http://www.Zotatimes.com

will not be the same. The coins are then "blinded" by multiplying them by a random factor. The customer then signs the blinded coins with his private key, encrypts the coins with the public key of the bank and then sends them to the bank.

When the bank receives the coins, the bank removes the signature, signs the coins with its own private key and registers its worth- thereby "stamping" a value on the certificate. The bank then encrypts the coins with the customer's public key and sends them to the customer. The customer then decrypts the coins with his private key and "unblinds" them by dividing out the random factor. By using the blinding/unblinding process, the customer prevents the bank form associating subsequently spent coins with withdrawals from his bank account. Therefore, the bank is unable to know when or where you shopped, or what you bought.

There are different kind of electronic money offered by different company, e.g. DigiCash, NetCash, Millicent.[41]

In DigiCash System[42] an account is established at a DigiCash-licensed bank with real money. Once established, the customer can withdraw e-cash that is stored on the user computer's hard drive. Using proprietary software, e-cash can be spent with an Internet merchant or with anyone else whose computer is set up to deal in e-cash. Using public-key cryptography, the digital tokens are said to be secure and can be registered and verified by the issuer without revealing to whom it was originally issued. In effect, these digital cash transactions are capable of being as anonymous as cash. No

[41] To get thorough description of Millicent technology, see at http://www.research.digital.com/src/personal/stev.

[42] For further details see, DigiCash Website at, http://www.digicash.com, Also see, Justin Stephenson and Laura Bennett, supra note 23, pp. 74-76.

transaction confirmations are necessary, meaning the merchant can immediately ship the product.

NetCash[43] concept is similar to e-cash, except that it does not require any special software to use. NetCash is transmitted across the Internet using an encryption scheme known as PGP (pretty good privacy). To get NetCash, a party must send a check or money order to the company's headquarters. The company returns electronic coupons via-e-mail.

Legal Nature of DigitalCash[44]

All of the proposed methods of implementing payments over the Internet share the characteristics that there is an "issuer". Digital coins are "issued" by a "bank" to a customer who then uses the coin via electronic messages to pay for goods or services via the Internet. In order to have legal effect, we must treat the issuer as a promisor who has promised to make or to guarantee payment.

To whom is the promise made? This will depend upon the particular implementation of the payment mechanism. An issuer could make it a condition that merchants may only accept payment by prior arrangement. They should re-establish the contractual restraints which are lacking in the general model. However, for the commercial reason outlined above, this is unlikely to be a stable long-term solution. In real life schemes for "digital coins", it seems that the issuer must be taken to promise at least to any one who takes a valid coin in good faith and for value that the coin will be met.

[43] For further details see, NetCash Website at, http://www.netbank.com/~netcash.

[44] Alan L Tyree, *Virtual Cash – Part – II*, available at http://www.law.usyd.edu.au/~alant/ netpay2. html.

Even that interpretation is not wide enough to make the anonymous payment schemes work. In such a case it must be taken that the issuing bank promises to give value for any valid coin to anyone who presents it for payment. But the problem here is that the issuing bank, the payer and the payee may have no geographical connection whatsoever. It is perfectly plausible that an Australian purchaser could pay a Bolivian supplier by means of digital coins issued by a Mangolian bank. In such a case which law will we use to settle disputes when the transaction goes wrong? How can we even begin to ensure integrity of the payment system or to implement consumer protection policies? How can we control and detect money laundering schemes?

KEY FEATURES OF E-MONEY SCHEMES

Various e-money schemes are being developed and they differ considerably in their features, many aspects of which are still to be finalized.[45]

Firstly, e-money products differ in there technical implementation. To store the prepaid value, card-based schemes involve a specialized and portable computer hardware device, typically a microprocessor chip embedded in a plastic card, while software-based schemes use specialized software installed on a standard personal computer.

[45] Some of the features are described in more detail in the report on Security of Electronic Money, by the Committee on Payment and Settlement Systems and the Group of Computer Experts of the Central Banks of the Group of Ten Countries, (Basle, August 1996), available at, http://www.bis.org/publ/cpss18.pdf. For performance comparison of different forms of money see, J. Chrisotpher Westland and Theodore H.K. Clark, *Global Elcetronic Commerec: Theory and Case Studies* (Massachusetts, 1999), p. 471.

Secondly, institutional arrangements may vary. Typically, four types of service provider will be involved in the operation of an e-money scheme: the issuers of the e-money value, the network operators, the vendors of specialized hardware and software and the clearers of e-money transactions.[46]

Thirdly, products differ in the way value is transferred. Some e-money schemes allow transfers of electronic balances directly from one consumer to another without any involvement of a third party such as the issuer of the electronic value. More, usually the only payments allowed are those from consumer to merchants, and the merchants in turn have to redeem the value recorded.

Fourthly, related to transferability is the extent to which transactions are recorded. Most schemes register some details of transactions between consumers and merchants in a central database, which could then be monitored, although a few schemes envisage keeping only limited records of individual transactions or no records at all. In cases where direct consumer-to-consumer transactions are allowed, these can only be recorded on consumer's own storage devices and can be monitored centrally only when the consumer contacts the e-money scheme operator (for example, to reload a card with more value). [47]

Finally, in most e-money schemes currently being developed or pilot-tested, the "value" stored on the devices is denominated only in the national

[46] Implications for Central Banks of the development of Electronic Money, BIS, (Basle, Oct. 1996), p.2, available at http://www.bis.org/publ/bisp01.pdf.

[47] Ibid.

currency. It is possible, however, for balances to be held and payments to be made in several different national currencies. [48]

In the next chapter we are going to discuss the legal and regulatory issues, which have been raised by electronic banking.

[48] E-money products may also have multifunctional features, whereby the e-money function is combined with other payment functions such as debit and credit card facilities and even with non-payment functions.

Chapter - III

Key Legal and Policy Issues Raised by Electronic Banking

CHAPTER III

KEY LEGAL AND POLICY ISSUES RAISED BY ELECTRONIC BANKING

Electronic cash transactions and systems raise a variety of questions of first impression under existing banking law. Since electronic fund transfers, are not carried out in a manner identical to paper based funds, changes in the law to adjust to the new procedures should be expected. Some of those questions are of principal concern to those who will use electronic cash- both consumers and commercial interests, while others are of principal concern to central banks, governmental policy makers and others concerned about monetary policy.

The key legal questions, which are going to be discussed in this chapter relate to:

I. Criminal laws, money laundering, taxation and other cross border issues.

II. Application of the law of evidence.

III. Security aspects of electronic banking.

IV. Privacy in electronic banking.

V. Banking and financial regulation and clearing and settlement arrangement for electronic money transfer.

VI. Consumer protection, contract terms and enforceability, and alternative dispute resolution.

VII. Risks and electronic payment system.

I) CRIMINAL LAWS, MONEY LAUNDERING AND TAXATION

CRIMINAL LAWS

Ordinarily, the law keeps pace with the technological changes in society. However, rapid technological advancements like the Internet clearly threaten to leave the law behind. Since the Internet is composed of computers, crimes occurring on the Internet are "computer crimes". Traditionally, criminal law has been seen as the province of national authorities. But the irrelevance of geography to the Internet poses serious questions with regard to jurisdictional matters that are fundamental for any criminal proceeding to take place. But as yet there has been limited international harmonization.

A critical issue in considering the application of criminal law is whether computer related conduct should be regarded as requiring technology specific legislation or whether it might satisfactorily be regulated through the application of more general criminal law provisions.

The *Information Technology Act, 1998*[1] defines a computer criminal as a person who: knowingly or intentionally accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer data base, computer, computer system or computer network in order to either (a) devise or execute any scheme or artifice to defraud, deceive, or extort, or (b) wrongfully control or obtain money, property or data.

A crime essentially consists of two elements, namely, *actus reus* and *mens rea.*

[1] This is the IT Act in its Earlier Form, Drafted by Department of Electronics in 1998.

Actus Reus in Internet Crimes

The element of *actus reus* in Internet crimes is relatively easy to identify but is not always easy to prove. The fact of the occurrence of the act that can be termed as a crime can be said to have taken place when a person is:[2]

i. Trying to make a computer function.

ii. Trying to access data stored on a computer or from a computer, which has access to data stored outside.

iii. If he or she uses the Internet to attempt to gain access, signals pass through various computers. Each of these computers is made to perform, a function on the instruction, which the person gave to the first computer in the chain. Each such function can be said to constitute actus reus.

iv. Attempting to login, even if those attempts fail. This is because most hackers have an automated system of trying passwords, the very running of which can be considered to be a function being performed.

Mens rea in Internet Crimes

An essential ingredient for determining *mens rea* on the part of the offender, is that he or she must have been aware at the time of causing the computer to perform the function that the access intended to be secured was unauthorized. There must be, on the part of the hacker, intention to secure access, though this intention can be directed at any computer or not a particular computer.[3] Further, this intention to secure access also need not be directed at any particular

[2] See for a Detailed Discussion, Nandan Kamath, *Law Relating to Computers Interest and E-commerce*, (Delhi 2000), pp. 235-36.

[3] This suits the prosecution in matters relating to unauthorized access on the Internet, because it is often complicated to prove that a person intended to login to a particular computer.

kind of programme or data. It is enough that the hacker intended to secure access to programmes or data per se.[4]

Thus, there are two vital ingredients for *mens rea* to be applied to hacker:

i) The access intended to be secured must have been unauthorized; and

ii) The hacker should have been aware of the same at the time he or she tried to secure the access.

The second ingredient is easier to prove if the accused hacker is a person from outside who has no authority whatsoever to access the data stored in the computer or the computers, however, it is difficult to prove the same in the case of a hacker with limited authority.[5]

Types of Internet Crimes

Broadly, there are three main types of crime, which can be committed through by means of, and using the Internet. They can be classified into:

i) Hacking[6] without any intention to commit any further offence or crime;

ii) Unauthorized access with intention to commit further offences, these can include theft, fraud, misappropriation, forgery, etc.

iii) Destruction of digital information through use of viruses.

As to number (1) a question of debate is whether such an act itself constitutes an offence. It may not be brought within the ambit of existing laws if it is interpreted conventionally. The act of such a hacker can perhaps, most appropriately, be considered in the light of

[4] C. Gringras, *The Laws of The Internet*, (London, 1997), p. 216.

[5] See Nandan Kamath supra note, 2.p. 238

[6] For definition see Section 441, IPC, 1860.

laws relating to criminal trespass. In applying the laws relating to criminal trespass to hacking on the Internet, the primary question that needs to be answered is whether websites are property. The fundamental issue is whether the treatment of websites as property makes sense in the light of the justifications for the institutions of property generally.[7] As trespass actions are grounded in the idea of protecting an owner's control over real property which is just a particular species of property, there is no inherent reason that a website could not be considered a species of property. Hence, there is no reason for not allowing a cause of action for trespass to websites.[8]

The other argument in support of this is that, when a computer owner who becomes aware that a party has secured unauthorized access would have to proceed on the assumption that further damage had been caused, and would be put to considerable expense in checking data and, perhaps replacing programs or data with back up copies. In fact in the *IT Act 2000*[9] *and Computer Misuse Act, 1990, U.K.*,[10] it has been made a crime.

According to the Second Council of Europe defines it as:[11]

> ...the input, alteration, erasure or suppression of computer data or computer programmes (sic), or other interference with the course of data processing thereby causing economic or possessory loss of property of another person with the intent of procuring an unlawful economic gain for himself or for another person.[11]

The prosecution of even such low technology conduct as the misuse of a cash-dispensing card has posed problems in certain

[7] See, Trotter Hardy, *The Ancient Doctrine of Trespass to Websites*, at http:// www.wm.edu/law/publications/jol/hardy.html.

[8] Nandan Kamath, supra note 2 p. 241.

[9] Section 43 (a), IT Act, 2000, India.

[10] Section 1, Computer Misuse Act, 1990, U.K.

[11] Ian J. Liyod, *Information Technology Law*, 3rd ed., (London, 2000), p. 209.

[12] Ibid.

jurisdictions where the basis of theft type offences is the removal of property without the consent of the owner.

In both England and Scotland such instances have been successfully prosecuted under the law of theft, with the determining factor being the perpetrator's intention to deprive the owner of his or her property.[12]

Generally speaking, it has been recognized that there are three stages at which fraud may occur, i.e. input fraud, output fraud and program fraud.

Input fraud involves the falsification of date prior to, or to the moment of, its entry into a computer. The instance of the misuse of cash dispensing card might be taken as an example of this form of behaviour, although the falsification might be considered to relate to the entitlement of the party to use the card rather than to the validity of the data inserted.

Output fraud, is a less frequent occurrence, and again raises questions concerning the applicability of provisions of criminal law. As the name would suggest, it consists of the fraudulent manipulation of data at the point it is enacted from a computer. In one case reported by the Audit Commission (U.K), a bank manager falsified accounts (input fraud) to conceal the fact that he was embezzling funds. The bank's computer system generated records, which would have revealed his activity, but he misused his position in order to suppress these records. The fraud was to the order of £ 44,000.[13] Once again the fact that the conduct at issue was criminal could not be doubted. But with this instance we see the first signs of what is one of the

[13] Ian J Liyod, supra note 11, p 210.

major difficulties arising from the involvement of computers, that of securing evidence relating to the conduct involved.

Program fraud involves either the creation of a program with a view to fraud or the alteration or amendment of a program to such ends. One of the most notorious cases of program fraud is the so called 'salami fraud'. This involves the perpetrator taking a small sum from many accounts and transferring this to an account, which he or she controls. Few customers might notice or query a withdrawal of very small sums from their bank account. In the event thousands of accounts may be involved and the process repeated over a period of months, could mean large sums of money.

The other type of fraud is the *Internet fraud.* Perhaps the most publicized form of fraud today involves activities conducted over the Internet. The fear is often expressed that credit card numbers might be intercepted by hackers in the course of transmission over the Internet, albeit there does not appear to have been a documented case of this occurring. The risk of credit card misuse is, however, significant. While not all of the complaints described above will involve criminal conduct, in cases where fraud is at issue there will generally be no doubt that an offence has been committed.

In considering the applicability of criminal law regarding computer fraud, two forms of conduct may be identified. The first occurs where a fraudulent scheme is devised with the aim of securing some direct pecuniary benefit, e.g. to cause £ 500,000 to be transferred to the perpetrators bank account[14]. The alternative form of advantage occur when the perpetrator is relieved of payments that he or she would otherwise be obliged to make, e.g. the perpetrator using

[14] R v Thomson (1984) 3 All ER 565. This case furnishes a helpful illustration in this respect.

a third party's password to secure free use of a database, with any bill being sent to the third party. In this situation, the perpetrator benefits in a more indirect manner.

In respect of the first form of conduct, there will be little doubt concerning the criminality of conduct. As indicated by law commissions 'when a computer is manipulated in order to obtain money or other property, a charge of theft or attempted theft will generally lie.[15] And *Section 2 of the U.K. Computer Misuse Act* deals with this type of crime. However, such a clear definition is conspicuously absent in the *IT Act, 2000.*

As regards to second form of conduct, an example is to be found in the facts of the *R v Gold*[16]. Here Gold together with his co-accused Schifreen obtained a password issued by British Telecom to one of its engineers allowing use of its 'Prestel' system. This system offers subscribers access to a variety of database services upon agreeing to pay rental charges plus further charges dependent upon the nature and extent of usage. Users would be allocated a password. This enabled Gold to obtain access to the 'Prestel' services without incurring any charges. The question then arose what, if any, offence had been committed. The comparable offence under English Law would be that of obtaining property or services 'by deception'. Although the point has not been definitively settled, the assumption has been that only a human being can be the victim of deception.

However, after applying relevant law the court came to the conclusion that the appellants' conduct amounted in essence to dishonestly obtaining access to the relevant 'Prestel' databank. That is not a criminal offence. If it is thought desirable to do so that is a

[15] Law Commission Working Paper No. 110, (UK) para 3.4.
[16] *R v Gold*, (1987) QB 1116 at, p. 1124.

matter for the legislature rather than the courts. However, this aspect of crime has been now dealt with in the *Computer Misuse Act, 1990. Section 66 of Information Technology Act* also deals with this aspect of crime. Even the Scottish Law Commission[17], expressed the view that in determining whether this offence has been committed, attention should be paid to the conduct of the perpetrator. If the intention is to obtain services dishonestly, the offence will be committed and the fact of whether the conduct operates upon a human or machine is irrelevant.

Destruction and Alterations of Digital Information.

The single largest menace facing the world of computers today is the threat of corruption and destruction of digital information induced by a human agent with the help of various types of programmes like Virus[18], Trojan Horse[19], Worms[20] and Logic Bombs.[21] It is clear that the menace of viruses and other such "computer pathogens" has to be regulated and controlled through the creation of a legal regime that is flexible enough to tackle existing as well as future contingencies.

It is imperative to look at the present legal system and examine whether it measures up to the challenges posed by such advanced instruments of crime. Under the Indian Penal Code, the offence that can be related to the alteration and destruction of digital information most closely is that of mischief. The offence of mischief is dealt with in the IPC in *Sections 425 to 440.*[22] It has been mentioned that a website could be considered to be property. Further, it cannot be

[17] Scottish Law Commission Consultative Memorandum no. 68, para 3.9.

[18] See, "Computer Viruses – An Executive Brief", at <http:// www.symontec.com/avcentre/refrence/corpst.html>.

[19] See,<http://www.netmcs.net/jargon/terms/+/Trojan-horse.html>.

[20] See, http://www.netmeg.net/jargon/terms/w/worm.html>

[21] See, <http://www.huis.hiroshima.u.ac.jp/computer/jargon/Lexicon entries logic-bomb.html>.

[22] For ingredients of mischief see Section 425 of IPC, 1860.

denied that all viruses, however, harmless, cause damage to some extent.[23] Thus, the requirement of damage to property is met in the case of alteration or destruction of digital information *Section 65 of The Information Technology Act, 2000* has described this kind of crime. As to the English Law the decision of *R v Whitely*[24] represents the authoritative endorsement of the view that an act causing amendment to data held on the computer storage device can constitute the offence of criminal damage. The remedy has also been provided in *Computer Misuse Act, (U.K.), 1990.*

From the above discussion it is clear that since the technology is unique it requires a different legislative approach to deal with the situation. For example, a number of problems might arise in the computer field creating circumstances where conduct might not constitute an attempt under the general provision of criminal law, but it is justified to give special treatment within the computer context. Such is the case of a hacker who secures access to a bank's computer system, and uses it for electronic fund transfers. In order to accomplish a transfer, a password would have to be transmitted. The hacker might attempt to transmit a large number of combinations in the hope of finding the correct one. In the event that the password was discovered, used and a transfer of funds accomplished, there is no doubt that the offence of theft would be committed. Albeit the act of transmitting combinations of numbers and letters in an attempt to discover a valid password would not, be regarded as more than conduct prepąratory to the commission of a crime. As such, it would not constitute a criminal attempt, especially in the event further steps would be required in order to complete the transfer. In such a

[23] See, *Computer Viruses–An Executive Brief* at http://www.symantec.com/avcenter/reference/corpst.html.
[24] *R v Whitely* (1991) 93 cr App R25.

situation the existence of the ulterior intent offence would serve to bring forward in time the moment at which a serious criminal offence might be committed.

The application of the ulterior intent offence was at issue in the case of *R v Levin*[25] The appellant had used his computing skills to obtain access from his computer in St. Petersburg to Citibank's computer system in New Jersey. He had been able to monitor the accounts of customers and to cause transfers to be made from these accounts to others controlled by him or a number of accomplices. If successful, it was alleged, the scheme could have obtained funds in excess of $ 10 m. In the event, the activity was discovered and traced to Levin, who was arrested. There was no doubt that Levin, in hacking into the Citibank's computer system, had committed the unauthorized access offence. The court also had little hesitation in holding that he did so with intent to commit further offences of forgery and false accounting.

Jurisdictional Issues

The capability of many computer systems to transmit and receive data takes no account of national boundaries. In the event that a user and a computer are located in different countries and conduct which might be regarded as criminal occurs, the question arises which legal system might have jurisdiction. In both England and Scotland, the status of the law relating to jurisdiction is unclear. The Law Commission (U.K.) has called for urgent reform in the area, arguing that:

> International fraud is a serious problem... it is essential that persons who commit frauds related to their country should not be able to avoid the jurisdiction

[25] *R v Levin* (1997) QB 65.

of their country's courts simply on outdated or technical ground, or because of the form in which they cloak the substance of their fraud.[26]

In the *Laird v HMA*[27] it has been pointed out that where 'continuous crime' is involved there may be dual jurisdiction within both countries concerned. Where a crime is of such nature that it has to originate with the forming of a fraudulent scheme, and that thereafter various steps have to be taken to bring that fraudulent plan to fruition, if some of these subsequent steps take place in one jurisdiction and some in another, if the totality of the events in one country plays a material part in the operation and fulfillment of the fraudulent scheme as a whole there, should have jurisdiction in that country. *The Computer Misuse Act 1990* introduces the concept of a [28] 'significant link' with one or the other of the UK's legal systems. In the case of *S.1.*(it renders criminal any attempt to obtain unauthorized access to programs or data held on a computer) *or S.3* (it applies in the situation where the contents of a computer system are subjected to an unauthorized modification), offences a domestic court will have jurisdiction if either the accused person is located in the territory at the time of the conduct complained of occurred or the computer to which access was obtained or whose data programme were modified so located. The position is slightly more complex with regard to *S.2* offences. Here the domestic tribunal will only have jurisdiction where the further acts intended would constitute an offence in the country in which it was intended that they should occur.[29] In fact *Section 75 of the Indian IT Act, 2000* talks about offence or contravention committed outside India involving a computer, computer system or

[26] Jurisdiction Over Fraud Offences With a Foreign Element (1987), Law Commission, U.K., Para 2.7.

[27] *Laired v HMA*, (1984) SCCR 469 at 472.

[28] Section 5 of the Computer Misuse Act 1990, U.K.

[29] Section 4(4) of the Computer Misuse Act 1990, U.K.

computer network located in India. But it does not talk about circumstances involving *S.2 of the Computer Misuse act, 1990.*

MONEY LAUNDERING

Perhaps the highest hurdle facing an anonymous e-cash system is the potential to facilitate illegal money laundering.[30] One commentator has noted that:

> While we would caution against establishing restrictive rules that could stifle innovation, the eventual opportunity for money laundering using electronic products may be serious... over the longer term... it seems possible that electronic mechanisms that can hold large untraceable transfers over communications network could become attractive vehicles for money laundering and other illicit activities- especially if they are widely used and bypassed the banking system. Existing anti-money laundering regulations may then need modification.[31]

Although there is law to combat this menace in almost every country, the difficulty here is one of enforcement. A number of features of e-cash render it particularly well suited to illegal money laundering activities. These include the rapidity of e-cash exchanges and the inability to mark bills in an anonymous transaction system. It can also be used to conduct transactions over large distances, unlike physical cash and its volume, is easier to conceal, and there is the inability of law enforcement officials to witness the transfer of large amounts of cash. The Mondex card will allow a criminal to store millions of dollar in his wallet, while others will be transferring money from the comfort of their own home to an offshore banking account in a matter of seconds. Laundering money via the Internet can easily be accomplished because electronic currency transactions can

[30] Money laundering means hindering attempts to trace illegally acquired cash by passing through ostensibly legitimate commercial transactions. Eric Huges, "Address before the seminar in Law, Internet, and Society" at *Harvard Law school* (Apr. 1.1996). Reproduced from *Harvard Journal of Law and Technology*, Vol. 10, No. II, winter 1997.

[31] Jashua B. Kanvisser, "Coins, Notes, And Bits: The Case for Legal Tender on the Internet", *Harvard Journal of Law and Technology*, Volume 10. No. 2, Winter 1997.

be undetectable and untraceable. The capability of accessing an account from beyond national borders raises the question of how to determine regulatory or investigative jurisdiction when on line activity might indicate money laundering. Thus, despite the formal applicability of the law, many question its continuing effectiveness in a world, which has accepted e-cash as a means of exchange.[32]

It may be possible to limit e-cash transactions to the small micro purchases to which they are best suited. While such a limitation would not make e-cash money laundering activities more detectable, it would make them less practicable.

Another possible solution is to use one-way anonymity in e-cash transactions i.e., the purchaser remains anonymous but the seller dos not. This is the method used by DigiCash and its issuing banks (Mark Twain Bank in the United States and Merita Bank in Finland). 33

Still another solution is to define a class of suspect transactions and isolate this class for recording. In the proposed system all e-cash tokens must go through the automatic clearance system upon receipt. Thus, it is possible for the system to record the identity of the receipt, even though it normally would not do so in order to preserve anonymity.

Though less satisfactory from a law-enforcement perspective a more reasonable solution along these lines may be recording the receipts of only suspect recipients (rather than suspect transactions)

[32] Eric. Hughes, supra note 30. It may appear that e-cash will not be worse in this regard than the electronic funds transfers and criminals can already use. It must be understood, However,, that electronic funds transfer do not guarantee anything like the anonymity of the e-cash transactions proposed here.

[33] See *E- cash and Crime*(1997 <http://www.digicash.com/ecash/about. html>.

and only under a court order.[34] Though it would not catch all criminal activity, this system seems the most appropriate in as much as recording would attach only if there were a probable cause.[35] The solution is also easily administrable, fitting well within the established framework for issuing search warrants.

However, some argue that the interest and activities of governments in fighting money laundering is directly contrary to the interest and activities of those seeking to develop anonymous digital commerce and e-money. Clearly law enforcement agencies that are responsible, for example, to monitor money laundering, are very concerned about the development and proliferation of anonymous, non-traceable electronic payment products. In this regard it can be said that while taking any decision government should also keep in mind the interest of private sector in developing more efficient money and payment system.

Regarding other illegal activity some observers fear that e-cash systems will facilitate embezzlement by members of the banking industry.[36] While current regulated bank auditing schemes have time lags on the order of days, e-cash transactions are almost instantaneous. Thus, a thief stealing e-cash could easily disappear before the audit uncovered any evidence of foul play. However, there are currently algorithms for instantaneous on-line auditing that would identify improper activity while maintaining anonymity of individual accounts and transactions.[37] By modifying bank regulations to require

[34] This solution assumes that the technology can be designed in such a way that the government can reliably record e-cash transactions. Joshua, B. Fonuissor, supra note 31.

[35] *Cf Katz v United States*, 389 U.S. 347 (1967) (holding that the warrant less wiretapping of a public telephone booth unconstitutionally denied the defendant's reasonable expectation of privacy.

[36] Hughes, supra note 30.

[37] Ibid.

such on-line auditing at least with respective e-cash embezzlement problem could be largely avoided.

The embezzlement problem may be more severe if unregulated non-bank entities such as Microsoft are allowed to mint and issue e-cash. With no regulatory framework to guide on line auditing, insider theft could become nearly impervious to direct governmental control.

TAXATION

E-cash presents a potential problem for income tax collection. The technology makes it quite easy for individuals to store vast sums of e-cash in offshore accounts- that is, on computers located outside the concerned states. And thus, hiding income to avoid paying income taxes.[38] Where as in pre Internet commerce, this would be an unrealistic option for most people because they would have to involve a domestic bank at some point in their transactions, Cyber banks could now issue untraceable currency that could be negotiated internationally. Furthermore, the transfer of such currency could be completed directly between the banks and account holder through personal computers, thus never creating any traceable information trail that is accessible to revenue officials. Already members of traditional tax havens are offering numbered and coded bank accounts combined with such services such as international wire transfers on-line and other on-line payment options.

Other thing parties engaged in international tax evasion and money laundering schemes avail themselves of the bank secrecy laws that tax haven countries provide. From the standpoint of the would be

[38] "When global digital cash becomes a reality, taxmen will have their work cut out deciding how to access assets that might be stored on a different computer in a different country every day, even assuming that they could ever find the assets or the computers". "Electronic Money: So Much for the Cashless Society", *The Economist*, Nov. 26, 1994, at 21.

tax evader, the optimal bank is one that is at least as accessible and well run as any local institutions, but that remains beyond the reach of the domestic tax authority. Not only the bank's holdings should be impervious to tax investigation, but also its dealings with its depositors and debtors, regardless of their location.

In addition to facilitating tax evasion in the form of hidden cash deposits, the availability to consumers and businesses of secure offshore electronic financial intermediaries may have an impact on corporate tax revenues from the domestic banking sector.[39]

Some commentators may argue that few of these characteristics are new and that many of the problems they pose for tax administration are similar to those posed by mail order business or by developments in the communication sector in 1970's. But few would dispute that the speed, global access and automation of functions provided by communications on the Internet, the mobility of offers and the potential for new payment systems creates a qualitative difference in the way existing activity can be carried out and taxed. As we can see that unaccounted payment system create the same tax evasion potential as is created by cash, but without the limitation of paper money. The principles, which govern offshore banking, are similar to those, which govern traditional banking, but the ways in which banking over the Internet may operate in the future will make a crucial difference to the ability of tax authorities to counteract international tax evasion and avoidance. Traditional banking systems, which today are characterized by a small number of very large banks, may be transformed by the availability of a large number of banking facilities on the Internet operating in an offshore

[39] "Electronic Commerce: The Challenges to Tax Authorities and Taxpayers: An Informal Round Table Discussion between Business and Government", Turku, OECD. Nov. 1997, at http://www.oecd.org/daf/fa/E-com/discusse.pdf

environment. This may make it more difficult for tax authorities to 'piggy-back' on the reporting requirements that central bank traditional place on their domestic banking sector.

CROSS BORDER ISSUES

Money and payment systems are by their very nature, multi-jurisdictional products. If there is one thing that is meant to be in commerce, it is money. Thus, the creation of new global electronic payment instruments and systems raises a threshold issue- whose laws apply? While today, there is a well worn path of understanding regarding the application of check clearing, ACH, credit card, Fed Wire and other traditional payment systems rules, the development of new forms of money and new payment systems that are based in Cyberspace necessarily raise jurisdictional questions. Which state or country will regulate the activities of the entity or the movement of the electronic value it creates?[40]

Two basic scenarios for cross border usage of electric money can be envisioned. First, consumers could use prepaid cards issued by domestic institutions to make payments to foreign- based merchants, for example, while traveling, or in making purchases over a computer network. In this case, consumer and the issuer may be located in one country, while the merchant is located in another. Second, an issuer in one country could issue electronic cash to consumers in another country, potentially in the consumer's home currency, for use at either domestic or foreign merchants. The second scenario could raise more difficult issues; like traditional banking, cross-border issuance of electronic money could limit the reach of national laws and regulations, particularly in the consumer's area, or create

[40] American Bar Association, *Achieving Legal and Business Order Cybserspace: Jurisdictional Issues Created by the Internet* (July 2000), available at www.abanet.org/buslaw /cyber.

jurisdictional ambiguities.[41] As a result, some countries may be concerned that issuers of electronic money have incentives to incorporate or establish facilities in countries with the least stringent regulatory requirements, giving rise to "regulatory arbitrage".

To the extent that new forms of money and payments system are to succeed, certain level of predictability and certainty is necessary so that the sponsors and participants can fairly evaluate the rules that will apply and estimate their obligation and liabilities. Of course, uncertainty about jurisdiction for application of consumer protection regulations on enforceability of contracts for electronic money products could discourage cross border usage. Incompatible laws across countries might potentially hamper or preclude cross-border operation of electronic money schemes in some instances. For example, if they prohibit the transmission of personal data across borders.

The Task Force[42] on stored value cards (U.S.A) believes that the only way for parties involved with these new payments products to protect themselves effectively is by knowing in advance what law will govern the use of these new products. The Task Force anticipates that most of the new payment product will rely on choice- of- law provisions in contracts to establish the law that governs duties and rights of the users and issuers. It further believes it would be helpful to have a uniform choice- of- law rule, particularly for products designed for national and international use. The rule could allow

[41] Electronic Money (Group of Ten) Consumer Protection, Law Enforcement, Supervision and Cross Border Issues. Group of Working Party Report Basle, 1998, p.27. available at http://www.bis.org/publ/gten01.pdf.

[42] "A Commercial Lawyer's Take on the Electronic Purse: An Analysis of Commercial Law Issues Associated With Stored Value Cards and Electronic Money: By the Task Force on Stored Value Cards", *The Business Lawyer*, vol. 52, Feb. 1997.

parties to select the governing law in contract and provide a default rule where such a contract provision does not exist.[43]

II) APPLICATION OF LAW OF EVIDENCE

Almost all evidence to prove facts in litigation involving the Internet will be computer generated. This is primarily because technology today only allows for Internet usage through computers.[44]

Computer generated documentary evidence will be of three types. First will be calculations or analysis that are generated by the computer itself through the running of software and the receipt of information from other devices such as built in clocks and remote sensors. This type of evidence is termed as real evidence.[45] Real evidence arises in many circumstances. If a bank computer automatically calculated the bank charges due from a customers based upon its tariff, the transaction on the account and the daily cleared credit balance, the calculation would be a piece of real evidence.

Then there are documents and records produced by the computers that are copies of information supplied to the computer by human beings. This material is treated as hearsay evidence. Cheques

[43] Alternatively, a uniform rule could be established that makes ineffective any choice- of- law provision relating to stored obligations that would operate to deny user of the consumer protection they would be offered in the state in which they are domiciliaries. That way, commercial parties would be free to contract or to be subject to whatever system rules are created but consumers would be guaranteed at least the level of protection afforded by their home states. Issuers, in turn would be free to avoid particular states by refusing to offer storage devices to merchants to vendors in those states.

[44] However,, technology is fast growing embracing mobile technology, where users can access the Internet, use E-mail, send and receive faxes etc. by mobile phones. Also a mushrooming industry is Internet service through television and cable companies. Either way all these modes of communication involve processing the transaction through a mechanic device. This is the crux of the issue, Nandan Kamath, *Law Relating to Computers Internet and E-Commerce; A Guide to Cyber Laws*, (Delhi 2000), p-51.

[45] Real evidence is defined as evidence of a tangible nature from which the tribunal of fact can derive information by using its own senses, Peter Murphy, *A Practical Approach to Evidence*, (London, 1988), p.186.

drawn and paying in slips credited to a bank account are hearsay evidence.

Finally there is derived evidence, which is information that combines real evidence with the information supplied to the computers by human beings to form a composite record. This, too, is usually treated as hearsay evidence. An example of derived evidence is the figure in the daily balance column of a bank statement since this is derived from real evidence (automatically generated bank charges) and hearsay evidence (individual cheque and paying in entries)

Now that the kinds of evidence have been identified, it would be logical to look into the admissibility of the above.

The UNCITRAL Model Law on Electronic Commerce (1996) deals with the admissibility and evidentiary weight of data messages in *Article 9.* The purpose of *Article 9(1)* is to establish that data massages should not be denied admissibility as evidence in legal proceedings on the sole ground that they are in electronic form. It puts emphasis on the general principle stated in *Article 4* and is needed to make it expressly applicable to admissibility of evidence, an area in which particularly complex issues might arise in certain jurisdiction.[46]

Both *IT Act 2001 and EC Act* has almost the some provision.[47] Further, the *Model Law* mandates that if there is a legal requirement of an original, this requirement will be met by a data message if it

[46] Article 9(1) deals with admissibility, while paragraph (2) of the same article deals with evidential weight of data messages.

[47] Both provisions provide that information (IT Act) or records or signature (EC Act) 'shall not be denied legal effect, validity or enforceability solely on the ground that they are in electronic form.' "The IT Act" though is wider in sweep as it uses the teen information" as opposed to the (EC Act)

satisfies the two tests laid down in *Article 13.*[48] The criteria for assessing integrity are also mentioned. Digital signature can also be used to ensure the integrity of messages or information. Despite the many advantages of digital structure, they lack several important features. For example, the lack of a built in verifiable time/data stamp is a flaw in current digital signature technology. Although a digitally signed message is dated at the moment of sending, the date and time can be manipulated easily, and therefore are untrustworthy. The only currently available method for verifying a digital signature is an independent time/date stamp from a Certification Authority (CA).[49] The CA must first verify the time and date the message was received from the Subscribe, the CA then forwards the message with time/date stamp to the intended recipient.

Although even this method of CA verification can present problems. One implication of the inability to ensure an accurate date/time stamp on a digitally signed message is the difficulty in proving the exact time the message was sent. The CA's date/time stamp only shows when the message was received from the subscriber. Thus, a party relying upon the date/time stamp of the CA can only prove that the subscriber sent the message at some date or time prior to date or time stamped on the message. A litigant attempting to prove the exact time the message was signed by the anchor would have to rely upon extrinsic evidence. Despite these difficulties the model law states that information in the form of a data message shall be given due evidential weight, after considering the

[48] The twin tests are: (a) there exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form, as a data message or otherwise; and (b) where it is required that information be presented, that information is capable of being displayed to the person to whom it is to be presented.

[49] See Lawrence Pinsky, *Digital Signatures: A Sign of the Times*, at <http://ww.lsus.edu/classes/csc/spring98/March24/GORYDETL html> Dr. Pinsky's paper provides more detailed explanation of the mathematical process used in digital signature encryption.

reliability of the manner in which data message was generated, stored or communicated, reliability of the manner in which the integrity of the information was maintained, the manner in which the originator was identified, and any other relevant factor.[50]

Thus, an electronic record should be admissible, be interpreted to constitute a document, and the data comprising the record should be taken to be a writing. There is one last hurdle that arises in the content of admissibility of electronic records. This is the rule against hearsay.[51]

The question that arises in the context of electronic documents is that since the document is subject to traceless tampering (because of electronic format) and does not state the truth of the matter contained therein, should not the rule against hearsay apply, and thus exclude the admissibility of electronic document?

Increasingly, litigants in complex commercial litigation and parties in criminal cases must rely on computer records or printouts to prove that a particular event or circumstance occurred. A computer printout has been considered an out of court statement, and when the printout is offered in court for the truth of what it asserts, it is deemed to be hearsay. The admissibility of a computer printout or record will, therefore, depends on whether it fits under any of the numerous exceptions to the hearsay rule.

As will be seen, computer stored evidence presents an issue different from more traditional record-keeping systems. At the same time, an implication for the hearsay rule posed by computer

[50] Article 9(2) UNCITRAL Model Law on Electronic Commerce, 1996.

[51] 'Evidence from any witness which consists of what another persons stated/ (whether verbally, in writing, or by any method of assertion such as gesture) on any prior occasion is inadmissible, if its only relevant purpose is to prove that any fact stated so by that person on that prior occasion is true. Such a statement may, However,,, be admitted for any relevant purpose other than proving the truth of facts stated in it", Peter Murphy, *Murphy on Evidence* 5th Edn., (New Delhi, 1988), p.172.

technology and use is that such technology will make computerized evidence potentially admissible under other hearsay exceptions. One such example is the Business Records Exception, which is applicable to electronic communications used in the regular course of business. A computer record will be admissible generally under this exception if it was the regular business practice to create the computer information.[52] However, if the court finds that the source of the information method, or circumstances of the preparation indicate a lack of veracity, the records will be excluded.

Interpretation of the Principle

However, the information of the printout as envisaged in a *UNCITRAL Model Law on E-commerce (1996) and IT Act 2000*, - that no record should be denied legal effect, validity and enforceability solely because it is electronic in format. However, one should proceed with care. Electronic records are vulnerable to tampering and there is no foolproof way of authentication, and the acceptance and reliance on such forms of evidence should be tailored to the needs of the case. The judges should exercise careful discretion as to testing the integrity of the data, there must not be any strict method of deciding this, as integrity depends on system to system.

III) SECURITY ASPECTS OF ELECTRONIC BANKING

Security issues are a major source of concern for every one both inside and outside the banking industry. Security is required at all phases of the information cycle gathering, creating, processing, storing, transmitting and deleting.[53] E-money increases security risks,

[52] See Mark S. Dischter and Michael S. Burkhardt, Electonic *Interaction in the Work Place: Monitoring, Retrieving, and Storing Employee Electronic Communications in the Workplace* available at <http://www.mlb.com/speech1.html>

[53] Guidelines for the Security of Information System, 1992. OECD, available at http://www.oecd.org, p.18.

potentially exposing hitherto isolated systems to open and risky environments. All retail payment systems themselves are vulnerable in some way. E-money products raises some more issues such as authentication and non-repudiation, integrity and privacy.

Security breaches could occur at the level of the consumer, the merchant or the issuer, and could involve attempts to steal consumer or merchant devices, to create fraudulent devices or messages that are accepted as genuine, to alter data stored on or contained in messages transmitted between devices, or to alter the software functions of a product. Security attacks would most likely be for financial gain, but could also aim to disrupt the system. Security breaches essentially fall into three categories, i) breaches with serious criminal intent (e.g. fraud, theft of commercially sensitive financial information), ii) breaches by 'casual hackers' (e.g. defacement of websites or 'denial of service' causing web sites to crash), and iii) flaws in systems design and/or set up leading to security breaches (e.g. genuine user seeing/being able to transact on other users' accounts).[54] All of these threats have potentially serious financial, legal and reputational implications.

Now we will examine some of these security breaches separately. However, all the three categories of security breaches are interrelated.

Fraud

Fraud could be accomplished by creating fraudulent electronic representations of electronic money that are accepted as genuine by the issuer or by other participants, or by stealing devices of data from another participant. If such fraudulent balances could be successfully

[54] Carol Sergeant, *E-Banking – Risks and Responses*. 2000 available at, www.fsa.gov.uk/pubs/speeches/sp46.html

exchanged for currency or other readily transferable forms of money or physical assets, this would cause financial loss to the issuer or other participants.

Other way of committing fraud could be the creation of a new device that is accepted by other devices as genuine. The objective would be to duplicate a genuine card, including its existing cryptographic keys, card balance and other data. Alternatively, an attacker could attempt to create a card that would function as a genuine card but would fraudulently contain balances without a corresponding load transaction and payment to the issuer.

The other type of fraud could be to modify data stored on a genuine electronic money device in an unauthorized manner. For example, if the balance recorded on a device were fraudulently increased without other evidence of tampering or damage to the card, the holder could perform transactions with the device that would appear genuine to the merchant terminal.

Alteration of data or functions on a device could be attempted through exploiting security weaknesses in the operating system or by physical attacks on the chip itself. In software- based systems, data stored on a consumer's device could be altered directly if not protected by software functions, or software could be modified to allow unauthorized alternation of data by the user. In a note-based system, a user could duplicate data representing electronic notes and attempt to use the notes to purchase goods and services.

Attackers could attempt to change the data or processes of a device by deleting messages, replaying messages, substituting an altered message for a valid one or observing messages for the purpose of attempting cryptographic attack. Communications between devices could be intercepted by outside attackers when sent across telecommunications lines, through computer networks or through direct contact between devices.

An attacker could change the destination device of messages during transaction by diverting a message sent over a computer network via electronic mail or by removing a smart card from a reader and inserting other with a lower balance. A smart-card reader device could be simulated and used to send false messages to the smart card; alternatively, a fraudulent smart card could be used in a valid card reader, with the intention of causing the card reader device to perform unauthorized functions. The critical date in a message, such as the transaction amount, could be changed. A message authorizing the loading of funds from a valid ATM or other terminal could be copied and replayed to a card from a fraudulent terminal. Transaction data transmitted from a merchant terminal to the acquirer could be duplicated in an attempt to receive double credit for the transactions. 55

As with traditional payment instruments, internal theft within an electronic money supplier could also be an avenue for attack. For example, one of the most significant threats to an electronic money system would be the theft or compromising of the issuer's cryptography keys by either an insider or an outside attacker.

Fraud would also be attempted through repudiation of transactions made with an electronic money payment.[56]

[55] The security of a system against the risk of duplication or "replay" of message is sometimes known as "idempotency", Security of Electronic Money, Report by the Committee on Payment and Settlement Systems and the Group of Ten Countries, Basle, August 1996, available at, www.bis.org/publ/cpss18.pdf.

[56] In practice, the potential for repudiation of transaction is not unique to electronic money products, and has not been a major source of fraud in existing payment instruments compared with theft and counterfeiting. Security of Electronic Money. Report by the Committee on Payment and

Prevention measures

Security features in electronic money systems, as well as in other payment system, are designed to safeguard the integrity authenticity and confidentiality of critical data and processes, as well as to protect against losses due to fraudulent application or repudiation of transaction. Tamper-resistant features of these cards are aimed at protecting the data and software from unauthorized observation or alteration. These highly sophisticated features include both logical (software) and physical (hardware) protection. Hardware protection features would very probably prevent the contents of a single chip from being successfully analyzed or "reverse engineered" even by sophisticated attacker.

In software-based electronic money systems, by definition, there is no physical protection built into the product itself that would prevent the user or an outside attacker from observing or tampering with the data or software used in the system. The software itself typically contains access control mechanism to prevent the user from changing or duplicating data in an authorized manner.

Meanwhile, some scientists remain unconvinced that smart card can be made tamper proof. Bell communication research scientists claim to have found a security flow in public key coding systems that would allow wrongdoers to counterfeit stored value cards, including those used by Mondex and other European companies.[57] In addition, Israeli computer scientists claim to have discovered security flaws in secret key data coding systems. Such as the American Data Encryption Standard. Deliberate application of heat or radiation

Settlement Systems and the Group of Computer Experts of the Central Banks of the Group of Ten Countries, Basle, August, 1996, available at www.bis.org/publ/cpss18.pdf.

[57] S.F. Chron,"Possible Defect in Smart Cards", *Scientists*, Sep. 26, 1996, at B2.

causes the computer chip in the card to generate an error, which can then be used to obtain the code key and copy the card.[58] It is also possible to modify program register values without physically tampering with the device case. For example, subjecting the device to ion, X-ray or ultraviolet radiation can flip bits in memory that may alter the value stored in a cash based register.[59]

Cryptography

Cryptography is one of the main components of fraud prevention in all electronic money systems. There are a number of different cryptographic techniques that are used for different purpose in electronic money systems.

Encryption is a technique used to protect the confidentiality of data during transmission or while stored on a device. Encryption is particularly important for certain types of sensitive data used in security processes, such as cryptographic keys.

Cryptography is also commonly used in electronic money products to authenticate the identity and privileges of devices in transactions. Digital signatures are one means of authenticating the identity of a device that sends a particular message and may also be used to prevent fraudulent repudiation of transactions.

Cryptography is commonly used for verifying the integrity of messages exchanged between devices and electronic money system that is, detecting whether or not a message has been altered before reaching its intended recipient. Message authentication codes may be used for this purpose. Creation of a fraudulent message that is

[58] Kerry Lynin Machinotogh, "How to Encourage Global Electronic Commerce: The Case for Private Currencies on the Internet", *Harvard Journal of Law & Technology*, vol. 11, 3, Summer 1998, pp-749.
[59] Anup K. Ghosh, *E-commerce Security: Weak Links, Best Defences*, (New York, 1998), p 141.

successfully received as a valid message would require knowledge of cryptographic keys. Cryptographic techniques can also be used to protect the integrity of software transmitted over open networks.

Systems using cryptography can be attacked through weakness in their implementation. For example, the software that performs cryptographic functions must be properly designed and implemented, and any use of random data to generate keys must be truly random or patterns should be recognized that would aid in a brute-force attack. Extensive testing of the product is the most effective means of correcting such implementation weaknesses.[60]

All electronic money systems involve cryptographic keys that must be kept secret, or secure against unauthorized observation, in order to prevent unauthorized duplication or alteration of data. In card-based systems, various security measures have been developed to safeguard keys in storage on devices and in transmission between devices. For software- based systems, in particular, those that involve access to open computer networks, storage of cryptographic keys poses greater challenges, because the user's device cannot be assumed to be secure with any degree of certainty.

Certification authorities (CA's) may be necessary for systems employing asymmetric cryptography. CA's are typically centralized databases that certify, store and distribute public keys and information identifying the holder of a corresponding private key. Owing to their limited use of active asymmetric cryptography, most electronic money systems provide their own CA facilities. Those that

[60] For example, such weakness have been uncovered and published in certain network access software following wide spread market introduction, Security of Electronic Money supra note 55, p. 16.

require widespread, routine distribution of public keys for each user face greater challenges.

Online Authorization

Online authorization is generally considered to be necessary for all transactions in software based electronic money products.[61] In order to deter a user or outside attacker from copying a particular electronic note and "spending" it several times over, a central authority must verify each transaction sequentially on the basis of information about notes that have previously been issued and redeemed. Such methods would not necessarily prevent fraud, however, but might only detect it after the event. In some systems, the use of sophisticated cryptographic techniques would enable the issuer to determine which party instigated the fraudulent transaction.

Other Measures

Electronic money systems may provide additional levels of security against fraud as well as malfunctions by requiring individual devices to perform additional verification during transactions. These could include, for example, verifying expiration dates, numbers of transactions executed with the device, balances on the devices (against its maximum balance) and the maximum balance itself.

Finally, procedural and administrative controls provide important safeguards against attempted fraud. Tasks such as card manufacture, cryptographic key management and card personalization are subject to strict access control and are separated geographically and administratively, increasing the number of employees that would

[61] Even the use of asymmetric cryptography by the consumer, merchant and issuer may not be sufficient if users' private keys are stored on standard personal computer rather than a specialized handware device, Security of Electronic Money, supra note 55, p. 17.

need to collude in order to gain enough information to compromise system security.

Detection Measures

In most of the card-based systems analyzed, each transaction can be identified by a unique number, based on the card's serial number and its transaction counter, which increases by one increment for each attempted transaction. In the case of note-based systems, each note has a unique serial number.

Security verification by the issuer or central operator involves verifying message authentication codes, transaction sequence numbers, information about previous payment and load transactions and other information contained in transactions or stored in devices. In note-based systems as mentioned earlier, serial numbers of notes used in transactions can be verified against a central list. Some verification of cryptographic information may be performed at the central operator or issuer level, using cryptographic keys that are not contained in merchant terminals. This provides an added level of security against the compromising of a merchant terminal.

Interactions With a Central System

Online interaction with the issuer or central operator of an electronic money system is a commonly used security feature of card-based systems. Such interaction allows the central operator to check security parameters on the card for consistency, to update security measures on the device, such as cryptographic keys, and, in some cases, to gather additional transaction data from the device.

Security measures for electronic money products are highly complex. There is no single security measure or set of measures that can be said to be sufficient for a particular product. Thus, it is more important to focus on the overall security risk management approach for a particular product rather than on the use of individual measures. However, security measures at each level of an electronic money system (e.g. consumers, merchants, financial institutions) should be commensurate with the degree of risk at that level.

Security of protocols and servers.

The TCP/IP protocol, which is the core component of the Internet, has been designed to provide a high level of resiliency with a minimum level of overhead network information in the messages. However, the TCP/IP protocol does not able to provide for a high level of security. The following measures have been aimed at providing additional security: (1) the development of an additional protocol (Netscape Secure Socket Layer) to establish encryption between Internet client and Internet server, (2) the development of an extension of the http language (s-http, secure http), which establishes a protocol by which an Internet client and an Internet server can negotiate the appropriate level of security before exchanging information; (3) an initiative by the IETF to extend the TCP/IP protocol to allow certain security functions.

Security Evaluation

Both protocols (TCP/IP) and components (mainly Unix based servers) of the Internet have security limitations that make the Internet, by itself, an unsafe environment. It is therefore the responsibility of its users and products suppliers to ensure secure transfer of information or payment transaction over the Internet. Public key cryptography and digital signatures are the key technologies, which provide for privacy and authentication.[62] In fact the use of these technologies (provided that keys are stored in a tamper resistant manner) can be viewed tantamount to creating private networks over the public network.

However, encryption, which is the basic requirement for electronic banking, raises a plethora of legal problems including: will courts tolerate the production of pivotal evidence in encrypted form? Will a party's counsel produce information or date without first having it decrypted, leaving the opposing counsel produce information or date without first having it decrypted, leaving the opposing council with a task of "cracking" the encryption? On what basis could counsel claim such a data file was irrelevant or privileged? Will the producer have the onus of contacting the ex – employee in the hope that the employee will remember the password necessary for decryption? Will the courts compel individual to provide their passwords?

The other problem is that, strong encryption is a double-edged sword. Law abiding citizens using strong encryption to protect their trade secrets and personal records could be lost forever if the decrypt key is lost. Depending upon the value of the information, the loss could be quite substantial. Encryption can also be used by criminals and terrorists to reduce law enforcement capabilities to read their communication. That is why many countries are having export import control on cryptography, which is detrimental to the growth of security measures.

In conclusion, we can say that fundamental objectives that security arrangements of e-money products should try to achieve are to:

[62] PGP (Pretty Good Privacy) is an example of software application that is used to provide such extra security, Security of Electronic Money, supra note 55 p. 48.

i. Restrict access to the system to those users who are authorized;

ii. Authenticate the identity and authority of the parties concerned to ensure the enforceability of transactions conducted through the Internet;

iii. Maintain the secrecy of information while it is in passage over the communication network;

iv. Ensure that the data has not been modified either accidentally or fraudulently while in passage over the network; and

v. Prevent unauthorized access to the bank's central computer system and database.

IV) PRIVACY IN ELECTRONIC BANKING

The electronic payment system must ensure and maintain privacy. Every time one purchases goods using a credit card, subscribes to a magazine or access a server, that information goes into a database somewhere.

Furthermore, all these records can be linked so that they constitute in effect a single dossier. This dossier would reflect what items were brought and where and when. This violates the unspoken laws of doing business; that the privacy of customer should be protected as much as possible.

The new electronic products and services have raised increasing consumer concerns about potential invasions of their privacy from in unauthorized access to and collection, dissemination and/or use of their personal information. For this reasons, while there are numerous other pressing legal and competitive issues raised by the new electronic products and services, issues of information privacy- which may be defined as an individual's claims to control the terms under which personal information, including both personal data and transactional data, in acquired, disclosed and used- will likely play a very significant role legally and operationally as these products and systems continue to develop.[63]The need to protect the individual is reflected in new restrictions on the collection, storage and public availability of this data.[64]

Actually sound practices require the ability to track and verify that the proper exchanges occur. However, consumers may fear that their financial, credit and spending information derived from e-money transactions or products could be used without their knowledge or permission. And these fears will be wide spread and strongly held when e-banking and the use of e-money becomes more wide spread. Here a question arises how to prevent criminals from obtaining a consumer's account information? Therefore, many parties want the options of anonymous financial transactions. However, it is difficult to be widely accepted due to security concerns and money laundering. Even so, to achieve wide spread confidence, all participants in the systems such as banks, other issuers, consumers and merchants, must have certain basic information about the rules governing the use of e-money products. Any e-cash system must balance the privacy of its users with the law enforcement benefits of traceable transactions.[65] Banks and financial service companies can buy, sell, trade, and share their customer's financial information, including accounts numbers and balances. Courts have consistently ruled that this information is

[63] Ellen d' Alelio, "The Challenge of Information Privacy in the World of Cyber Banking, Electronic Banking Law and Commerce Report", *Glasser Legal Works*, (New York, June 1996), p 88.

[64] See e.g. The European Union's Directive on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data, 94/96/EC (October 1995).

[65] Joshua B. Konvisser, supra note 31, at 344.

the property of the company, not the customer.[66] However, many banks have curbed the practice because of public outcry.

However, it is not possible to live in human society without interacting with others, and this requires the sharing of personal information. A privacy law thus consists of two elements:

i) A definition of the circumstances in which third parties have the right to collect, use and disseminate personal information about others; and

ii) A mechanism for preventing collection, use and dissemination outside those limits.

The first of these is largely culturally determined, with nation states taking very different views of what information should be treated as private. For example, in Sweden tax returns are publicly available information. The second also reflects cultural differences, and in particular the national view as to what role the state should play in protecting privacy. At one extreme, the US tends to have the question of privacy to be dealt with by state legislation and common law, although there are some laws, which apply to particular sectors of industry or the administration.[67]

The position is quite different in those countries, which take the view that the state should play the primary role in protecting privacy. The clearest example is the European system of data protection, which initially covered only personal information, held in

[66] Daniet Tynan, "Privacy 2000 In Web We Trust?" *PC World*, Vol. 18, No. – 6, June 2000, p. 107.
[67] See e.g. US Electronic Communications Privacy Act. 1986, applying to the federal sector; US Children's Online Privacy Protection Act 1988.

computerized form, but has recently been extended to cover organized collections of manually accessible information.[68]

Current constitutional, legislative common law, and state privacy protections fail to provide consumers with comprehensive privacy protections and, as such, offer little, if any, privacy protections against information collection on Internet. Indeed, the statutory protections are sectorial in nature however, it can be said that promises made in the privacy policy are as much a part of transactions as what is delivered to the consumer. If a company fails to observe its policy, it can be sued under various common laws.[69]

The online privacy debate centers on this issue- is comprehensive legislative regulations safer for the consumer and more efficient for the industry or would public policy be better served by allowing the industry to continue it attempts to establish a form of self-regulations?[70]

In the modern information economy, the protection of privacy has an economic element as the collection of personal information is wide spread, and the information gathered is put to such diverse usage as marketing or as nefarious as fraud. Thus, exerting control over who has access to personal information has a definite economic value. Cryptography can be used as a tool to keep personal information private and prevent such unauthorized use.[71]

Banking industries response to consumer concerns about privacy issues has not in the past been comprehensive. Some but not

[68] Directive 95/46 EC on the protection of individuals with regarded to the processing of personal data and on the free movement of such data, OS No. L281, 23.11.1995.

[69] Daniel Tynin, *Privacy 2000 In Web We Trust?* available at, <www.pcworld.com/janoo/info__brokers.>

[70] Lee S. Adams and David J Martz, "Developments in Stored Value Cards and Cyber Banking", *The Business Lawyer*, vol 54, May 1999 p. 1382.

[71] Marcus Maher, Note, *International Protection of US Laws Enforcement Interests in Cryptography*, available at, <http:// www.richmond..edu/jolt/maher.html>

all individual financial institutions and some financial service providers such as Visa, Master card have developed or are developing model privacy codes.[72]

Since no express legislation has been established for banking secrecy, it can be assumed that this requirement would be met under already existing law. Even if the application of banking secrecy does not emerge expressly from the contract with the bank, it is still assumed in general that banking secrecy applies. It can be said that the legal institution of banking secrecy is anchored in the constitution.

Beyond the subject of banking secrecy, it should be pointed out, that of course, any storing of data is subject to the restrictions and requirements set forth in the data personal law which is emerging. This is of significance, first because banking secrecy provides protection only against the data being passed on by the cyber banks to third parties, whereas the banks internal storage and use of data is possible without restriction. Second, data is also stored, for example, on the premises of the payee, who, of course is not subject to banking secrecy.[73]

Essentially it follows there from that the storage and processing of personal data within the framework of electronic fraud transfer must be reduced to the absolute minimum. The safeguarding of this principle is, therefore, also a fundamental requirement to be satisfied by any system, which aspires to achieve practical significance.[74]

[72] This is a particular area of concern for online banking services where the risk of unauthorized access and data alteration increases exponentially in a network environment. The availability/ exportability of effective encryption to achieve security of online data communication has become a subject for much debate, see, e.g. Philip S Corwin, "Encryption: From Obscurity to Political Controversy", *American Banker, Future Banking*, May 20, 1996 at 8A.

[73] Dennis Campbell (Eds) : *Law of Online Business: A Global Perspective*, (London, 1998), p. 417.

[74] Ibid, p 418.

The banking industry should start by undertaking a systematic and detailed appraisal of the privacy issues raised the new electronic products and services, and analyzing the impact of governmental initiatives such as the EU Directive on banks, their holding company parents and their non-banking subsidiaries, particularly with respect to their data processing activities. This effort should evaluate, for example: (a) the confidentiality and security of the personal information: is it protected against unauthorized access, modification, use or dissemination? (b) the quality of the personal information: is the information accurate, complete and current? (c) the disclosure made to the data subject regarding the collection of personal information: is the data subject informed that the data are being collected? informed of the purpose of collection, its intended use and period of retention?

International aspects of privacy and data banks

For a number of reasons the problems of developing safeguards for the individual in respect of the handling of personal data cannot be solved exclusively at the national level. The tremendous increase in data flows across national borders and the creation of international data banks (collections of data intended for retrieval and other purposes) have highlighted the need for concerted national action.

One basic concern at the international level is for consensus on the fundamental principles on which protection of the individual must be based. Such a consensus would obviate of diminish reasons for regulating the export of data and facilitate resolving problems of conflict of laws. Moreover, it could constitute a first step towards the development of more detailed, binding international agreements[75].

However, problems regarding the choice of jurisdiction, choice of applicable law and recognition of foreign judgments have proved to be complex in the context of trans border data flows. Similarly, opinions may vary on the question of exceptions, are they required at all? Of so, should particular categories of exceptions be provided for or should general limits to exceptions be formulated. However, there will never be a complete resolution of the tradeoffs between privacy on one-side and convenience, service and public policy interests on the other.

Privacy will always be a contentious problem; indeed, it's already a mess of contradictions[76].

V) BANKING AND FINANCIAL REGULATION AND CLEARING AND SETTLEMENT ARRANGEMENT FOR ELECTRONIC MONEY TRANSFER

BANKING AND FINANCIAL REGULATION

The development of electronic payment systems based on the Internet raises a whole range of regulatory issues. A effective global low value electronic payment system will certainly remove what is currently a major obstacle to the expansion of trade and commerce. Traditionally, central banks have four duties: they manage monetary policy, they supervise the payment system, they promulgate regulations, and in many countries, they supervise the banking system as a whole. Each

[75] See OECD Guidelines on the Protection of Privacy and Trans Border Flows of Personal Data, available at http://www.oecd.org

[76] Peter Keen, "Designing Privacy for Your E-business". *PC Magazine*, Vol. 19, No. 11, June 6, 2000. p. 133

of these roles is going to be affected by the development of e-money to some extent.

First question is whether existing banking or other regulations apply to e-money arrangements. It's answer depends on its status. If it is given legal tender status then only entity issuing e-cash will be the central government, and no new regulatory frame work will be necessary. Because e-cash is fungible with hard cash in this system and the current framework of bank regulation will suffice, if it is decided that e-money balances are a form of deposit, any existing regulations concerning deposits are likely to apply. However, even in this case there may be a need to review the regulatory approach, for it does not necessarily follow that the existing regulations will be the most appropriate for e-money schemes.

Second issue which is related to the status of e-money is, whether electronic money be considered as negotiable instrument. As with the question of assignment, arguments based on the requirement of writing and signature must be considered as vulnerable. One of the problems is to determine precisely what the instrument might be. For example, when a payment is made with a "stored value card" the card itself is not delivered. *Galvin* considers carefully whether the "stored value" may be negotiable, concluding that it is probably not.[77] However, the view taken here is that "Stored value is nothing more than an accounting mechanism so that nothing is "delivered" or transferred", when the card is used. Alternative technology stored value cards would not even have electronic interaction with terminals, so the question could hardly arise. Generally, the question of negotiability is not relevant to the payment system as such. The other

[77] Andrew Galvin, "The Legal Nature of Stored Value Card Transactions", *Journal of Banking, Finance, Law, and Practice* vol.10, No. 1, 1999, pp.54-65.

way new payment products would have to be viewed as an unconditional promise or order to pay a fixed amount of money. The promise to pay associated with the new payment products is likely to be conditional, subject to the terms of a contract.[78]

Still in certain jurisdictions, because the financial institutions do add electronic signature to some forms of electronic money, they may be considered as negotiable instruments. But generally the message constituting the 'money' will not be in the form of a promise.[79] Again it is not usually contemplated that a holder may claim directly against the issuing institution.

Another issue comes into question when e-money payments are made across border (particularly with software based schemes that operate over computer networks). It may be difficult to establish to what extent, if at all, e-money schemes fall within the scope of particular jurisdictions.

Most countries require banks to be licensed or authorized by a regulatory body. The determining factor in deciding whether a financial institution falls under national banking law is normally whether it accepts deposits in that country. Thus, the definition of 'credit institution' for the purposes of EU banking law is 'an undertaking whose business is to receive deposits or other repayable funds from the public and to grant credits for its own account.[80]

The Internet bank would normally enter into arrangement with a third party in each country where it wished to accept deposits.

[78] The Task Force on Stored Value Cards, "A Commercial Lawyer's Take on the Electronic Purse: An Analysis of Commercial Law Issues Associated With Stored – Value Cards and Electronic Money". *The Business Lawyer*, Vol.52, Feb. 1997, pp. 697-698.

[79] Alan L Tyree, "Regulating the Payment System – Part I", *Journal of Banking and Finance Law and Practice,* Vol. 10, No.1, March 1999 pp. 66-68.

[80] First Council Directive 77/780/ESC of 12th Dec. 1977 on the condition of the Laws, Regulation and Administrative Provisions Relating to the Taking up and pursuit of the Business of Credit Institution OJL. 322, 17th Dec. 1977, p. 30, art.1.

Would this mean bank was accepting deposits in the jurisdiction (ie through its agent), and thus obliged to register?

An analysis of the EU jurisprudence indicates that the use of an independent intermediary to deal with customers does not amount to the establishment of a branch in that jurisdiction, even if the intermediary works solely for the foreign enterprise, provided the intermediary is truly independent.[81]

Most jurisdictions do not regulate the provision of electronic payment services per se, although some aspects of payment transactions may be regulated. This is because normal interbank electronic funds transfer systems work by moving funds from one account to another, adjusting the sending and receiving account balances and settling through a Central Bank or a correspondent account. An institution, which provides such an account, will be a deposit taker, and thus fall under normal banking regulation. Similarly, on-line credit card payments are regulated not on the basis that they are payment services, but because of the credit facilities provided to cardholders.

However, new forms of payment service are developing which do not necessarily require the manipulation of bank accounts or credit facilities, and therefore may be provided by enterprises, which do not have authorization as banks. These are generally known as digital cash or electronic money systems and fall into three main types.[82]

i) Systems which effect transfers between accounts, although the accounts are not general bank accounts but specifically limited to electronic money transactions.

[81] Chris Read, *Internet law: text and materials*, (London, 2000), p. 243.

[82]. For an explanation of the working of these systems, see sutter, *Law and Technology convergence: Electronic payment systems*; available at http://www.jura.unimuenster.de/ eclip/

ii) System where value is purchased from the electronic money service provider and stored on a smart card.

iii) Systems where the electronic money service provider pays the recipient on behalf of the payer and is then reimbursed by debiting the payer's credit card account or via an inter bank transfer initiated as a 'pull' transaction

The mere fact that the enterprise accepts money from payers will not amount to taking a deposit if the payment is consideration for providing a service, and the enterprise has no obligation to return it unless the service is not provided.[83] Most electronic money systems operate by treating the issue of digital cash as a withdrawal from the customer's deposit. Admittedly the issuer normally undertakes to accept that digital cash for re-deposit, but this undertaking will not be sufficient to allow the transaction to be classified as the transformation of a deposit from one form into another. The defining factor is repayment, which by definition requires the funds to be in the custody and control of the depository. True digital cash gives custody and control to the customer. The result is that institutions, which provide the new Internet payment services, do not need to be licensed as banks or to comply with bank supervision rules. Similarly, they also fall outside credit licensing regulations.

Another regulatory issue is, should government regulate global electronic currency? If nations accept the argument that global electronic currencies would benefit internet commerce without seriously undermining government power then other questions still remain to be answered: to what extent, and in what ways, should

[83] Ellen d Alelio and Collins, "Electronic Cash Under Current Banking Laws", in Ruh (ed) *The Internet and Business: A lawyer's Guide to the Emerging Legal Issues*, (Washington, 1996), pp 91 - 98.

government regulate companies that issue global electronic currencies.

Even if issuers of global electronic currencies would not be engaged in banking as such, two questions remain: Would the issuance of such currencies raise the same policy concerns as banking and if so, would some form of government regulation be the best way of addressing those concerns.

Global electronic currencies could raise the same policy concerns, but to a lesser extent. For example, suppose that rumours began to fly that a private issuer 'A' was experiencing financial difficulties. Then, users might begin to demand that electronic currency be exchanged or redeemed at the guaranteed minimum value. If 'A' did not have enough liquid assets to meet these demands, it might be forced into insolvency. However, this single run on a single company need not trigger a panic. The e-money would be an independently issued, managed, and denominated currency, unlike any other, and exist outside the traditional network of government currencies and banks. Holders of competing private and government currencies would have no reason to believe that 'A's financial problems spelled troubled for other, independent companies or the financial system in general.

Nevertheless, lawmakers and regulators unfamiliar with global electronic currencies could respond by passing new laws that would subject 'A' and other issuers to banking laws and regulations, such as regulatory supervision, reserve requirements and insurance. Unfortunately, this response would restrict issuance to banks.[84]

[84] In Sep. 1996, the American Bankers Association Payments System Task Force Released a Report Recommending that "Only Regulated Depository Institutions have Direct Access to the Federal Reserve's Payment Services, and Issuance of Third-Party Instruments (Such as Stored Value Cards)

The policy implications of electronic money extend beyond the realm of banking laws. As technology advances, banks are becoming "information service" companies. 'The rules, the regulations, the technology, and the different issues have to be dealt with have transcended, what, normally would confront a banking institution'[85].

There are several excellent reasons to favour, market rather than regulatory, solutions at this time. *First,* oppressive and inflexible regulations could prove harmful to the development of electronic payment systems.

Second, any legal framework for commercial transactions on the Internet should be governed by consistent principle across national borders.[86]

Third, hasty enactment or application of laws and regulations is unnecessary because global electronic currencies would not pose a significant threat to either users or the economy in the near future. Thus, government could afford to monitor the progress of these currencies and determine whether the market is providing adequate solutions on its own to safety and soundness concerns.

Fourth, restraining issuers of digital coins may be impossible. The technology required is minimal. There are enough experiences to show that countries, which see a benefit, will provide 'digital coins

Should be Limited to Regulated Depository Institutions". Joseph Radigan, "Locking up: The Money Monopoly", *U.S. Banker*, Jan. 1997, pp. 26.

[85] Randell W. Sifers, "Regualting Electronic Money in Small Value Payment Systems: Telecommunication Law as a Regulatory Model", *Federal Communications Law Journal,* April 1997, p.719.

[86] Kerry Lynn Machintosh, "How to Encourage Global Electronic Commerce: The Case For Private Currencies on the Internet", *Harvard Journal of law and Technology*, vol. 1, no. 3, summer 1998, p. 776.

havens' for operators who are prevented from operating by the regulatory bodies of other countries. [87]

CLEARING AND SETTLEMENT FOR ELECTRONIC MONEY

Most of the legal problems of electronic clearing and settlement have nothing to do with the "electronic" part of the process. But it is also true that in the absence of the electronic clearing systems, many of the problems could not have arisen.

Many of the legal problems concerning electronic clearing and settlement are related to the recovery of money already paid, usually to an insolvent entity. The problem may be circumvented in some circumstances merely by showing that payment has not occurred at the relevant time. Problems concerning the time of payment are often confused because the number of parties involved in a modern payment transaction. It is necessary to identify clearly which payment is the subject of contention[88]. The question whether the issues arising from new electronic clearing & settlement system should be settled by central bank or should it be left for participants.

Virtually all e-money schemes under development will need inter-institutional clearing and settlement arrangement. Those clearing agents usually require each issuer to maintain an adequate balance between e-money outstanding and the chosen reserve banking. However, if there is a sudden increase in demand for redemption of e-money, it may be a serious problem for the issuer. Failure to meet redemption demands in a timely manner could also lead to reputation damage. Other than the reserve requirement, issuers

[87] Alan L Tyree, "Virtual Cash Payments On The Internet", *Journal of Banking Finance Law and Practice*, vol. 7, 1996, pp. 35-38.

[88] Alan L Tyre, "Payment and Clearing Systems (Chapter III)" in David Allen (ed), *Australian Finance Law*, LBC 4th Edition, 1999, pp. 65-80.

should also be required to invest funds in liquid assets and conduct regular and comprehensive audits. Moreover, operators and overseers of inter-bank clearing and settlement systems need to ensure that such systems are sufficiently robust in terms of institutional and operational arrangements, risk management and settlement procedures. Because e-money allows a transaction to clear almost instantaneously, diligence is required to account for electronic cash and trace redemption patterns.

There are fears that concern that electronic cash systems can defeat current mechanisms, for tracking foreign exchange transactions. In addition, some schemes might offer e-money in more than one currency, which might, for example make it more difficult for central banks to measure accurately the stock of e-money denominated in the home currency.

Another regulatory issue is whether e-money products affect the monetary policy? The introduction of e-money could potentially have an effect on the demand for monetary aggregates and on the formulation of monetary policy. This will depend upon whether its primary impact is on the demand for bank reserves or on the central bank's capacity to supply these reserves.

The most important development in connection with e-money is a reduction in the demand for cash. As cash circulation is a lever by which central banks can control the money, credit expansion of private banks, and hence provide some more monetary stability. It is conceivable that a very extensive substitution could complicate the operating procedures used by central banks to set money market interest rates. However, since e-money is expected to substitute mostly for cash rather than deposits, operating techniques need not to be adjusted significantly. On the other hand, with e-money transaction, the whole process including clearing can be carried out in a matter of seconds. Such acceleration in the circulation rate amounts to an increase in the quantity of money, and increased money circulation could lead to increase inflation.

Since cash is a large or the largest component of central banks liabilities in many countries, a very extensive spread of e-money could shrink central bank balance sheets significantly. Since banknotes in circulation represent non-interest-bearing central bank liabilities, a substitution of e-money for cash would lead to a corresponding decline in central bank asset holdings and the interest earned on these assets that constitutes central bank seigniorage revenue.[89]

However, in principle, central banks have several policy options to reduce the shrinkage of their balance sheets. *Firstly*, central banks could consider issuing e-money themselves, or issuing e-money without actually operating e-money schemes themselves thus to encourage competition and incentives to innovate.[90] *Secondly*, central banks could expand the coverage of reserve requirements to cover e-money or other liabilities, and governments could grant the central banks the exclusive right to own and operate the electronic payment network. *Finally*, as an alternative to these measures, central banks might rely on off-balance-sheet transactions and, in the case of large lender of last resort operations, use private banks as their agents. Furthermore, governments could levy transactions taxes on the use of e-money by charging a tax at the time of the issue[91].

[89] Implications for Central Bank of the Development of Electronic Money, Bank for International Settlement, Basle, October 1996, pp. 7 available at <http://www.bis.org/publ/bisp01.pdf.
[90] Ibid, p.10.
[91] Mauro Cipparone, *The Role of the Central Bank in the Growing Industry of Internet Payments*, p. 3, available at http://www.geocities.com/wall street/2486.

Another issue arises, whether, the new payment systems be regarded as telecommunications networks or banking networks. Technological changes will cause a convergence among the different kinds of policy domains that exist in the current regulatory schemes. Separate banking and non-banking factions will become increasingly connected. The problem for banks is the existence of regulations that prohibit diversification and limit the use of bank- owned telecommunications networks to the transmission of financial data or information related to banking.[92]The integration of telecommunications and financial services strains traditional regulatory practices in both fields. No longer are there distinct boundary lines between the two industries. For example, "when a bank offers an online transactional service to customers, there may be some debate as to whether it is providing a regulated banking service, a telecommunications service that might be regulated (depending on the jurisdiction in which it is offered), an unregulated information processing service, or some hybrid service that has never been the subject of regulation.[93]

Yet another issue is, whether escheat laws apply to electronic cash. As a general matter, states have regulatory power over abandoned property and may use their legislative power to dispose of property within their reach, subject to constitutional projections. State laws typically include intangible property within the categories of abandoned property that they can reach, and bank deposits would fall within that category. Such escheatment statutes raise various questions with respect to electronic cash. The first is whether either (a) unclaimed funds held by an issuer is pooled balances, or (b)

[92] Randall W. Sifers, supra note 85, p. 722

[93] Ibid.

unused "value" on stored value cards or computers would fall within the applicable definition of intangible property used in the state statute. Another question is that under what circumstances electronic cash or the associated funds held by the issuer are deemed to be "abandoned". These questions can be resolved only by reference to the particular state law in question. But again problem comes here, such as how one knows when a non – traceable electronic asset, like electronic money, is subject to escheat, when it is not possible to tell where it is, where it has been or if it has been abandoned.[94]

It is, however, difficult for a Central Bank to exercise its powers over foreign companies, as this would infringe the sovereignty of other states.

VI) CONSUMER PROTECTION, CONTRACT TERMS and ALTERNATIVE DISPUTE RESOLUTION

CONSUMER PROTECTION

The use of electronic money could influence the level of costs, benefits and risks facing consumers in their day-to-day economic transactions. Potential consumer benefit could include the availability of lower cost, faster and more convenient means of payment, as well as increasing the diversity of payment options.

A whole lot of legal issues do arise in connection with these additional benefits. Like, what will happen with lost cards? What will happen when there is an unauthorized transaction? What will happen when a transaction goes wrong in some way? How are costs and charges to be distributed among the players in a smart card/digital coin system? And so on. So, it would be nice to think that "*Smart*

[94] Unif. Unclaimed Property Act (1995), available at http://www.law.openn.edu./bll/ulc/fnact99/1905/uupa95.html.

Card Code of Conduct" or a "*Digital Coin Code of Conduct*" could be agreed upon before the inevitable and predictable problems occur.

As a simple example of one of the problems, consider the responsibilities for a lost smart card. In one view, it is the same lost currency and the cardholder should bear the loss of the stored value. On the other hand, it is easy to program a "lock" into the card so that it cannot be used without a key. Should issuer be required to issue cards that may be locked? Should the liabilities be different where there is a possibility of locking the card? These problems are entirely foreseeable and which could be settled before they arise. However, because of the distributed nature of the digital coin system the consumer protection problem is more difficult.

Now the question here arises who will bear the risk attached to electronic banking and how consumers can protect themselves?

Consumers can protect themselves against the risk of financial loss in using electronic money by safeguarding their cards or computers on which electronic money is stored and any access codes or PIN numbers, and by limiting the amount of funds they choose to hold in this form. At the same time, issuers of electronic money products have incentives to disclose relevant information about the functions and terms of use of electronic money products in order to help consumer to use the products and to prevent legal actions in the event that problem arises. In some multi-issuer electronic money schemes voluntary insurance or loss sharing arrangements are anticipated, such that if one institution becomes insolvent, the others would jointly honour electronic money claims issued by that institution.[95]

At a basic level, governments can further their policy objectives in the banking and payment sectors by ensuring that the relevant legal framework provides adequate incentives for fair, practical and a strong foundation for reasonable private agreements and contracts.

Liability for Damages for Transfer Failure Due to Technology.

For an electronic fund transfer, there is the possibility that technology will malfunction and the attempted transfer will be frustrated. This frustration will likely be inconsistent with the representation made about the product's performance and anticipated by the parties. Here the question arises, who is liable and what is the measure of damages?

A court would likely apportion damages based on the ownership of the technology, which causes the failure of the attempted transfer. Assume, for example, the transfer involves a user's personal computer, then the user would be responsible for whatever damages were sustained. If, on the other hand, the issuer's equipment malfunctions (e.g., A Card reader causes a stored obligation be erased rather than transferred, then the issuer should be liable.[96]

The above rules would probably not apply in "*force majeure situation*", i.e. if such interruption or failure was beyond the control

[95] The G-10 Deputies Report on Electronic Money – Consumer Protection, Law Enforcement, Supervisory and Cross Border Issues, Basle, April 1997. available at, http://www.bis.org/publ/gten.pdf.

[96]. There may be other possibilities. For example, there may be an execution failure because of the technology used by the certification authority and the certification authority is unable to verify the digital signature because its equipment is not able to function, the certification authority bear any loss due to execution failure. By the Task Force on Stored Value Cards, supra note 84, p. 706.

of the party relying on the interruption or failure to excuse performance.

Measures of Damages where Transferor or Transferee is Liable

Determining the measure of damages is perhaps even more important than determining who is liable. It is a general rule that the aggrieved party may be put in as good a position as if the other party had fully performed. The general rule is subject to a caveat that "neither consequential or special nor penal damages may be had except as specifically provided in the Act or by other rule of law.

If the issuer is liable for the failed transaction, the measure of damages for execution failure, either due to the failure of a storage device or to the software or hardware provided by the issuer, could be derived from the measure used where there is breach of an implied warranty of merchantability. The application of this measure will depend on whether the contract between the users and the issuer is deemed to be a sales contract. *Liability for the Spawning.*

As to the issue of the spawning whether the problem be one of innocent "spawning" or whether it is a problem where a malefactor has found a method of counterfeiting the issuer's obligation so that it is impossible to distinguish an authentically issued obligation from a counterfeit, the problem for the issuer is same. If a legitimate claim has become indistinguishable from an illegitimate claim, the obliger may have to pay both classes. This is the natural consequence of the issuer not being able to distinguish a legitimate claimant from an illegitimate claimant.[97]

[97] Task Force on Stored Value Cards, supra note 84 p. 710.

Fraudulent Obligations

There is always a possibility that someone will try to defraud a party by creating and transferring an obligation that was not issued by the issuer. Who should bear the loss for these fraudulent obligations?

The obligations stored on the new payment products are represented by electronic data, in some cases stored on specialized hardware. Verification of the obligation is accomplished by means of cryptography and other security measures included in the software and/or hardware used by the product. If the actual data representing an obligation is copied perfectly and the new payment products do not permit the users to identify a "counterfeit," then the issuer should bear the loss if there are fraudulent and undetectable obligations in circulation.[98]

Lost, Stole, Destroyed, and Disputed Transactions

Who will bear the risk for a lost or stolen stored obligation?[99] There are two possible commercial law analogies that could be used to resolve this issue for most of the payment products. The first analogy would be of promissory notes. If a Rs. 100 note is lost, stolen, or destroyed, the person who lost the note will not be able to obtain a replacement from the Reserve Bank. If check analogy is used, the user would be able to stop payment on the stored obligation provided the stop-payment order was received by the issuers in time to act on it.

Finally, it can be said that the design of the new payment products will dictate the way in which a court would view the product for stop payment purposes. A cash analogy will likely be used where the check analogy fails; namely, where the obligation are not

[98] Ibid. p. 716.

[99] This will be an extremely important issue if the amounts involved in the new products grow beyond the high volume, ibid, p. 718.

individually identifiable and/or it is not possible to provide advance warning to sellers or other transferees who take the obligation in good faith.[100]

CONTRACT TERMS AND ENFORCEABILITY

All of the participants in a smart card scheme have generally contractual relationship with at least one other member of the scheme. At the time obligation is created, the issuer of the obligation will likely want to bind the user of the obligation to a number of conditions limiting the manner in which the product can be used.[101] Product promoters intend to rely upon the common law of contract to achieve these limitations. Whether an issuer (either directly or through an agent) can bind or effectively impose these limits on a user depends on a number of factors:

It is important to recognize that one of the factors a court would surely consider when deciding whether to enforce a particular contract term is that these products are designed for sale to consumers and not sophisticated commercial counter parties. It would be a significant error of judgment to turn a blind eye to such a commercial reality.

Some of the new products will use traditional contracting techniques, requiring original signatures of the user on all contracts. If a dispute arises over a specific covenant, there will be a tangible contract to show a judge or jury. Some of the new products, however, may try to establish contractual obligations through unilateral electronic communications. Although the validity of these contracts could be called into question under a statute of frauds because there is

[100] Task Force on Stored Value Cards, supra note 84, p. 720.

[101] In fact, the exact nature of the stored obligation will likely be set out in these terms and conditions, Task force on Stored Value Cards, supra note 84, p. 683.

no "writing" evidencing the contract and no signatures. Under most statutes of frauds, these forms of undertakings, even in the absence of writing, should be enforceable. Where writing is required, the use of digital signatures could be explored. Digital signatures use public key encryption to verify the source of a document.[102] Whether a digital signature will be recognized in a court will likely depend on the law of the state where the obligation arose.

An alternative to the use of digital signature may be the use of cybernotaries to certify and authenticate computer-based transactions and records. Cybernotaries might be "particularly helpful in ascertaining when an agreement was made", particularly given that the time and date can be easily altered in computer messages.[103]

Until there is an established methodology for verifying computer contracts, it will be difficult to conclude with certainty that an electronic contract will be enforceable under the existing rules of evidence and contracts. If an issuer of a particular product is concerned that the rules regarding computer contracts as applicable to its product are not sufficiently certain, the issuer might consider eliminating the uncertainty with paper contracts.

A related question is whether the issuer may amend the agreement unilaterally. The right to amend is currently claimed by credit card issuers and by banks in deposit agreements[104]. As a general rule, however, contract law does not permit unilateral amendment of a bilateral agreement with respect to an obligation already incurred. This means unilateral amendments will usually be

[102] Public key encryption can be used to verify that the contents of a document have not been altered, ibid, p. 684.

[103] Task Force on Stored Value Cards, supra note 84. p. 685.

[104] Credit Card issuer have successfully amended contract terms unilaterally by notifying card holders that an out standing obligation which is not repaid by a specified date will be subject to unilateral amendment after that date, Task Force on Stored Value Cards, supra note 84, p.686.

given only prospective effect. Accordingly, for issuers to be able to enforce amendments, issuers must identify and communicate any changes in rights arising from an amendment. However, with the advent of Digital cash, relationships may no longer be directly controlled by an express contract. To illustrate, a merchant may confidently accept a credit card or a smart card because he or she knows that the contract that they have with the issuer will guarantee that they receive value for consideration. No appeal to general law is necessary. By contrast, a merchant who is offered digital coins in payment may have no prior contractual arrangement with the issuing bank. If the systems have to flourish, the merchant must be able to rely upon some general law, which governs the relationship of the parties. However, an issuer could make it a condition that merchants may only accept payment by prior arrangement. This would re-establish contractual restraints which are lacking in the general model. However, for the commercial reason, this is unlikely to be a stable long-term solution.

ALTERNATIVE DISPUTE RESLUTION (ADR)

Awareness of the potential legal and other barriers arising from resorting to courts in disputes resulting from cross-border online interactions is widely shared: which law applies, which authority has jurisdiction over the dispute, which forum is competent to hear the dispute, is the decision enforcement across borders?[105] Another legitimate concern, though less legal in nature, is related to the cost of court proceedings, or the length of the procedure. In contrast, a pragmatic approach aimed at providing individuals and businesses

[105] Anne Carblanc, "Privacy Protection and Redress in the Online Environment: Fostering Effective Alternative Dispute Resolution", *22nd International Conference On Privacy and Personal Data Protection*, (Venice, 28-30 September, 2000), available at http://www.oecd.org/dsti/sti/it/secur/fprod/venice_paper.pdf.

with easily accessible and potentially more efficient means to settle disputes that cannot otherwise easily be resolved may offer an interesting alternative. In particular, online Alternative Dispute Resolution (ADR) may help obviate the perplexing issue of a competent forum: the forum will no longer be tied to a geographic location but will be virtual.

ADR systems, used in both the online and offline worlds for B-to-C interactions and transactions internationally have proved to be successful and appropriate in various countries. ADR is used off-line to resolve many different types of disputes, from local disputes between neighbours to international commercial transactions. ADR mechanisms are also being developed in the online environment to resolve a wide range of disputes (e.g. domain names, insurance, privacy, family, commercial transactions) between parties (B-to-B, C-to-B, C-to-C) involved in electronic interactions.

Most stakeholders agree that the on-line alternative dispute resolution (ADR) can be very helpful to both parties in electronic interactions or transactions, especially in cross-border complaints. They see incentives for fostering ADR, whether economic (e.g. reducing costs), legal (e.g. avoiding the difficulty to establish jurisdiction), or more sociological (e.g. improving confidence, and bridging cultural differences). Potential negative impacts have also been highlighted such as lack of consumer choice, disparity between the parties or possible lack of enforcement of decisions. While it is easy to imagine how ADR will work, in the general sense, to resolve disputes related to consumer protection like failure to deliver a good or delivery of a non-confirming good, it is more difficult to grasp how

ADR will work for disputes related to protection of personal data, as privacy is more intangible.[106]

VII) RISKS AND ELECTRONIC PAYMENT SYSTEM

The development and use of electronic money and some forms of electronic banking are still in their early stages. It has been recognized that along with the benefits, electronic banking and electronic money activities carry risks for banking organizations. However, because of rapid changes in information technology, no list of risks can be exhaustive. At this stage, it would appear that operational risk, reputational risk and legal risk may be the most important risk categories of electronic banking and electronic money activities, especially for diversified international banks.

Operational Risk

Operational risk arises from the potential for loss due to significant deficiencies in system reliability or integrity.[107] Operational risk can also arise from customer issues, and from inadequately designed or implemented electronic banking and electronic money systems. Other kinds of operational risk are, volume forecast, management information systems and outsourcing.

i) System Design, Implementation and Maintenance

A bank faces the risk if the system it chooses are not well designed or implemented. Many banks are likely to rely on outside service providers and external experts to implement, operate and support portions of their electronic money and electronic banking activities. However, reliance on outsourcing exposes a bank to operational risks.

[106] Ibid.

[107] Risk Management for Electronic Banking and Electronic Money Activities, Basle committee on Banking Supervision, Basle BS/97/122, March 1998, available at http://www.bis.org/publ/bcbc35.pdf.

Service providers may not have the requisite expertise to deliver services expected by the bank, or may fail to update their technology in a timely manner.

ii) Customer Misuse of Products and Service

As with traditional banking services, customer misuse, both intentional and inadvertent, is another resource of operational risk. Risk may be heightened where a bank does not adequately educate its customers about security precautions. In addition, in the absence of adequate measures to verify transactions, customers may be able to repudiate transactions they previously authorized, inflicting financial losses on the bank.

Reputational Risk

Reputational risk is the risk of significant negative public opinion that results in a critical loss of funding or customers. Increased reputational risk can be a direct corollary of heightened risk exposure or problem, in other risk categories, particularly operational risk.

Mistakes, malfeasance, and fraud by third parties may also expose a bank to reputational risk. Reputational risk can arise from significant problems with communication networks that impair customer's access to their funds or account information, particularly if there are no alternative means of account access. The situation is aggravated because the speed of the Internet considerably cuts the optimal response times for both banks and regulators to any incident. Banks must ensure their crisis management processes are able to cope with Internet related incidents (whether they be real or hoaxes).[108]

[108] Carol Sergeant, *E-Banking: Risks and Responses*, 29th March 2000, p. 8, available at www.fsa.gov.uk/pubs/speeches/sp46.htm.

Legal Risk

Given the relatively new nature of many retail electronic banking and electronic money activities, rights and obligations of parties to such transactions are, in some cases, uncertain. Banks engaging in electronic banking and electronic money activities can face legal risks with respect to customer disclosures and privacy protection. Customers who have not been adequately informed about their rights and obligations may bring suit against a bank. Failure to provide adequate privacy protection may also subject a bank to regulatory sanctions in some countries.

As electronic commerce expands, banks may seek to play a role in electronic authentication systems such as those using digital certificates.[109] The role of a certification authority may expose a bank to legal risk. For example, a bank acting as a certification authority may be liable for financial losses incurred by parties relying on the certificate.

Other Risks

Traditional banking risks such as credit risk, liquidity risk, interest rate risk and market risk may also arise from electronic banking and electronic money activities, though their practical consequences may be of a different magnitude for banks and supervisors than operational, reputational, and legal risks.

Cross Border Issues

Electronic banking and electronic money activities are based on technology that by its very nature is designed to extend the

[109] A digital certificate issued by a certification authority is intended to ensure that a given digital signature is in fact generated by a given signer. A bank that undertakes to act as a certification authority could be considered to be providing services to clients similar to those associated with providing an accounts access device or acting as a notary public, ibid, p. 8.

geographic reach of banks and customers. Banks may face different legal and regulatory requirements when they deal with customers across national borders. For new forms of retail electronic banking, such as Internet banking and for electronic money, there may be uncertainties about legal requirements in some countries. In addition, there may be jurisdictional ambiguities with respect to the responsibilities of different national authorities. Such considerations may expose banks to legal risk associated with non-compliance with different national laws and regulations, including consumer protection laws, record-keeping and reporting requirements, privacy rules and money laundering laws.[110]

Risk Management

A risk management process that includes the three basic elements of assessing risks, controlling risk exposure, and monitoring risks will help banks and supervisors attain these goals. Banks may employ such a process when committing to new electronic banking and electronic money activities, and as they evaluate existing commitment to these activities. Apart from this operational risk associated with e-cash can be mitigated by imposing constraints,[111] such as limits on (i) the time over which a given electronic money is valid, (ii) how much can be stored on and transferred by electronic money, (iii) the number of exchanges that can take place before a money needs to be re-deposited with a bank or financial institution, and (iv) the number of such transactions that can be made during a given period of time.

[110] The G-10, Deputies Report on Electronic Money – Consumer Protection, Law Enforcement, Superiority and Cross Border Issues, Basle, April 1997, available at http://www.bis.org/publ/ gten01.pdf.

[111] Ravi K Kalakota and Andrew B Winston, *Frontiers of Electronic Commerce*, (Massachusetts, 2000), p.308.

In this chapter we have discussed the issues raised by electronic banking and electronic money. In the next chapter we will discuss how some countries have dealt with these issues or how some countries are planning to tackle these issues, what are the responses form international organizations because electronic banking and electronic money raise a whole lot of cross border issues, the responses from industry in solving these issues and the Indian position regarding e-banking at present.

Chapter - IV

Electronic Banking: International and National Responses

CHAPTER IV

ELECTRONIC BANKING: INTERNATIONAL AND NATIONAL RESPONSES

In this chapter we are going to emphasize on the work done by international organizations, to embark upon the issues, which have arisen with the advent of electronic banking and electronic money. We will also discuss the various legislations enacted specifically in the U.S.A and the U.K., and finally the Indian response towards these issues.

INTERNATIONAL RESPONSES

UNITED NATIONS COMMISSION ON INTERNATIONAL TRADE LAWS (UNCITRAL)

UNCITRAL has come up with *Model Laws on International Credit Transfers*[1], *UNCITRAL Model Law on Electronic Commerce, with Guide to Enactment 1996, with additional Article 5 bis, as adopted in 1998*[2], *draft Model Law on legal Aspects of Electronic Data Interchange and Related Means of Communication*[3], *together with draft Guide to Enactment*[4], *draft Guide to the enactment of the UNCITRAL Model Law on Electronic Signature*[5], *and UNCITRAL Legal Guide on Electronic Funds Transfers 1986*[6]. This Legal Guide is very important in understanding international funds transfers.

[1] Sales No. E. 99. V.11, United Nations, 1992.

[2] General Assembly Resoultion 51/ 162 of 16th December, 1996, UNCITRAL Model Law on Electronic Commerce.

[3] Annex II to Document A/ 50/ 17, United Nations, 1996.

[4] A/ CN. 9/ 426, United Nations, 1996.

[5] A/ CN.9/ WG. IV/ WP.88, United Nations, New York, 2001.

[6] A/ CN.9/ SER. B/ 1, Sales No. E. 87. V.9, United Nations, 1986.

It explored altogether forty-one issues that would have to be faced, in moving from a paper based to an electronic funds transfers system. Since the focus of the Legal Guide was on the impact of the shift from paper to electronics, it discussed both credit and debit transfers.

The first issue was whether major changes in the law were required by the development of electronic funds transfers? The Legal Guide notes that since electronic funds transfers are not carried out in a manner identical to paper-based funds transfers, changes in the law to adjust to the new procedures should be expected. The new technology requires an adjustment of the law in regard to such matters as the periods of time within which various actions are to be taken, the presence or absence of liability arising out of computer failure at one of the banks, clearing-houses or communication networks, a time when a funds transfers becomes final and the consequences of the finality. Modifications of this nature to existing legal rules do not affect their structure, but they may modify their content to an important degree[7].

Due to the continual change in technology, it may lead to new subdivisions in the law. Therefore, it found it useful to distinguish between batch-processed funds transfers and individual funds transfers sent by tele-communications, between transactions using debit cards and those using credit cards, between those initiated on customer-activated terminals and those the electronic communication initiated at a bank. To some extent these distinctions may be satisfactorily expressed in bank-customer contracts and in inter-bank rules governing different types of funds transfers networks. However, in some cases these distinctions may need to be expressed in the statutory law governing funds transfers. If the number of special rules, which are the result of these distinctions, is small, these can be handled within the general law of funds transfers. If the number of special rules is

[7] Issue 1, para 4, A/ CN.9/ 266/ Add.2, United Nations, 1985. As it is, not possible to discuss all the issues here, we will be discussing only some important issues.

too large, it may be preferable for special laws to be adopted, as there currently are for debit transfers and credit transfers.

Some questions arising in the context of electronic funds transfers are common to all forms of automatic data processing and the legal rules may also be common to all such transactions. Prominent among these questions is the evidential value of the computer records of funds transfer instructions sent and received in computer readable form and of account records stored in that manner. Of particular concern is the acceptability of the authentication used in the electronic funds transfers.

A second issue, which is raised is, should internationally agreed rules be proposed to govern international electronic funds transfers?[8] International funds transfer starts once the transferor instructs his bank to transfer funds to the transferee at a bank in foreign country[9]. Here the main problem for discussion was that of difference in laws, as some part of the, of funds transfer is carried out in a foreign country in conformity with the local banking laws and practice. Here *UNCITRAL Group on International Payment* took the help of Draft Convention on International Bills of Exchange and International Promissory notes[10]. The basic approach followed in the draft has been that the draft convention should govern the funds transfer instruction issued by the transferor and all of the funds transfer transactions necessary to implement that instruction. However, draft convention specifies that certain legal problems concerning the bill are not governed by it.

A third issue is whether the rules of evidence give records of funds transfers kept in computer-readable form the same legal value as records kept in paper-based form?[11] According to the results of a survey conducted by the secretariat of the UNCITRAL, it appears that in most countries records kept in computers can be used as evidence in case of litigation. In common law countries,

[8] Issue 5, note 7.

[9] Ibid, para 1.

[10] A/ CN.9/ 211, United Nations, 1988.

[11] Issue 7, Note 7, Also see, *Legal Value of Computer Records: Report of the Secretary General* (A/ CN.9/ 265).

it is the usual rule that computer records can be admitted as evidence only if the proponent of the records establishes certain facts about the record and the computer system.

In several countries with an exhaustive list of types of admissible evidence, computer records are admissible in commercial disputes but may not be admissible in non-commercial disputes. Since the latter category may include most transactions made through automated cash dispensers, automated teller machines and point-of sales terminals, the potential problems for electronic funds transfers may be significant in those countries. In particular, when a non-commercial customer denies having used a customer-activated terminal, it may be difficult or impossible for a bank to prove that he did so on the basis of computer record of the transaction alone[12]. Here it has been argued that in that case surrounding circumstances should be taken into account. However, when the surrounding circumstances neither substantiate nor raise serious doubts about customer's claim, then a question comes up, who should bear the burden of proof? At present provisions found in many bank-customer contracts cite that the customer is responsible for all transactions initiated by the use of his debit or access device, unless he has reported that the device was lost or that the means of access were compromised in some other way[13].

A fourth issue is, should banks have written contracts with their customer's covering rights and duties of the customer's and the banks, in respect of electronic funds transfers?[14] In respect of new funds transfers techniques, and especially electronic funds transfers, banking tradition and practice in countries where written contracts are not common, may not be able to provide the necessary content for many of the questions that may arise. It was commented that it appears that banks always require written agreements before they issue credit cards or

[12] Issue 21, Ibid, Should the bank or the bank's customer carry the burden of proof whether a debit to the transferor's account was aut6horized by him or occurred through fault?

[13] Issue 21, Ibid.

[14] Issue 10, note 7.

debit cards. Written contracts seem not to be always required before customers are allowed to participate in cash management programmes and other large-value funds transfers, although they may be particularly useful in this regard since some aspects of the bank-customer arrangement may differ from customer to customer.

A fifth issue is, should there be legal requirements as to the form of authentication necessary in an electronic funds transfer?[15] Here it was thought desirable to require by law that electronic funds transfer instructions must be authenticated, it may also be thought desirable to indicate the type of authentication, which would be legally acceptable. But here one problem was felt, that in contrast to authentication of a paper-based document, where a reasonable exhaustive list of means of authentication, including signatures, could be given if desired, there are innumerable ways to authenticate a message sent by telecommunications. With the rapid development of technology, some current methods of authentication can be expected to become weaker while new and more secure forms of authentication can be expected.

A sixth issue discussed is, where should customer accounts be considered, to be located for the purpose of the legal rules governing funds transfers?[16] Here it was said that when a bank has a centralized data processing center to which funds transfers instructions must be brought for processing, it may be thought that the basis for the 'old rule'[17] is eroded and that, at least for some purposes, the centralized data processing center might be considered to be the location of the customer accounts.

A seventh issue is, should public telecommunications carriers, private data communication services, electronic funds transfers networks and electronic clearing-houses be responsible for losses arising out of errors or fraud in

[15] Issue 12, note 7.

[16] Issue 15, note 7.

[17] So long as computer accounts records, were maintained exclusively on paper, the usual rule was that the customer account was considered to be located for legal purposes of the place where it was maintained for book-keeping purposes. When a bank had multiple branches, customer accounts were usually maintained at each branch, and therefore were located at the branch for legal purposes.

connection with a funds transfer instruction?[18] Here one important point was made that the contractual allocation of loss between these entities and the participating banks should be the best way to sort out the problem[19]. It was also thought that the telecommunications carriers, data communication services, electronic funds transfers networks and electronic clearing-houses, should be liable for the loss caused by the fraud of its employees. But here it argued that a distinction might be drawn between losses from fraud made possible as part of the employment relationship, for which the employer would be responsible, and losses from fraud made possible by knowledge acquired by the employee in the course of his employment, for which the employer would be responsible.

A eighth issue is, should a bank be free from responsibility for errors or delayed funds transfers caused by failures in computer hardware or software?[20] Here it was argued that a generalized exoneration from liability may not be justified, but in a situation when a bank could not be expected to have prevented the failure of reduced its consequences in that situation exemption from liability for computer failure may be justified.

A ninth issue is, should a bank be liable to its customer for having entered a debit or credit to the account according to the account number indicated on the funds transfer instruction it has received if the name on that account does not correspond to the name given on the funds transfer instruction?[21] Here with other possibilities it was argued vociferously that in an automated data processing a bank that entered a debit or credit according to the account number on a funds transfer instruction it received would not be liable even though the entry was made to an account bearing a different name from that on the instruction. Any loss would be borne by the transferor or the bank at which the incorrect account number was first entered on a funds transfer instruction. This might be expressed

[18] Issue 18, note 7.

[19] Ibid, para 2.

[20] Issue 19, note 7.

[21] Issue 20, note 7.

as a rule that in case of conflict between the account number and the account name, the account number prevailed.

A tenth issue is, under what circumstances should the bank be liable for consequential damages?[22] Although delay or error in the processing of the funds transfer instruction can usually be fully compensated by payment of interest, or exchange loss and the making of the similar financial adjustments, in a few cases the failure to complete the funds transfer by the anticipated date may cause consequential damages to the transferor arising out of cancellation of a contract, incurring of a penalty of forfeiture of rights with damages far exceeding compensation measured as interest. For these types of cases it was suggested in the discussion that there should be a standard procedure available whereby a transferor could notify the transferor bank that it was of particular importance that the funds transfer be completed on time. An additional fee might be charged based on a special priority procedure required for handling the funds transfer.

From the above discussion it is clear that the *Draft Legal Guide on Electronic Funds Transfers* is very useful in understanding Electronic Funds Transfer and issues attached to it in general and international funds transfer in particular.

UNCITRAL Model Law on International Credit Transfers

When *UNCITRAL* authorized the publication of the *Legal Guide in 1986*, it also decided to prepare model legal rules so as to influence the development of national practices and laws governing the newly developing means of funds transfers. As indicated by its title, and in contrast to *Legal Guide, the Model Law* applies to credit transfers only, and not to debit transfers[23]. The other point that may be noted is that *Model Law* is not restricted to credit transfers made by computer-to-

[22] Issue 29, note 7.

[23] In telex transfers and computer-to-computer transfers it is the originator of the funds transfer who begins the banking procedures by issuing a payment order to its bank to debit its account and to credit the account of the beneficiary. A funds transfer in which the originator of funds transfer initiates the banking procedures is often called a credit transfer, and that it is the term used in the Model Law, UNCITRAL On International Credit Transfers: Note by the secretariat, A/ CBN.9/ 384.

computer or other electronic techniques, even though it was the explosive growth of electronic credit transfer systems that brought about the need for *Model Law.*

Article 2 (a) of the Model Law defines Credit transfer i.e. 'Credit transfer' means the series of operations, beginning with the originators payment order, made for the purpose of placing funds at the disposal of beneficiary...'

From this it is clear that money credit transfers require the services of one or more intermediary banks.

The other thing, *Model Law* is restricted to is international credit transfers. In part this decision was taken in recognition of the fact that *UNCITRAL* was created to unify the law governing international trade[24]. And whether credit transfers is international or not, it depends on whether any sending bank or any receiving bank in the credit transfer, are in different Sates or not. However, a criterion has been set out in *Article 1 of Model Law*[25].

As to the extent to which *Model Law* is mandatory *Article 4*, provides that 'except as otherwise provided in this law, the rights and obligations of parties to a credit transfer may be varied by their agreement'. From this it is clear that the *Model Law* is not mandatory law. The parties to a credit transfer may vary their rights, obligations by agreement and the agreement must be between parties whose rights, and obligations are affected. However, certain rights and obligations of the parties may not be varied by agreement, or may be varied only to a limited extent or under limited circumstances[26].

As to the question of fraud, it has been dealt in *Articles 5 (1), 5 (3), and 5 (4)*, where the liability of different parties has been fixed according to the circumstances.

As to the banks liability for failure to perform one of its obligations, it has been mentioned that the originator's bank must refund to the originator the amount

[24] Ibid.

[25] This law applies to credit transfers where any sending bank or its receiving bank are in different States, Article 1 (1), Note 1.

[26] See Article 5 (3), Article 14 (2) and Article 17 (7) of the Model Law, Note 1.

of the transfer plus interest if the credit transfer is not completed[27]. However, according to Article 18, one exception is when the failure to execute the payment order, or to execute it properly, occurred '(a) with the specific intent to cause loss, or (b) recklessly and with actual knowledge that loss would be likely to result'. In those unusual circumstances of egregious behavior on the part of the bank, recovery may be based on whatever doctrines of law may be available in the legal system outside the *Model Law.*

UNCITRAL Model Law on E-Commerce.

For the purpose of discussion *Articles 5, 7, 9 and 11* are important[28]. *Article 5,* talks about the legal effects, validity or enforceability of data messages. *Article 7 of the UNCITRAL Model Law on Electronic Commerce,* is based on the recognition of the functions of a signature in a paper-based environment. It focuses on the two basic functions of a signature, namely to identify the author of a document and to conform that the author approved the context of that document. *Article 7,* does not introduce a distinction between the situation in which users of electronic commerce are linked by a communication agreement and the situation in which parties had no prior contractual relationship regarding the use of electronic commerce.

Thus *Article 7,* may be regarded as establishing a basic standard of authentication for data messages that might be exchanged in the absence of a prior contractual relationship and, at the same time, to provide guidance as to what might constitute an appropriate substitute for a signature if the parties used electronic communications in the context of communication agreement.

Another thing under *Article 7,* is that it requires a reliable method, which is able to identify the person as also indicating his approval of the information contained. Not only should it be reliable but it should also be appropriate for the

[27] See Article 17 of the Model Law, Ibid.

[28] See UNCITRAL Model Law on Electronic Commerce, note 2.

purpose. However, *Working Group on Electronic Commerce* has left the method open for the parties to decide on a case-to-case basis[29].

Article 9 of the Model Law, deals with the admissibility and evidentiary weight of the data messages in *Article 9*. The Article mandates that in any legal proceeding, the rules of evidence should not apply to exclude a data message, either, solely because it is a data message[30] or, if it is the best evidence that the person adducing it could reasonably be expected to obtain, on grounds that it is not in its original form[31]. *Article 11 of the Model Law*, deals with the formation and validity of contract, using a data message.

Draft Guide to Enactment of the UNCITRAL Model Law on Electronic Signature.

The increased use of electronic authentication techniques as substitutes for hand-written signatures and other traditional authentication procedures has suggested a need for a specific legal framework to reduce uncertainty as to the legal effect that may result from the use of such modern techniques, which may be referred to generally as 'electronic signature'[32]. Since the use of the electronic signature was an International phenomenon, it was thought desirable that there should be a uniform rule on an International plane.

The objective of the *Model Law* is to enable or facilitate the use of electronic signature and to provide equal treatment to both users of paper-based documentation and users of computer based information. It has dealt with the legal basis, supporting certification process, including emerging digital authentication and certification technology, the applicability of the certification process, the

[29] See Kenneth A. Freeling and Ronald E. Wiggins, *States Develop Rules for Using Digital Signatures*, available at http://www.lix.com/ internet/ 1020esig.html.

[30] Article 9 (1) (a), note 2.

[31] Article 9 (1) (b)

[32] See Planning of Future Work on Electronic Commerce: Digital Signatures, Certification Authorities and Related Issues, A/ CN.9/ WG IV/ WP. 71 31.

allocation of risk and liabilities of users[33], providers[34] and third parties in the context of certification techniques, the specific issues of certification through the use of registries and incorporation by reference[35], recognition of foreign certification and electronic signatures.[36]

To that effect *UNCITRAL* has intended to develop uniform legislation that can facilitate the use of both digital signatures and other forms of electronic signatures. *UNCITRAL* has attempted to deal with the legal issues of electronic signature, issues at a level that is intermediate between the high generality of the *UNCITRAL Model Law on Electronic Commerce* and the specificity that might be required when dealing with a given signature technique. In any event, consistent with media neutrality in the *UNCITRAL Model Law on Electronic Commerce,* the new *Model Law* is not to be interpreted as discouraging the use of any method of electronic signature, whether already existing or to be implemented in the future.[37]

The Model Law applies to all kinds of data messages to which a legally significant electronic signature is attached, and nothing in the *Model Law* should prevent an enacting State from extending the scope of the *Model Law* to cover uses of electronic signatures outside the commercial sphere. For example, while the focus of the *Model Law* is not on the relationships between users of electronic signatures and public authorities, the *Model Law* is not intended to be inapplicable to such relationships. Footnote to *Article 1* provides for alternative wordings, for possible use by enacting States that would consider it appropriate to extend the scope of the *Model Law* beyond the commercial sphere.

However, *Model Law* does not deal with certain issues related to *Public Key Infrastructure (PKI)*, such as, (i) the extent to which the use of cryptography should be authorized for confidentiality purposes, (ii) whether Government

[33] Article 8, Draft Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures, A/ CN.9/ WG IV/ WP. 88, 2001.

[34] Article 9, Ibid.

[35] Official Records of the General Assembly, Fifty-First Session, Supplement No. 17 (A/ 51/ 17), Paras, 223-224.

[36] Article 12, note 33.

[37] Article 3, Ibid.

authorities should retain access to encrypted information through a mechanism of key escrow or otherwise, and (iii) whether the certification authorities certifying the validity of cryptographic key pairs should be public entities or private entities.[38] However, one more thing to be pointed out that review of each article of the Draft *Model Law* reveals an astonishing similarity to the *American Bar Association's (ABA's) Digital Signature Guidelines.*[39]

UNCITRAL Model Law on Legal Aspects of Electronic Data Interchange and Related Means of Communication, together with a draft *Guide to Enactment.*
The *Model Law*[40] applies to any kind of information in the form of data message used in the context of commercial activities, whether contractual or not.[41]

Three articles in the *Model Law* deal with the problem of statutory requirements for writing, signature and originals. First, *the Model Law*, suggests that where a rule of law requires information to be in writing, or presented in writing, or provides for certain consequences if it is not, a data message satisfies that rule if the information contained therein is accessible so as to be usable for subsequent reference[42], secondly the requirement for a signature will be satisfied in relation to a data message if a reliable method is used to identify the originator and to indicate the originator's approval of the information in the message[43],thirdly, a data message will satisfy a rule that information be presented or retained in its original form if a method of authentication based on the following elements is established: (a) a simple criterion as to integrity of data,

(b) a description of the elements to be taken into account in accessing the

[38] Draft Guide to the Enactment of UNCITRAL Model Law on Electronic Signature, note 5, para 52.

[39] W. Everett Lupton, Comment, *The digital Signature: Your Identity by the Numbers*, available at, http://www.richmond.edu/ jolt/ V 6i2/ note 2. html.

[40] UNCITRAL Draft Model Law on Legal Aspects of Electronic Data Interchange and Related Means of Communication, (Annex II to Document A/ 50/ 17), together with a Draft Guide to Enactment (A/ CN.9/ 426), 1996.

[41] Article 1, Ibid.

[42] Ibid, Part Two General Principles No. IV.

[43] Article 5, Ibid.

integrity; and, (c) an element of flexibility (i.e. reference to circumstances).[44] *The Model Law* establishes the admissibility of the data messages as evidence in legal proceedings, and their evidential value according to the reliability of the manner in which the data message was generated, stored or communicated; the reliability of the manner in which the integrity of the information was maintained; and the manner in which the originator was identified, together with any other relevant factor[45].

However, it has also dealt with the attribution of data messages and the problem of an unauthorized person sending a message[46].

ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD)

Now we are going to deal with the work done by *OCED,* with regard to electronic banking and electronic money and the issues that arise from these thereupon.

OCED Guidelines for Consumer Protection in the context of electronic commerce, 1998[47].

Because of the nature of electronic commerce, OECD member countries have recognized that internationally co-ordinated approaches may be needed to exchange information and establish a general understanding about how to address those issues. In particular, the purpose of the guidelines is to provide both a framework and a set of principles to assist. In this regard, for our purposes guidelines number five (V) is important, where it has been stated that[48]:

> A consumer should be provided with easy-to-use, secure payment mechanisms and information on the level of security, such mechanisms afford.

[44] Article 7, Ibid.

[45] Article 8, Ibid.

[46] Article 11, Ibid.

[47] OCED Guidelines for Consumer Protection in the context of Electronic Commerce, 1998, available at http://www.oecd.org/ news-and-events/release/ guidelines consumer.pdf.

[48] Ibid, Part Two General Principles No. V.

Further it has been stated that consumer should be provided meaningful access to fair and timely alternative dispute resolution and redress without undue cost or burden[49].

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 1980. [50]

However, not going into detail, the core of the Guidelines consist, of the principles set out in *Part Two of the Annexture.* It is recommended to member countries with a view to[51]:

i. achieving acceptance by Member countries of certain minimum standards of protection of privacy and individual liberties with regard to personal data;

ii. reducing differences between relevant domestic rules and practices of Member countries to a minimum;

iii. ensuring that in protecting personal data they take into consideration the interests of other Member countries and the need to avoid undue interference with flows of personal data between Member countries; and

iv. eliminating, as far as possible, reasons, which might induce Member countries to restrict transborder flows of personal data because of the possible risks, associated with such flows.

As stated in the Preamble, two essential basic values are involved: the protection of privacy and individual liberties and the advancement of free flows of personal data. The Guidelines attempt to balance the two values against each other

However, *OECD Guidelines* are not legally binding.

[49] Ibid, General Principles- VI-B.
[50] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal and Data, 1980, available at, http://www. Oecd.org/ dsti/ sti/ it/ ec/ act/ paris-ec/ Pdf/ progress-e. pdf
[51]Ibid.

OECD Inventory of Approaches to Authentication and Certification in a Global Net worked Society 1998[52].

Authentication is used in the electronic environment to establish identify or privileges or as part of payment mechanisms, for instance through the use of a password or smart card or by using a cryptographic, shared secret or biometric technique. Certification mechanisms can provide assurances about information in the electronic environment to reduce uncertainty in electronic transactions between parties or systems.

This Inventory of approaches to Authentication and Certification in a Global Networked Society surveys activities in *OECD* countries related to authentication and certification on global networks, including laws, policies and initiatives in the public and private sectors, and at the national, regional and international levels. Specifically the report looks at[53]:

- the range of authentications and certification and related services;
- legal and policy issues under consideration;
- public sector approaches and sector initiative; and
- international aspects

Further it has made survey to national approaches also.

OECD Inventory of Controls on Cryptography Technologies also[54].

This Inventory intends to facilitate international co-operation by surveying international and national instruments relating to controls on the export, import and domestic use of cryptography technologies in OECD Member countries. Specifically, the report addresses:

- to what extent do countries have domestic controls on encryption and what amendments to domestic laws if any, are contemplated; and

[52] OECD, Inventory of approaches to Authentication and certification in a Global Networked Society, DSTI/ICCP/REG (98) 3 REV3, September 1998.

[53] Ibid.

[54] OECD, Inventory of Controls on Cryptography Technologies, DSTI/ICCP/REG (98)4/Final, Jan.1999.

- to what extent do countries have import or export controls on encryption, and what amendments to such import or export laws, if any are contemplated.

The main international instrument dealing with export controls on cryptography technologies is the *Wassenaar Arrangement on Export Controls for Conventional Arms and Dual use goods and Technologies (July 1996)* [55]

OECD Guidelines for Cryptography Policy 1997[56]

It has been provided in it that users should have a right to choose any cryptographic methods, subject to applicable law[57]. It has been further stated that fundamental rights of individuals to privacy, including secrecy of communications and protection of personal data, should be respected in national cryptography policies[58]. National cryptography policies may allow lawful access to plaint text, or cryptographic key, of encrypted data[59] and governments should remove, or avoid creating in the name of cryptography policy unjustified obstacles to trade[60].

Lastly, while the *OECD Cryptography Guidelines* identify the various interests, which must be balanced in the context of *International Cryptography Policy*, they do not resolve the fundamental question of how governments can give the benefits of cryptography to legitimate users, without empowering criminals to use it for illegal purposes.

[55] For further details see Wassenarr Arrangement, at http://www.Wassenaar.org. / The *Wassenaar Arrangement* is a collaboration of countries that defines a set of preliminary guidelines, covering both armaments and sensitive dual use goods and technologies, which need to be fully implemented at the national level. Participants agree to control through their national laws, regulations and policies those items and technologies contained in a list of Dual-Use Goods and Technologies - that includes cryptographic goods and technologies - and a separate Munitions List.

[56] OECD, Guidelines for Cryptography policy.

[57] Ibid, Principle.2

[58] Ibid, Principle.5

[59] Ibid, Principle.6

[60] Ibid, Principle.8

Guidelines for the Security of Information Systems 1992[61].

Security of information systems is an international matter and the issues to which they give rise may most effectively be resolved by international consultation and co-operation.

The guidelines identify nine principles in connection with security of information systems. They are the *Accountability Principle, the Awareness Principle, the Ethics Principle, the Multidisciplinary Principle, the Proportionality Principle, the Integration Principle, the Timeliness Principle, the Reassessment Principle and the Democracy Principle*[62].

However the objective is the protection of interests of those relying on information system from harm resulting from failures of availability, confidentiality, and integrity. It has been stated in the guidelines that security is required at all phases of the information cycle gathering, creating, processing, storing transmitting and deleting[63].

OECD has also worked in the field of taxation where its report[64] recognized that although the new payment system has posed new challenges to tax authorities. Now establishing identity of parties to a business transaction will be difficult to determine, whereas establishing location will be very easier. Again obtaining acceptable documentation of proof will become more difficult and tax havens and off- shore banking facilities will become more accessible. However, it also recognized that Intranet type networks might open up new possibilities for tax authorities to exchange information in a more timely and secure way. Already the *OECD* has developed an *OECD* standard Management Format for automatic

[61] OECD Guidelines for the security of information systems, C (92) 188/ Final, November 1992.

[62] Ibid

[63] Ibid, Principle. 6

[64] *Electronic Commerce: The Challenges to Tax Authorities and Taxpayers*, 1997 available at http://www.oecd.org/dof/fa/e-com/turku_e.pdf.

exchange of information and work is advancing on developing *EDIFACT Standard for Electronic Exchange of Tax Information*[65].

Further *OECD report on Bank Secrecy* says there should be international access to bank accounts for tax investigation on administrative application[66].

FINANCIAL ACTION TASK FORCE (FATF)

Now we will examine the work of *Financial Action Task Force on Money Laundering.* Money laundering is now recognized as a global problem by most governments, which has led to establishment of the *FATF*, the *OECD* sponsored body that oversees international anti-money laundering standards in regulation and law enforcement. To combat Money laundering, it came up with *Forty Recommendations*[67], where it examines the role of National Legal Systems, role of the financial systems, role of regulatory and other administrative authorities to combat money laundering, and further it examined role of international co-operation and accordingly it made the recommendations.

The FATF has for long time worked with the *Society for World Wide Inter Bank Financial Telecommunication (SWIFT)* on measures which would help to prevent wire transfers being misused by money launderers[68]. It is also continuously analyzing the question of co-operation between anti-money laundering authorities and tax administrations.

EUROPEAN UNION AND EUROPEAN COMMISSION

In 1998 *EC* came up with draft *EC Directive on a Common Framework for Electronic Signature*[69]. The *EC* Directive sets out the general principles under which *EU* member States should institute accreditation schemes, but leaves the implementation to national law. This means it does not by itself provide

[65] Ibid

[66] Niger Morris, Cotterill, "Secrecy Laws Under Assault", *The Banker*, Volume 150, No-894, August 2000.

[67] The Forty Recommendations, Financial Action Task Force on Money Laundering, available at http:// www. oced.org/ fatf,

[68] Annex C, Record and Conclusions of the Third FATF Forum with Representatives of the Financial Services Industry. Financial Action Task Force on Money Laundering, Annual Report 1999-2000, available at http://www. oced.org/fatf.

[69] OJ 98/ C325/ 04 (23)/ 10/ 98)

harmonization since it does not apply to" non contractual formalities requiring signatures". However it establishes a legal framework for certain certification services made available to the public. One interesting aspect it provides for out of court dispute settlement also[70].

Due to space constraint now we will examine *European Regulatory Framework* as a whole. A key measure for preventing the member states from adopting a fragmented approach in the field of regulation of information society is the *June 1998, Transparency Directive*[71]. This text imposes Member states to notify the commission and other member states of any draft rules and regulation activity they undertake in the field of information society services.

Other key legislative Acts are the *Directive on the Protection of Consumer with respect to Distant Contracts*[72] *(Distance contracts Directive). Article 12 of the Directive* states that the consumers cannot waive the rights granted to them by the national laws transposing the Directive. But above all, contractual choice of the law of a non-EU country cannot have the consequence of depriving consumers of the protection granted by the Directive, if the contract has a close connection with the territory of at least one member state.

The Directive on the legal protection of databases[73]. *The Database Directive* imposes its application[74] when the processing of personal data is carried out in the context of activities of an establishment of the controller on the territory of one member state, or when the controller, not established within the community, makes use- for the purpose of processing personal data - of equipment, automated or otherwise, situated on the territory of one Member State,

[70] Ibid, Article, 17.

[71] European Council and Parliamentary Directive 98/34/EC, June 1998, OJ L204, 1998, as amended by the Directive 98/48/EC, July 1998, OJ L217, 1998, available at http://europa.eu.int/eur_lex/en/lif/dat/1998en_398 L0048.html.

[72] European Parliament and Council Directive 97/7/EC, May, 1997, OJL 144, 1997, available at http://europa.eu.int/comm/dg24/policy/ developments/dist_sell/dist01_en.html.

[73] Council and European Parliament Directive 96/9/EC, March 1996, OJL77, 1996, available at http://www2. echo.lu/legal/en/ipr/database/database html.

[74] More exactly, the application of the national law of member states having transposed it.

unless such equipment is used only for purposes of transit through the territory of the community.

The European Union has also set up a coherent regulatory framework for protecting personal data, and ensuring at the same time the free circulation of this data within the internal market[75].

'Personal data' are very broadly defined by the data protection directive as 'any information relating to an identified or identifiable person[76]'. To determine whether a person is identifiable , account shall be taken of all the means reasonably likely to be used by the controller or by any other person to identify the person. No restrictions are to be placed on data flows across borders within the EC but trans-border flows to third countries may only take place if those countries provide adequate protection for personal data[77].

Then there is European Model EDI Agreement, which forms annex 2 to Commission Recommendation 94/820/EC[78].

The provisions of the agreement cover:

i) Validity and formation of contract[79],

ii) Admissibility in evidence of EDI messages[80],

iii) Liability[81],

iv) Dispute resolution[82],

v) Applicable law and so on.

Then there is *E-commerce Draft Directive*[83]. Here it has been said that any information service provider established in Europe to carry out E-commerce

[75] Directive 95/46/EC of the European parliament and of the Council of October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 23.II.1995 NOL.281, available at http:// www.2 echo.lu/legal/en/dataprot/directive/directive.html. A second directive has been enacted in 1997 in the specific field of telecommunications and complements the general Directive, OJ-1996 (315/30.

[76] Directive 95/46/EC, Article 2 (a)

[77] Ibid, Article 25

[78] 1994 OJ L 338/98.

[79] European Model EDI Agreement, 1994 O.J.L.338/98 Article 3

[80] Ibid, Article 4.

[81] Ibid, Article 11.

[82] Ibid, Article 12.

business would be under the control of the member state where it is establish[84]. This is the solution preferred by the Draft E-commerce Directive. And *Article 9* of the Draft Directive gives legal validity to electronically formed contract.

Then there is *EC draft Directive on Electronic Money*[85]. This proposal has come from European Commission.

Basically there were two proposals. One proposal for a directive was to amend the definition of credit institution within the meaning of the first Banking co-ordination Directive so as to bring electronic money institutions within the general regulatory regime of the First and Second Banking Directive (77/780//EEC and 89/646/EEC). This would allow enterprises issuing electronic money but which do not wish to undertake the full range of banking operations to nevertheless enjoy the benefits of being able to operate throughout the Single Market on the basis of authorization in one Member State (i.e. the single passport' based on home country control) and so be on an equal footing with credit institutions.

At the same time, an effect of this proposal will be on all issuers of electronic money, rather then just credit institutions, could be subject to reserve requirements imposed by the European Central Bank as part of monetary policy measures. However, issuers of electronic money which do not carry out the full range of banking operations would be exempt from certain other prudential supervision rules established in the First and Second Banking Directives and would instead be subject to specific rules established in the proposal on issuing electronic money.

[83] European Commission proposal of November 1998, available at http:// www.ispo.cec.be/E-Commerce/Legal.html#legal.

[84] Ibid Article 2.

[85] European Commission proposal for a directive on the taking up the pursuit and the prudential supervision of the businesses of electronic money institutions of July 1991, available at http:// Europa.eu.int/ISPO/e commerce/legal/documents/ 52000 of 0008_en.pdf.

A second proposal for a directive would define electronic money in a technology neutral manner and the type of business activities that could be undertaken by electronic money institutions. It would also lay down rules concerning. On the issue of cryptography technology, the Regulation[86] and *Decision of the Council of the European Union* of 19th December 1994[87] concerning the contract of the export of dual use goods is the basis for the *EU* regime, which governs the export of cryptography technologies. Another *EU* work is the report released by the payment systems group of the *European Monetary Institute (the EMI)* in 1994, which recommended that banks be given more or less exclusive license to issue prepaid cards[88].

BANK FOR INTERNATIONAL SETTLEMENT (BIS)

The *BIS* has come up with different reports dealing with different issues of electronic banking. In October 1996 it published a report on implications for central banks of the development of electronic money. It provides a brief overview of the main policy issues that arise for central banks as a result of the development of electronic money.

BASLE COMMITTEE ON BANKING SUPERVISION

Other report is *Risk Management for Electronic Banking and Electronic Money Activities 1998.* Here the report has examined the various risks associated with electronic banking and electronic money and has provided possible solutions.

COMMITTEE ON PAYMENT AND SETTLEMENT SYSTEMS

Another Report is *Security of Electronic Money 1996,* this study was carried out by the *Committee on Payment and Settlement Systems and the group of Computer Experts of the Central Banks of the Group of Ten Countries.*

This Report highlights the main design features and functional aspects of electronic money products and analyzes the technical risk specific to these

[86] Council of European Union Regulation, (EC) 3381/94.

[87] Council of European Union Decision on Dec. 1994,94/942/PESC.

[88] Critique of the 1994 EU Report on Repaid cards, 199 of 6, available at DRVSPACE ics.com/docs/papers/1994_critique.html#cb_comp"cpmpetition between Nations.

products. It also describes the possible security measures that can be relied upon to prevent, detect and contain fraud. Another Report by the *Committee on Payment and Settlement System (CPSS)* was Clearing and Settlement Arrangement for Retail Payments in selected countries, September 2000[89].

This Report focuses primarily on *Clearing and Settlement Arrangements for Retail Payment* services provided by financial intermediaries, that as opposed to a physical transfer of cash (banknotes and coins), and it requires the adjustment of accounting entries at financial institutions. Retail payment services include non-cash funds transfer services provided by financial, and in some cases non-financial institutions to end user-clients association with cheques, credit cards and debit transfers, card payments (debit and credit cards) and emerging payment instruments such as electronic money. Another Report by CPSS is, *Survey of Electronic Money, May 2000*[90].

This Report provides information on electronic money products that are in use or being planned to be used in 68 countries or territories. The Report also includes some information on the policy stance adopted by the various authorities concerned, including Central Banks (the CPSS is formed by the central banks of the Group of Ten Countries.

Another Report by *CPSS* was, *Core Principles for Systematically Important Payment Systems, 2001.* [91] The Core Principles in this Report are intended for use as universal guidelines to encourage the design and operation of safer and more efficient systematically important payment systems worldwide. The focus of this Report is on payment systems, i.e. systems that compromise a set of instruments, procedures and rules for transfer of funds among system participants. The most direct application is for systems, which involve only funds transfer.

[89] Report is available at http://www.bis.org/publ/CPSS 40.pdf.

[90] For further details see http://www.bis.org/publ/ 38.pdf.

[91] For more detail see at, http://www.bis.org/publ/cpss.pdf.

Another Report is by, *Basel Committee on banking Supervision,* which came up with consultative document on *Customer Due Deligene for Banks*[92]. Here, this Report has examined the importance of *know your customer* (KYC) standards for supervisors and banks and implementation of KYC standards in a cross-border context.

Another Report which BIS has influenced is the G-10 Deputies Report on Electronic Money Consumer Protection, Law Enforcement, Supervisory and Cross Border Issues, April 1997[93]. This Report focuses on the identification of broad policy objectives among the G-10 countries, like potential consumer risk posed by electronic money and potential policy approaches to consumer protection, potential criminal offences involving electronic money and regulatory and enforcement regimes, potential cross-border concerns and analysis to national approaches to combat these issues to date.

INTERNATIONAL CHAMBER OF COMMERCE (ICC)

The ICC has drafted the *General Usage of Internationally Digitally Ensured Commerce (GUIDEC)*[94]. The principle objective of the *GUIDEC* is to establish a general framework for the ensuring and certification of digital messages, based upon existing law and practice in different legal systems. It also provides standard practices or recommendations relating to ensuring or secure authentication of digital information, and comments upon relevant Civil and Common Law issues. The *GUIDEC* framework attempts to allocate risk and liability equitably between transacting parties in accordance with existing business practice, and includes a clear descriptions of the rights and responsibilities of subscribers, certifiers and relying parties.

[92] For further details see http://www.bis.org/publ/ bcbs 77.pdf

[93] http://www.bis.org/publ/ gten 01.pdf.

[94] For Details see http://www.iccwbo.org/ cust/html/guidec%20a%20 living% 20 document.htm.

NATIONAL RESPONSES

UNITED STATES OF AMERICA (USA)

United States is having comprehensive legislation on electronic banking, electronic money and related issues. However, since technology is constantly changing, so is the legislation on these issues.

United States Law provides criminal sanctions for certain on-line conduct, including intercepting electronic communications, obtaining unauthorized access to computer networks. Federal Law contains two *Criminal Statutes*, directed specifically at on-line activities: *The Computer Fraud and Abuse Act (C.F.A.A.)*[95], *and the Electronic Communications Privacy Act (EC.P.A.)*[96]. The *C.F.A.A.* prohibits a user from gaining unauthorized access either:

- To a computer containing classified or restricted government information, such as national defense information[97],
- To a computer belonging to a financial institution to obtain financial information[98],
- To a computer belonging to a credit card issuer or a credit reporting agency to obtain credit card or credit information[99], or
- To a so-called 'protected computer'[100], which is either a computer operated by or on behalf of the United States government or a financial institution, or a computer used in interstate or foreign commerce[101].

The statute provides civil as well as criminal penalties[102]. The intent required to violate the *C.F.A.A.* is merely the intent to access the concerned computer.

[95] 18 U.S.CC, Section 1030.

[96] Ibid, Sections 2510-2711.

[97] Ibid, Section, 1030 (a) (1).

[98] Ibid, Section, 1030 (a) (2).

[99] Ibid, Section, 1030 (a) (3).

[100] Ibid, Section, 1030 (a) (4).

[101] Section, 1030 e (2).

[102] Section, 1030 (c),(g).

The user need not have the intent to damage the files stored on that particular computer[103].

Federal law under the *E.C.P.A.*, also prohibits the user from intercepting or disclosing electronic communications or intentionally accessing, without authority, a facility where electronic communication services are provided[104]. Other likely 'hacking' activities are similarly prohibited. For example, it is a federal crime, under the *Credit Card Fraud Act*, for a user to key multiple combinations of numbers into credit card Company's computer to discover a valid account[105].

Apart from providing legal solutions to security issues, technical solutions have also emerged. For instance, to insure the security and authenticity of electronic information, businesses can employ encryption technology, digital signatures, or both. For legality of digital signature, *American Bar Association's digital Signature Guidelines and Utah Digital Signature Act* are very important[106]. The use of digital signatures in commerce, like a hand written signature is subject to the uniform commercial code[107], and the *Parol Evidence Rule*[108].

The Parol Evidence Rule allows courts to consider evidence (i.e. digital signatures), beyond that found in the contracts in some situations. Another evidentiary application of digital signatures is the *Best Evidence Rule*[109]. The *Federal Rules of Evidence* expressly provides that;

- The data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an

[103] *United States v Morris*, 928 F. 2d 504 (2d cir 1991), cert denied, 502 U.S 817 (1991) in Dennis Campbell (ed), *Law of International On-line Business: A Global Perspective*, London, 1998.
[104] 18 U.S.C, Sections 2511, 2701, 2702.
[105] *United States v Taylor*, 945 F 2d, at pg. 1051 (8 cir. 1991) in Ibid.
[106] See, Everett Lupton, Comment, *The Digital Signature: Your Identity by Numbers*, Fall 1999, at http:// www.richmond.edu/jolt/v6i2/ note 2.html.
[107] See U.C.C, Section 1-206 (i), 1995.
[108] W. Evertt Lupton, note 106 p. 8.
[109] See Federal Rule of Evidence, 1001-1008.

original[110], although an electronic message is authenticated, a party must still overcome the hearsay rule if it is to be admissible.

- A party may find an application hearsay exception that will admit the electronic communication as evidence for the jury's consideration, one such instance is that of the Business Records Exception[111].

However, since each state has a different law on electronic signatures, some groups are attempting to unify and to standardize the various laws into a uniform law. In this regard, two *Model Laws* addressing electronic signatures, *the Uniform Electronic Transactions Act (U.C.T.A.), and the Uniform Computer Information Act (U.C.I.T.A),* are important. In addition in 1999, two important Bills were introduced in the *House of Representatives* [112], *the Digital Signatures Act of 1999 and the Electronic Signatures in Global and National Commerce Act 1999.*

Apart from this, new forms of implementations of authentication technology are also providing valuable experience and feed back on how authentication technologies and practices can best meet market needs and answer user requirements. US private sector projects based authentication protocols, systems and methodologies include:

- *NACHA/Internet Council*[113]. CA Interoperability Pilot, Working Groups on Authentication and Networks of Trust and CA Rating and Trust,
- *Secure Electronic Transaction*[114] *(SET),* development of protocols to enable secure credit transactions over the Internet utilizing digital signature technology,
- *Financial Services Technology Consortium*[115] *(FSTC),* Bank Internet Payment System (BIPS), protocol for securing and processing secure electronic payments[116].

[110] Federal Rule of Evidence, 1001 (3).

[111] Federal Rule of Evidence, 803 (6).

[112] W. Evertt Lupton, note 106 p. 8, also see for further reference H.R. 1572, 106 H, Cong. 1999, at http:// www.mbc.conn/ecommerce/legis congress.html# 1999_House_Bill_1572 and http:// www.mbc.com/ecommerce/legis congress.html# 1999_House_Bill_1714.

[113] See http:// internet council.nacha.org.

[114] See http:// www.secto.org.

As to the encryption there is no restriction for the use of strong encryption within the country but license for export is required for encryption software with more than 56-bit. Another regulations attached to encryption technology are governed by *Wassenaar Arrangement (1996).*

To combat money laundering *US Department of Treasury's Financial Crimes Enforcement Network (FinCen)*, has issued proposed regulations on May 1997 and they could apply to *Bank Secrecy Act (BSA 1970)*[117] and to electronic banking also.

The proposed regulations however, go even further than the *BSA*, by imposing three additional obligations to the electronic banking sector. Financial institutions are required to provide *FinCen* with detailed reports for currency transactions exceeding $10,000. They must also keep records for all international funds transfers of more than $3,000. Lastly, *FinCen* requires financial institutions to report on *'suspicious transactions'* and *'known or suspected criminal violations'* by filing *Suspicious Activity Reports (SARs).* In addition to these substantive requirements, all money service businesses (other than depository institutions) must register with *FinCen* and provide detailed operational information.

Now we will examine current laws governing electronic funds transfers between businesses, and those involving the consumers.

Credit transfers- whereby the buyer instructs its bank to transfer funds for credit to the sellers account- are governed by *Uniform Commercial Code article 4A*[118], while consumer credit and debit transfers are covered by the *Electronic Fund Transfer Act of 1978*[119], and *Regulation E*[120].

[115] See http:// www.fstc.org.
[116] See http://www.fstc.org/projects/bips.
[117] 12 U.S.C. 1829b and 1951-1959, and 31 U.S.C. 5311-5330.
[118] U.C.C, Article 4A (1991). Debit transfers between businesses are not covered by article 4A.
[119] 15 U.S.C., Section 1693 et seq.
[120] 12 C.F.R., Section 205.

Under *article 4A* , an electronic instruction to a bank to transfer funds to a payee is valid, and the bank is authorized to transfer the funds in accordance with the instruction either if the bank's customer actually authorized the order or if the order is '*verified*' pursuant to a '*commercially reasonable*' security procedure, such as digital signature, on which the parties have agreed, irrespective of whether the customer actually authorized the order[121].

The Electronic Fund Transfer Act, as implemented by *Regulation E*, governs the relationship between banks and consumers regarding electronic transactions in consumer accounts, such as the Automated Teller Machine (ATM) card transactions. Unlike *U.C.C., article 4A*, a consumer will not be bound where his or her electronic signature is used without authority, and the consumer's liability for unauthorized electronic funds transfers is limited as long as the unauthorized transfer is reported diligently[122].

As to the consumer protection, apart from *EFTA, Truth in Lending Act (TILA)*. *TILA* governs the issuance of credit cards and cards with access features, the credit features of an access device, and matters such as finance charges, limitations on consumer liability for fraudulent use, billing errors and other related matters[123].

As to the protection of privacy of consumers financial information, *the Fair Crĕdit Reporting Act (FCRA)*, imposes standards regarding the content and the use of consumer credit reports[124].

As to whether the funds underlying the stored-value cards or other similar electronic payment systems qualify for federal deposit insurance. *The Federal Deposit Insurance Corporation* recently issued a *General Council's* opinion

[121] U.C.C. Section 4A-202 (1991), Also see Ieuan G. Mahony, Chapter 17 in Dennis Campbell (ed), *Law of International On-line Business: A Global Perspective*, London, 1998.

[122] 12C.F.R., Section 205.6, and also Ieuan G. Mahony note 121.

[123] The Truth in Lending Act 1968, 15 U.S.C., 1601et seq, also see Ellen d Alelio and John T Colli, Chapter 8 in Ruh (ed), *The Internet and Business: A Lawyers Guide to the Emerging Legal Issues*, Washington, 1996, pg, 91-96.

[124] See also Fair Credit Billing Act, 15 U.S.C., 1666 (1994), under it credit card issuer must investigate cardholders claims of billing errors.

concluding that the funds underlying stored-value cards do not give rise to a deposit liability and are not deposits under the *Federal Deposit Insurance Act.* However, it stated that depository institutions could design cards in such a way as to carry deposit insurance[125].

Now we will examine other regulatory developments and proposals.

The Consumer Electronic Payment Task Force issued its report in 1998[126]. This report, focused specially on electronic money products as opposed to

Internet applications of existing retail payment systems such as credit cards. It focuses on four principle areas: access, privacy, financial condition of issuers and consumer protection and disclosures. *The Task Force Report regarding privacy concludes that:*

> Privacy protections are essentially evolutionary in the United States, and there is little precedent for comprehensive government established privacy protections. Until e-money has had more time to develop, it is premature to access whether and the degree to which it will present threats to privacy that would warrant government action[127].

The third section addresses consumer concern surrounding e-money issuer insolvency and the fourth section addresses consumers concerns about their rights and liabilities with respect to e-money system.

The Task Force's response regarding these issues is that: (i) existing legal mechanisms may provide a remedy, (ii) industry participants are subject to appropriate market place incentives to enhance consumer protection, and (iii) government responsibilities with respect to e-money be limited at present.

Another important report was the report by the *Task Force on Stored Value Cards*[128].

[125] 61F.R. 40490, August 2 1996. For further details see Ieuan G. Mahony, note 123 pp.664.
[126] The Report of the Consumer Electronic Payments Task Force, 1998, available at http://www.occ.treas.gov/money/ceptfrpt.pdf.
[127] *Ibid*, p. 36.
[128] By the Task Force on Stored Value Cards, "A Commercial Lawyers Take on the Electronic Purse: An Analysis of Commercial Law Issues Associated with Stored Value Cards and Electronic Money", *The Business Lawyer* Vol.52, Feb. 1997, p. 653-727.

The Task Force recognized that for most of these new-stored products legal rules will be the terms and conditions established by the products promoters. There may, however, be instances in which certain aspects of the payment process may not be adequately addressed by the contract terms or the system rules developed by the promoters, so consideration of the applicable commercial law principles is necessary.

US has also proposed, proposed for an *International Convention on Electronic Transactions.* The US government believes that *UNCITRAL* should consider giving substantial attention to an *International Convention on Electronic Transactions.* The convention would remove paper-based obstacles to electronic transactions, and address electronic authentication issues[129].

UNITED KINGDOM (UK)

UK is also having comprehensive legislation on electronic banking and related issues and on some other aspects work is still in progress.

Electronic funds transfers at the point of sale have been in use in the UK since the late 1980's[130] however, law governing this is a recent phenomena. In UK those who issue electronic cash or the money related services are likely to require authorization under the *Banking Act 1987.* However, issuers of products, which do not represent deposit taking (*within the meaning of the Act*) are not subject to authorization, accept where they are owned by commercial banks. Failure to obtain this would be a criminal offence. Companies can get away with issuing pre-paid phone cards or luncheon vouchers because under *Section 5(2) of the Act* ' money paid on terms which are referable to the provision of property or services' is not caught by the Act (provided such money is repayable only in the event that the relevant property or services are not provided[131]. The need for authorization is embodied in *Section 3(1) of the Act* and focuses on the definition of 'deposit' and

[129] Proposal by the United States of America, UNCITRAL Working Group on Electronic Commerce, Thirty Third Session, A/CN.9/WG.IV/WP.77, May 1998.

[130] Hugh Flemington, *England,* Chapter 7, in Dennis Campbell (ed), *Law of International Online Payments: A Global Perspective,* London, 1998.

[131] Ibid, p.264.

'deposit taking business'. Foreign bodies issuing electronic cash must be careful that they do not issue the cash so that they are regarded as accepting deposits within the UK (or their agent is) as they may then require authorization under the Act. Such authorized organization must conduct their business in a prudent manner, which includes ensuring that sufficient capital and liquidity levels are maintained[132].

A further consideration for providers of electronic funds are the *Money Laundering Regulations 1993,* whereby such organizations must adopt systems to clearly identify their customers, monitor transactions, and be able to report suspicious activities, all of which need careful record-keeping, analysis, and audit trails.

The provisions of the *Money Laundering Regulations, 1993* will apply to all forms of electronic money. A second European Union Money Laundering directive is expected in future and this is, likely to make specific reference to electronic money[133].

The majority of the On-line business-to-consumer transactions are currently affected by credit or debit card payments. Here consumer protection is provided by the *Consumer Credit Act 1974*[134]. Under this Act, a consumer cannot generally be made liable for the misuse of credit card by a third party[135], although the terms of the credit card agreement can make the card holder liable, once the card has been accepted, for the first £ 50 while the card is not in their possession and any loss accrued by a third party who has the possession of the card with their permission, until the card issuer receives notification of the loss of the card[136].

[132] Ibid, p.265.

[133] Survey of Electronic Money Developments, CPSS, May 2000, available at http://www.bis.org/publ/CPSS38.pdf.

[134] Section 75 of this Act applies to transactions whereby any single item is worth Pound 100 and Pound 30,000 and there is a pre-existing agreement between the card issuer and the supplier. This gives the debtor the right to pursue the supplier or the card issuer itself for misrepresentation of breach of contract, as the Act makes the card supplier jointly and severally liable.

[135] Consumer Credit Act 1974, Section 83.

[136] Ibid, Section 84.

As to the fraud on On-line credit card payments, much will depend upon the provisions of the relevant contracts between Card Company, retailer and customer as to where any resulting loss lies. In *Orr v. Union Bank of Scotland*[137], it was established that a bank cannot debit a customers account following presentation of a forged cheaque (although it may have been undetectable). This ought to apply to fraudulent card instructions. However the Orr principle is limited to certain exceptions. The principle in Orr may be varied contractually[138], but this may be unlikely, given the hurdles imposed by the *Unfair Contract Terms Act 1977, the Unfair Terms in Consumer Contract Regulations 1994, and the Good Banking Code of Practice 1999.* As to the criminal sanctions for certain on-line conduct, including intercepting electronic communications, obtaining unauthorized access to computer network and so on. It has come under *Computer Misuse Act of 1990*, which has already been dealt in Chapter III.

Now we will examine the legal status of the electronic signature and encryption, which are the keys to the security of e-banking and electronic money.

The *Electronic Communications Act 2000* provides recognition to the electronic signature and the activities of what are referred to as cryptography service providers. The Act eschews the distinction between electronic and advanced electronic signature, instead providing that:

> 'In any legal proceeding[139], (i) an electronic signature incorporated.....with particular data, and (ii) the certification by any person of such a signature, shall be admissible in evidence in relation to any question as to the authenticity of communication.....'

Section 6 of the Act deals with cryptographic service provider, where it has been stated that the service must either be provided from premises within the UK

[137] 1854, Macq H.L (as 512), also see, Hugh Flemington, note 130, p. 266

[138] However, much of the difficulty inherent in trading on the Internet is that there may not be any express contract governing the transaction and it may therefore be necessary to rely upon the doctrine of implied terms. As in other contracts, this is not an ideal way to proceed as the outcome of litigation would be by no means certain.

[139] Electronic Communication Act 2000, (Section 7/1)

or provided to persons carrying on business in the UK. As to regulation of encryption technology, there is no restriction on use and also there is no restriction on import or export of strong encryption.

As to the data protection and privacy it has been safeguarded by *UK Data Protection Act 2000.* It applies when a person is established in the UK, i.e. is ordinarily residing in the UK or is a UK incorporated body, or is not established in the UK but uses equipment in the UK for processing data, or practically, if data is exported to that person from the UK. The types of information, which the *UK DPA* is concerned with, are personal data. Failure to comply with the *UKDPA* may result in criminal penalties for Companies and their individual managers and personal data shall not be transferred to a country outside the EEA, unless that country ensures an adequate level of protection (eighth principle).

INDIA

Now we will examine the Indian response to electronic banking and electronic money issue and what is the present scenario.

First we will examine the *Information Technology Act 2000 (IT Act).* In the *IT Act 2000*,legal recognition is given to digital signature [140] and authentication of electronic record[141] through digital signature. It has also dealt with certifying authority to issue digital certificate[142]. Further *IT Act 2000* also deals with computer crimes which has been dealt in *Section 45* and criminal action which have been dealt in *Section 44, 45, 65, 66 and 67.* It has already been dealt in detail in Chapter II. It also covers data protection, which has been dealt in *Section 72.* As to the evidential value of digital signature, the new section, *Section 67 A*[143] and *Section 73 A*[144] has been inserted in *Indian Evidence Act, 1872.* As to the

[140] See Section 5 of the IT Act, 2000.

[141] See Section 3 of the IT Act, 2000.

[142] See Section 35 of the IT Act 2000.

[143] Section 67 A talks about proof as to the digital signature.

[144] Section 73 A talks about proof as to verification of digital signature

admissibility of electronic records it has been dealt in *Section 65 B of the Indian Act, 1872.*

Amendment has also been done to the *Banker's Book Evidence Act 189*, for recognition of printouts of data stored in floppy disc, tape or any other form of electromagnetic data device as prima facie evidence in the Courts of Law and the *Reserve Bank of India Act 1934*[145]. However, this *IT Act 2000* does not apply to a negotiable instrument[146] as defined in *Section 13 of the Negotiable Instruments Act, 1881 (26 of 1881).*

The following are the main legal issues, attached with EFT which the Shere Committee has examined and recommended[147]:

(a) Irrevocability- Finality of payment

As to irrevocability, the point of time upto which payment instructions can be changed or cancelled by the issuer when the instructions are without any paper is not provided by the existing law. *The Shere Committee*, has recommended that the payment order shall become irrevocable when the sending bank executes it. 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. As to the finality of payment, *the Negotiable Instruments Act 1881*, which provides for rules of finality of payment, cannot be applied to EFT, as EFT does not involve any paper instrument. *The Shere Committee* has recommended that payment under the EFT shall be final when receiving bank credits the funds to the account of the beneficiary whether or not the beneficiary is advised of the credit.

(b) Liability for loss in case of fraud, technical failures and errors

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

[145] See Section 93 and Fourth Schedule of the IT Act 2000.

[146] Section 1 (4)(a) of the IT Act 2000.

[147] The report is available at http://www.securities.com.pl/public/public98/RBI/publican/pul 990717-7html. Discussion on the report is available at http://www.bankersIndia.com/committeesksshere_committee,htm.

times negligence may lead to error. This rule for allocation of loss arising on account of errors are generally based upon principles of Contracts and Torts. Generally, if the loss can be attributed to the conduct of the 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 the party whose conduct lead to the fraud to take place or caused an error to take place, must bear the loss.

(c) Allocation of loss in case of insolvency

EFT is a method or means. But the incidence of insolvency of any bank involved in EFT could be substantially different from those arising in a paper-based payment. In EFT, there could be a float between a point of time the payment order is issued by a customer to the point of time when payment is complete. The issue that needs to be focused 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 the beneficiary's bank bear the loss?

The Companies Act or Banking Regulation Act, 1949 (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.

A predetermined fee towards the corpus of the contingency fund could be raised from the participating members. This however, will not be possible unless the existing provisions of the Insurance Act are amended.

(d) Evidence and burden of proof

The Committee has pointed out that there are basically two issues in regard to proof of *EFT*:

- Should there be any legal obligation on any service provider to issue a print out of written record on completion of an electronically completed transaction?
- Whether and to what extent computer print out should be admissible evidence?

The Committee suggested that, 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 need to be made. Rules of evidence in regard to computer-based transactions have already been developed in the UK, both in civil and criminal proceedings. It is time that we address ourselves to those problems. However, this problem in parts has been solved by the amendment to *Evidence Act 1881*, as it was previously pointed out.

(e) Data protection

A clear understanding of the risk involved in transmission of data through a communication network and keeping records of transactions and other electronic devices is necessary. The possibility of unauthorized 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 unauthorized access, it may be different if the design of the system depends on general telecommunication facility. However, much of the problem has been solved through the enactment of the *IT Act, 2000*[148].

(f) Dispute resolution

Provision for separate investigation and dispute resolution mechanism is felt necessary especially in regard to high value funds transfers. In the US, in regard to *EFT* of all types, specific statutory provisions are made to provide 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

[148] See Section 72 of the IT Act 2000.

understanding of the concepts and technological aspects in investigating and resolving disputes.

Under the existing framework of Indian Law, the bank customers have the following remedies:

- To approach civil courts by suit for damages, injunction or specific performance.
- To approach *Consumer Forums* established under the *Consumer Protection Act.*
- To avail *Customer Grievance Redressal Machinery* provided within the banking system (such as complaint to *Banking Ombudsman*, complaint to *Reserve Bank Grievance Cell* etc).

Given the existing rules of *Evidence Law* and the general delay in judicial system, resolution of grievances through courts may not be suited to *EFT* disputes.

The question whether a separate system of arbitration or other forms of adjudication of disputes between banks and their customers, arising under the *EFT* would be necessary, can be better understood when a clear idea about the types of disputes commonly raised and the number of such disputes are known.

(g) Prevention of Fraud

Fraud in an *EFT* involves an unauthorized instruction, alteration of the amount or alteration of the name of the beneficiary etc. Prevention is the elimination of the cause itself, by directing the incidence on the person who causes it. There are basically two issues involved here:

- What should be the responsibility of the service providers and users in regards to design of the system?
- Whether fraud in *EFT* should be made a punishable offence and if so, what elements should constitute the offence?

Misuse of computers and other electronic devices through unauthorized access is not the problem of the *EFT* only, rather, it is common to all computer-based transactions. It is for special significance for *EFT* due to high potential and intensity, given the sums involved, especially in high value transfers, and the ease with which it can be penetrated.

Though much of the problem has been tackled by the *IT Act, 2000*. But, still *EFT* specific resolution is required[149].

(h) Settlement of Inter-bank payment obligations

In an *EFT* environment, the following specific aspects need special mention[150]:

- The frequency with which the transactions are netted,
- The period of time after netting, within which settlement of net balance is made,
- Whether netting or settlement is by pairs of banks or for the clearing as a whole, and
- The means of settlement.

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.

Recommendations of the Shere Committee Report[151]

The Shere Committee had recommended framing of *RBI (EFT system) Regulations under Section 58 of the Reserve Bank of India Act 1934 (RBI Act)*, amendments to the *RBI Act 1934* and to the *Bankers Books Evidence Act 1891*, as short term measures, and enacting of a new Acts such as the *Electronic Funds Transfer Act, the Computer Misuse and Data Protection Act* etc, as long term measures.

Narasimham Committee Report[152]

The Committee on Banking Sector Reforms (Narasimham Committee II) has in its report dealt with, the issues in technology up-gradation and observed that most of

[149] For further discussion see, P.S. Bindra, *IT Implementation in Banking-Legal Implications*, available at http://www.securities.com.pl/public/public98/RBI/publican/pub 981222-2.html

[150] Ibid.

[151] Report is available at http://www.bankersindia.com/committees/Shere Committee.html.

[152] Recommendations of the Report are available at hhtp://www.bankersindia.com/committiees/ Narasimham II Committee html.

the technology that could be considered suitable for India in some form or the other has been introduced in some diluted form as a pilot, but the desired success has not, however, been achieved because of the reasons *inter alia* lack of clarity and certainty on legal issues.

The Committee has also suggested implementation of necessary legislative changes keeping in view the recommendation of the *Shere Committee*. The need for addressing the following issues was also emphasized:

- Encryption on the *Public Switching Telephone Network (PSTN) lines*,
- Admission of electronic files as evidence (this has been legally recognized in the inserted *Section 65 B of the Indian Evidence Act 1872, the Second Schedule of the IT Act 2000*),
- Treating electronic funds transfers at par with crossed cheques/drafts for purposes of income tax, etc

Vasudevan Committee Report[153]

The Vasudevan Committee appointed by the Reserve Bank of India, submitted in July 1999 its report on technology upgradation in the banking sector. The legal framework for electronic banking has been specifically identified by the Committee. The Committee has made the following recommendations:

- The Reserve Bank may suggest the amendments in the *Reserve Bank of India Act 1934*, and assume the regulatory and supervisory powers on payment and settlement systems. Simultaneously, the *RBI* may promote a new legislation on *Electronic Funds Transfer System* to facilitate multiple payment systems to be set up for banks and financial institutions.
- *The RBI and the IBA* should pursue with the *Department of Telecommunications (DoT)* / other competent authority to permit encryption of data files/ messages transmitted through communication

[153] The Report is available at http://www.securities.com/public/public99 RBI/publican/pub 990717-10.html.

channels for facilitating easier access to remotely located branches of the *INFINET* network.

- A standing Committee to examine legal issues on *Electronic Banking* with members drawn from the legal departments of the *RBI, IBA* and a few banks, may be set up by the Reserve Bank.
- *CBDT* would need to take up the questions of amending the relative provisions of the *Direct Tax Laws like Section 40 A of the Income Tax Act 1961*, to accord electronic funds transfer the status of crossed cheques/ drafts for the purpose of payment of income tax and other taxes.
- The definition of the presentment in the *Negotiable Instruments Act 1881*, have to be amended to permit electronic presentment of data or image of the cheaque to facilitate the introduction of cheaque transaction in India. *The Reserve Bank* may be empowered to frame *Regulations on Cheaque Truncation* by suitable amendment to the *Reserve Bank of India Act 1934.* Appropriate changes may accordingly be incorporated in the *Clearing House Rules and Regulations* as well.
- There should be a clear distinction between the role of a service provider and that of a regulator and supervisor.
- The proposed *Standing Committee of legal issues on Electronic Banking* may, among others, consider the need for appropriate regulation/ legislation on netting of inter-bank payment obligations arising out of the EFT systems which would operate on deferred/ discrete/ netting basis.
- Issues on confidentiality of data in the computerized environment and in the context of the bankers secrecy obligations require a detailed scrutiny which may be examined by the proposed *Standing Committee of legal issues on Electronic Banking.*

We can say that many of the recommendations have been given effect in the *IT Act 2000.* However, there is still a need for a separate Act for *Electronic Funds Transfers* because certain transactional issues like payment, finality, rights and obligations of the parties involved in the electronic funds transfer etc cannot be covered by general purpose Act like the *IT Act 2000.*

RBI has already prepared draft EFT *(RBI System) Regulation under Section 58 of the RBI.* However, *EFT (RBI System) Regulation prepared by the Reserve Bank* would address only the specific type of EFT system that the Reserve Bank would be involved with as a service provider as well as a regulator. The *EFT (RBI System) Regulations* would , moreover, cover only credit transfer related transactions and not *Debit Clearing Transactions.* A separate legislation on the lines of *Electronic Funds Transfers Act of USA* is, therefore, required which would be consumer protection oriented and would at the same time address transactional issues like execution of payment order, settlement and finality, etc.

The existing provisions of the *RBI Act and BR Act* give power to *RBI* to regulate payment system only within the banking and financial sector. Separate legislative framework either by further empowerment of *RBI* or a separate Act is necessary if multiple *EFT* systems should be allowed to develop.

Now we will discuss issues relating to e-money[154].

The issuance of paper currency and coinage in India as legal tender is governed by the Constitution of India and some Central statutes. The Reserve Bank has the sole right to issue currency notes[155]. Issue of e-cash in a closed system where redemption of money occurs frequently may not be viewed as a substitute to currency notes and coins. But when e-money products allow multiple transfers among individuals without requiring the direct involvement of a third party, in a manner similar to person-to person exchange of currency notes, it is likely that such e-money could act as a substitute to cash, However, e-money would not constitute valid legal tender.

Here the question is, who can issue e-money? At present, there is no legislation in India that governs the issue of e-money. The government needs to

[154] E-money includes: E cash, Net cash, Digital cash, and Cyber cash.

[155] Section 22 of the Reserve Bank of India Act, 1934.

decide who will be allowed to issue e-money. Will only banks be allowed or will other financial institutions and corporations also be allowed? In the US for example, nationally chartered banks have been given the right to operate a subsidiary to carry out digital cash operations subject to an intensive scrutiny[156]. In this regard it can be said that rather than simply clarifying whether under the existing laws private issuers can issue e-money, the *RBI* should address the issue of whether the private sector should be allowed to issue e-money. If the *RBI* decides to permit private issuance, it will have to develop rules and regulations affecting the issue and conduct of e-money business in India.

The problem of varying standards of regulations among nations and within nations can be overcome when we have some supranational organization (like *Bank for International Settlements*) or association laying down uniform standards. With the blurring of boundaries within the sectors (security business, insurance and banking) of the financial system a unified regulator along the lines of the *Financial Service Authority of the UK* might be the most effective regulatory body[157].

As to the money laundering and tax evasion many jurisdictions have cash/ financial reporting requirements. In India the *Income Tax Act of 1961*, has some provisions that seek to control or track the flow of funds through electronic means. However, some specific law is required to combat these menaces in a society.

As to the use of encryption for the security of e-money in electronic funds transfers at present there are no restrictions on the use and export but license for

[156] In considering whether or not to permit banks to operate such a subsidiary the Office of the Comptroller of the Currency (OCC) applied four criteria, (i) is the operation related to banking, (ii) Do the banks have sufficient control to dis-allow non-banking activities?, (iii) is the banks loss exposure limited, (iv) is the investment related to the banks ordinary banking business? The approval was granted in cases where the OCC found that the answers to all the questions were yes.

[157] Nishith Desai, *Legal and Policy Framework for E-Commerce in India*, available at http://www.giic.org/pubs/indiawhitepaper.pdf.

import is required[158]. However, there are no encryption standards for transactions within the country.

[158] Daniel Amor, *The E-Business Revolution: Living and Working in an Inter-Connected World*, London, 1999, p.126.

Chapter - V
Conclusion

CHAPTER V

CONCLUSION

From the above discussion it is clear that electronic payment systems are widely used in commerce and include wholesale payments, wire transfers, recurring bill payments, the automated clearing house, and electronic check presentment. They also include e-cash, electronic checks, smart cards and electronic purses. However, payment systems are an area of ongoing innovation, and as our discussion suggests, new technology will continue to emerge.

Banks now have a variety of technological means to initiate online banking programs without incurring the investment needed to develop their own systems. The reach and delivery capability of computer networks such as the Internet far exceeds any proprietary bank network ever built, and makes it continually easier for customers to manage their money anywhere, anytime. Therefore, there is an increasing pressure to move from existing paper-based payment systems to electronic transfer. Microsoft's Chairman, Bill Gates, is not alone in believing that the convergence of money, commerce and personal computers represents one of the great new markets of modern times. New and unforeseen opportunities can be expected to arise once a secure and cost effective "mass" market electronic system for making low value payments is successfully established.

In India too, changes are taking place in the payment system. The Indian Bank's Association (IBA), recently launched EFT (electronic fund transfer) and ECS (electronic clearing system), as major electronic banking products. EFT is the safest and fastest way to transfer money, regardless of bank, branch, or city. ECS enables deposit of dividends into the shareholder's account, if the bank account is given. In September 2000, the Institute of Development and Research in Banking Technology (IDBRT), implemented its long-awaited EFT and Real-Time Gross

Settlement (RTGS) system, with services available throughout India. The Indian Financial Network (INFINET), a VSAT based communication backbone for the national payment system, was equipped with a full transponder on the INSAT- 3B satellite to carry out its operations. IBA has also introduced a system of shared payment network (Swadhan). Basically this is the name given to the ATM network of public sector banks and some private banks.

However, as discussed in Chapter III, there are a whole lot of legal and policy issues attached to electronic banking and electronic money, and some concerns are attached with the working of the electronic payment system itself. A key issue is: the security of the transaction of the payer and the payee. It includes issues relating to the privacy of the transaction, who precisely should have access to the details of the payer, the identity of the payer, the irrevocability of the payment, the identity of the cash issuer where some form of electronic cash is being used, the ease with which small value payments can be handled, the universality of acceptance of the type of electronic payment. Apart from this the main legal and policy issues are: money laundering, tax evasion, application of law of evidence, consumer protection, contract terms and enforceability, and implications for Central Banks of the development of electronic money.

How are these issues to be addressed? There is no denying that there is an important common thread running through the various aspects of electronic banking laws. Despite this the emerging legal regime for electronic banking suffers from a major problem in the disparity among the national laws. In a nutshell, the type and scope of transactions covered, and remedies provided by national "electronic banking laws" is not the same across national jurisdictions. However, not much legislation has been enacted for dealing with the different aspects of electronic banking. Since the basic banking procedures are the same, whether a funds transfer is made by paper-based means or electronically, should not make much difference. Therefore, many of the rules governing paper-based funds transfers can be applied to electronic funds transfers with appropriate results. Where necessary, rules should be reconsidered in the light of the new banking and legal environment. USA's proposal in this regard is that, nations shall make only those changes to the laws that are necessary to support the use of electronic funds transfer. Existing rules should be modified and new rules should be adopted only in co-operation with the private sector and that too where it is necessary.

As to criminal laws, different nations have enacted laws but they are not electronic banking specific. For example in UK, *the Computer Misuse Act 1990* and in India, *the Information Technology Act, 2000* and in USA, *the Computer Fraud and Abuse Act*, exist, but their provisions will also apply in the area of electronic banking. In the area of prevention of money laundering, nations have modified their existing money laundering acts. In USA Treasury's Financial Crimes Enforcement Network (FinCen), issued proposed regulations on May 1997 applying Bank Secrecy Act 1970, to electronic banking. In UK the provisions of the Money Laundering Regulations 1993 will apply to all forms of electronic money. In India however, legislation is still awaited. In addition, the Financial Action Task Force on Money Laundering is also working on this issue.

As to question of tax evasion, electronic cash presents a potential problem for income tax collection. The technology makes it easy for individuals to store vast sums of electronic cash in offshore accounts. Unlike a notational or accounting system based on an electronic bank balance or credit facility, these accounts could be anonymous, making it much easier for people to evade tax. However, efforts are going on, to sort out problems associated with electronic cash. In particular, the OECD, has undertaken a project to assess tax evasion issues in electronic commerce and the implications of the development of electronic money for the relevance of existing tax principles. The OECD report on Bank Secrecy recommends that there should be international access to bank accounts for tax investigations on administrative application.

Another problem relates to the law of evidence, because electronic records are vulnerable to tampering and there is no foolproof way of authentication. Some of the concerned problems have been dealt with by the UNCITRAL Model Law on Electronic Commerce, UK Electronic Communications Act, 2000, USA, Uniform Electronic Transactions Act and in India Information Technology Act, 2000.

As for the security, secure communications protocols such as SSL and S-HTTP can be used to secure web-based sessions including commercial data transactions. Although these protocols authenticate both parties and provide privacy in the transaction, they do not provide protocols for payments. To fill this void, a number of payment systems have emerged, from CyberCash and SET to DigiCash, Mondex and VisaCash. However, as was concluded by the Task Force (Committee for Payment and Settlement Systems, Group of Ten Countries), on Security of Electronic Money, no system can be made fully secure against all types of attacks. Determining the appropriate level of security for a particular product should involve consideration of the magnitude of potential risks, the cost of implementing varying level of security, the impact on the functionality of the product and the implications for privacy. Owing to the technical complexity of these products and the high level of scientific expertise required to assess many aspects of security, it may be difficult for one organization to evaluate objectively and comprehensively, the security of an entire product. The Task Force concluded that an integrated, overall risk-management approach to security, including independent security assessments, is an important component of the security of these new products.

As should have been clear from the discussion in Chapter III and IV secure payment needs, use of digital signature and authentication and certification, which in turn uses encryption products. However, there is no clear-cut and uniform rule about digital signature, authentication, certification and encryption. The international nature of the Internet makes it imperative that national definitions of

" signature" be harmonized as they relate to electronic authentication. This can best be done by understanding the changing role of written signatures, educating policy makers and governments, and developing an internationally oriented definition of the "signature". A basis for such a definition could be a scalable set of signature requirements based on the security needs of the particular application, such as whether electronic authentication was used to establish identity, to demonstrate a particular attribute of the signatory, or for some other purpose. However, UNCITRAL Uniform Model Law on Electronic Signature will be helpful in developing national laws in this regard. In USA a proposed Uniform Electronic Transaction Act and the Uniform Computer Information Act, contain appropriate provisions in this regard. Similarly, UK has come up with Electronic Transactions Act 2000. And in India provisions regarding this are contained in Information Technology Act 2000. In this regard OECD's Inventory of Approaches to Authentication and Certification in a Global Networked Society is commendable.

As to the encryption, different countries have different regulations. In USA there is no restriction in domestic use but there are restrictions on the export of it, which is hindering the growth of electronic money products. But here the problem is that if there is no restriction then it can be used by criminal elements also, so it will pose a threat to law enforcing agencies.

As to cryptography, the international nature of crime and cryptography make it necessary for there to be international regulation of cryptography. The current technological and legal environment does not adequately protect legitimate law enforcement interests in regard to access of information. A solution may yet be possible that would restore the balance between privacy and law enforcement needs for access. However, any such solution must be implemented on an international scale if it is to be effective.

As regards to the privacy protection, laws have been introduced or will be introduced shortly in many of the countries. Here EU Privacy Directive 1995 appears to be the driving force for all nations including the USA. The USA protects personal data through Electronic Communication Privacy Act, 1986. UK also has a separate legislation in the form of UK Data Protection Act, 2000. In India Information Technology Act, 2000, provides for some protection but not of an appropriate standard. However, in any proposed privacy legislation a balance should be maintained between individual and industry interests.

As has been discussed in Chapter III, there are many risks associated with electronic payment systems. But the issue here is who should bear the risks? As of now there is no clear-cut law regarding this. Most of the time it is governed by the contractual relationship between the issuer of money and the customer. As to this type of contract, it is important to recognize that one of the factors a court would surely consider when deciding whether to enforce a particular contract is that these products are designed for sale to individual consumers and not to sophisticated commercial parties. Some level of protection has been afforded to consumers in USA by Electronic Fund Transfer Act, and in UK through Consumer Credit Act, 1974 and some other laws. In India there is no specific legislation in this regard. The UNCITRAL Model Law on International Credit Transfer, 1992 provides for some protection but this is for an international credit transfer. Here, one suggestion can be of development of alternative dispute resolution in solving consumer problems.

Another problem is of determining the jurisdiction and law, as to whose law will be applicable in a given situation, because the nature of the electronic money is such that geographical and political boundaries are rendered irrelevant. As the problems attached to e-banking are trans-national in their scope and dimension, they require international co-operation.

As to the implications for Central Banks, it has been said that substitution of electronic money for cash would lead to a corresponding decline in Central Banks asset holdings and the interest earned on these assets that constitutes Central Banks seigniorage revenue. However, till now the impact is not yet felt, but if the spread of electronic money becomes extensive, the loss of seigniorage could become a concern to Central Banks. To the Central Bank Regulation, to new electronic payment products. It is argued that only a policy of minimal regulation is likely to be structurally practical. Other ways of thinking include that the electronic payments and electronic money be placed in the legal mainstream i.e. giving legal tender status to electronic money.

One of the biggest hurdles in the development of electronic baking specific laws is that most of the work has been done in the field of electronic commerce in general, and from here one derives the rule for electronic banking. And attached to it is the fact that no international organization has tried to develop a Model Law on electronic banking. Whatever work has been done, it is in bits and pieces, as is clear from our discussion in Chapter III and IV. UNCITRAL has come up with electronic banking specific Model Law, but it is, as the name suggests, for international credit transfers, and does not apply to debit transfers and domestic transfers.

Designing an appropriate regulatory framework for electronic money involves balancing different objectives including the system stability and security, financial integrity of the issuers, protection of consumers and the promotion of completion and innovation. Therefore, in general, the framework should be e-neutral. However, at the early stage, without any successful experience, authorization and supervisory regime for electronic banking and electronic money would be similar to that for conventional banking service and products, and they should be adjusted and readjusted following the development of electronic money. Regulatory authorities also face a choice concerning the timing of the introduction of any possible regulatory measures. On the one hand, establishing a comprehensive regulatory framework at an early stage risks stifling innovation. However, as Greenspan, the Chairman of the Federal Reserve Board of the USA, recognized, that in the current period of change and market uncertainty, there may be a natural temptation for the regulators and market participants to have the government step in and resolve the uncertainty, through standards, regulation, or other government policies.

Finally, it may be said that while the emergence of new cyber space payment systems is unsettled, the role of law and lawyers in the development of these systems is equally unsettled. There are a few existing sources of public laws, which clearly apply to these new products. The product has to work with existing payment systems before associated legal issues become important. Standards-setting bodies are therefore, initially, the most important sources of rules, and proper information security practices are more important than legal certainty.

Ultimately, the new payment system aspires to a state where, as with legal tender and credit cards, the legal rules are well settled.

Appendix

APPENDIX I

GLOSSARY

Access products: products that allow consumers to access traditional payment instruments electronically, generally from a remote location. Examples include electronic funds transfers at the point of sale and home-banking facilities through a personal computer.

Acquirer: in an electronic money system, the entity or entities (typically banks) that hold deposit accounts for merchants and to which transaction data are transmitted.

Asymmetric cryptography (also called public key cryptography): a set of cryptographic techniques in which two different keys (private and public keys) is used for encrypting and decrypting data. The private key is kept secret by its holder while the public key is made available to communicating entities.

Authentication: the methods used to verify the origin of a message or to verify the identity of a participant connected to a system.

Balance-based system: an electronic money system in which the electronic funds are stored on a device as a numeric ledger, with transactions performed as debits or credits to a balance.

Biometric: refers to a method of identifying the holder of a device by measuring a unique physical characteristic of the holder, e.g. by fingerprint matching, voice recognition or retinal scan.

Bit: the basic data element: a binary digit, either 0 or 1.

Brute-force attack: a method of cryptanalysis in which every possible cryptographic key is tried.

Byte: a series of 8 bits.

Certification authority: an entity entrusted with creating and assigning public key certificates.

Challenge-response: a means of authentication in which one device replies in a predetermined way to a challenge from another device, thus proving its authenticity.

Chip card: also known as an IC (integrated circuit) card. A card containing one or more computer chips or integrated circuits for identification, data storage or special-purpose processing used to validate personal identification numbers (PINs), authorise purchases, verify account balances and store personal records. In some cases, the memory in the card is updated every time the card is used (e.g. an account balance is updated).

Ciphertext: the encrypted form of data.

Clearing system: a set of procedures whereby financial institutions present and exchange data and/or documents relating to funds or securities transfers to other financial institutions. The procedures often also include a mechanism for the calculation of participants' bilateral and/or multilateral net positions with a view to facilitating the settlement of their obligations on a net basis.

Closed network: a telecommunications network that is used for a specific purpose, such as a payment system, and to which access is restricted.

Confidentiality: the quality of being protected against unauthorised disclosure.

CPU (Central Processing Unit): area of a computer system (and of an IC card) that performs computations.

Credit card: a card indicating that the holder has been granted a line of credit. It enables the holder to make purchases and/or withdraw cash up to a prearranged ceiling; the credit granted can be settled in full by the end of a specified period or can be settled in part, with the balance taken as extended credit. Interest is charged on the amount of any extended credit and the holder is sometimes charged an annual fee.

Credit institution: the definition given to a "bank" in the European Union. The First EC Banking Directive defines it as an undertaking whose business is to receive deposits or other repayable funds from the public and to grant credits for its own account.

Cryptanalysis: area of cryptography dedicated to studying and developing methods by which, without prior knowledge of the cryptographic key, plaintext may be deduced from ciphertext.

Cryptographic algorithm: a mathematical function used in combination with a key that is applied to data to ensure confidentiality, data integrity and/or authentication. Also called cipher.

Cryptography: the application of mathematical theory to develop techniques and algorithms that can be applied to data to ensure goals such as confidentiality, data integrity and/or authentication.

Debit card: a card enabling the holder to have purchases directly charged to funds on his account.

Derived key: a cryptographic key that is obtained by using an arithmetic function in combination with a master key and a unique identification value such as a card serial number.

DES (Data Encryption Standard): a symmetric cryptographic algorithm (ANSI standard) that is widely used, in particular in the financial industry. Triple-DES consists of operating three times on a set of data (encrypting-decrypting-encrypting) using a double-length DES key.

Digital signature: a string of data generated by a cryptographic method that is attached to a message to ensure its authenticity as well as to protect the recipient against repudiation by the sender.

EEPROM (Electronically Erasable Programmable Read-Only Memory): the area of an IC chip used to store data. Data in EEPROM can be electronically erased and rewritten under the control of the operating system.

Electronic money (e-money): monetary value measured in currency units stored in electronic form on an electronic device in the consumer's possession. This electronic value can be purchased by the consumer and held on the device and is reduced whenever the consumer uses the device to make purchases. This contrasts with traditional electronic payment transactions such as those with debit or credit cards which typically require online authorisation and involve the debiting of the consumer's bank account after the transaction.

Electronic purse: typically an IC card containing an application that stores a record of funds available to be spent or otherwise used by the holder; the record of funds is updated as transactions are made. Additional funds may be added to the stored balance through a withdrawal from a bank account or by other means. Sometimes referred to also as a stored-value card.

Electronic wallet: a computer device used in some electronic money systems which can contain an IC card or in which IC cards can be inserted and which may perform more functions than an IC card.

Embedding: in IC card manufacturing, the process by which the chip module is mounted on the plastic carrier (card).

Encryption: the use of cryptographic algorithms to encode clear text data (plaintext) into ciphertext to prevent unauthorised observation.

EPROM (Electronically Programmable Read-Only Memory): the area of an IC chip used to store data. Data in EPROM can only be written once and cannot be erased selectively.

Face-to-face payment: a payment carried out by the exchange of instruments between the payer and the payee in the same physical location.

Firewall: a hardware- and/or software-based system that is used as an interface between the Internet and a computer system to monitor and filter incoming and outgoing communications.

Fleckless: from the German "fleckenlos", which means spotless; a device (card) or a system is said to be fleckless when it can provide evidence that it has not been tampered with.

Home banking: banking services which a retail customer of a financial institution can access using a telephone, television set, terminal or personal computer as a telecommunication link to the institution's computer centre.

Hot list: in a card-based system, a list - held by the merchant terminal or other device – of suspicious card numbers or ranges of suspicious card numbers. The hot list is used to detect and to block any transaction with such cards.

IC Card (Integrated Circuit): a plastic card in which one or more integrated circuits are embedded. Also called chip card.

Integrity: the quality of being protected against accidental or fraudulent alteration or of indicating whether or not alteration has occurred.

Internet: an open worldwide communication infrastructure consisting of interconnected computer networks and allowing access to remote information and the exchange of information between computers.

ISO (International Organization for Standardization): an international body whose members are national standards bodies and which approves, develops and publishes international standards.

Issuer: in a stored-value or similar prepaid electronic money system, the entity which receives payment in exchange for value distributed in the system and which is obligated to pay or redeem transactions or balances presented to it.

Key length: the number of bits comprising an encryption key.

Key management: the design of the life cycle of keys and the relationships between keys which are used in a computer system for cryptographic purposes. Alternatively, when referring to a system in operation, the processes by which cryptographic keys used in a computer system are generated, stored and updated.

Key: a unique series of digits used in combination with a cryptographic algorithm.

Large-value funds transfer system: a funds transfer system through which large-value and high-priority funds transfers are made between participants in the system for their own account or on behalf of their customers. Although, as a rule, no minimum value is set for the payments they carry, the average size of payments passed through such systems is usually relatively large. Large-value funds transfer systems are sometimes known as wholesale funds transfer systems.

Large-value payments: payments, generally of very large amounts, which are mainly exchanged between banks or between participants in the financial markets and usually require urgent and timely settlement.

Limited-purpose prepaid card: a prepaid card which can be used for a limited number of well-defined purposes. Its use is often restricted to a number of well-identified points of sale within a well-identified location (e.g. a building, corporation or university). In the case of single-purpose prepaid cards, the card issuer and the service provider may be identical (e.g. cards used in public telephones).

Load: the action of transferring electronic balance from an issuer to a consumer's device.

MAC (Message Authentication Code): a hash algorithm parametrised with a key to generate a number which is attached to the message and is used to authenticate it and to guarantee the integrity of the data transmitted.

Mask: the hardware specifications that define the physical and functional properties of the IC chip.

Master key: a cryptographic key, often used to generate other cryptographic keys.

Memory card: an IC card capable of storing information only.

Multipurpose prepaid card: a prepaid card which can be used for a wide range of purposes and has the potential to be used on a national or international scale but may sometimes be restricted to a certain area.

Non-bank financial institution: a financial institution that does not come under the definition of a "bank" (e.g. a financial institution other than a credit institution in Europe or a depository institution in the United States).

Note-based system: an electronic money system in which the electronic funds are represented by records (electronic notes) that are uniquely identified by a serial number and are associated with a fixed, unchangeable denomination.

Off-balance-sheet transactions: financial transactions that are not reflected on the balance sheet of the financial institution conducting them. An example would be the purchase or sale of financial assets in futures markets.

Offline: in electronic money systems, a transaction in which no direct connection is made between the device(s) involved in the transaction and a centralised computer system for the purpose of authenticating or otherwise authorising the transaction before it is executed.

One-way hash function: a mathematical algorithm (hash algorithm) applied to a message to generate a number that is attached to the message and is used to verify the integrity of the data transmitted. The result of the application of
a hash function to a message is called a hash value.

Online: in electronic money systems, indicates that a direct connection is made to a centralised computer system for authorisation or validation before a transaction can be executed.

Open network: a telecommunications network to which access is not restricted.

Operating system: that part of the software of a computer system (including chips) that is closely tied to the hardware on which it runs and that performs basic input/output operations, computations, memory management, etc.

Payment system: a set of instruments, banking procedures and, typically, interbank funds transfer systems that facilitate the circulation of money.

PCMCIA card (Personal Computer Media Control Interface Adapter): a device that is attached externally to a PC and that can perform various functions such as memory storage and modem communications. PCMCIA cards can be designed in such a way as to provide a certain level of tamper-resistance.

Personalisation: the phase of the IC card manufacturing process during which customer information is loaded into the card.

PIN (Personal Identification Number): a sequence of digits used to verify the identity of a device holder.

Plaintext: data which are not encrypted and are therefore in a readable form.

Prepaid card: a card on which is stored a record of funds available to the holder. Also used to refer to a card that provides its holder with access to a limited range of services (e.g. a telephone card) or goods which have been prepaid, even though the card itself does not store a record of funds.

Privacy: in the context of a payment system, the fact that no information which might permit determination of behaviour may be collected without the consent of the individual to whom it relates.

Protocol: procedures for the interchange of electronic messages between communicating devices.

Public key cryptography: see asymmetric cryptography.

RAM (Random-Access Memory): the volatile memory area of a chip that is used for calculations and can only store data when electrical current is being supplied.

Remote payment: a payment carried out through the sending of payment orders or payment instruments (e.g. by mail) from a remote location.

Repudiation: the denial by one of the parties to a transaction of participation in all or part of that transaction or of the content of the communication.

Retail funds transfer system: a funds transfer system which handles a large volume of payments of relatively low value in such forms as cheques, credit transfers, direct debits, withdrawals at automated teller machines and electronic fund transfers at points of sale.

Retail payments: this term describes all payments which are not included in the definition of large-value payments. Retail payments are mainly consumer payments of relatively low value and urgency.

Reverse-engineering: the process of analysing software code in order to determine how the software works.

ROM (Read-Only Memory): typically the area of a chip that holds the operating system and possibly parts of the application.

RSA (Rivest, Shamir, Adleman): a commonly used asymmetric cryptographic algorithm.

SAM (Security Application Module): a tamper-resistant computer component typically integrated into a terminal.

Scattering: the process of mixing the IC chip components so that they cannot be analysed easily.

Secret key cryptography: see symmetric cryptography.

Seigniorage: In a historical context the term seigniorage was used to refer to the share, fee or tax which the seignior, or sovereign, took to cover the expenses of coinage and for profit. With the introduction of paper money, larger profits could be made because banknotes cost much less to produce than their face value. When central banks came to be monopoly suppliers of banknotes, seigniorage came to be reflected in the profits made by them and ultimately remitted to their major or only shareholder, the government. Seigniorage can be estimated by multiplying notes and coin outstanding (non-interest-bearing central bank liabilities) by the long-term rate of interest on government securities (a proxy for the return on central bank assets).

Sequence number: a number attributed sequentially to a message and attached to it to prevent the duplication or loss of messages.

Server: a computer that provides services through a network to other computers.

Session key: a cryptographic key which is used for a limited time, such as a single communication session or transaction, then discarded.

Settlement system: a system used to facilitate the settlement of transfers of funds.

Smart card: an integrated circuit card with a microprocessor, capable of performing calculations.

Stored-value card: a prepaid card in which the record of funds can be increased as well as decreased. Also called an electronic purse.

Symmetric cryptography: a set of cryptographic techniques in which devices share the same secret key in combination with algorithms. For encryption, the same key is used for encrypting and decrypting and the decrypting algorithm is the reverse function of the encrypting algorithm.

Systemic risk: the risk that the failure of one participant in a transfer system, or in financial markets generally, to meet its required obligations will cause other participants or financial institutions to be unable to meet their obligations (including settlement obligations in a transfer system) when due. Such a failure could cause significant liquidity or credit problems and, as a result, might threaten the stability of financial markets (with subsequent effects on the level of economic activity).

Tamper-evident: the capacity of devices to show evidence of physical attack.

Tamper-proof: the proven capacity of devices to resist all attacks.

Tamper-resistant: the capacity of devices to resist physical attack up to a certain point.

TCP/IP (Transmission Control Protocol/Internet Protocol): a set of commonly used communications and addressing protocols; TCP/IP is the de facto set of communications standards of the Internet.

Time-stamp: a value inserted in a message to indicate the time at which the message was created.

Traceability: in electronic money systems, the degree to which value-transfer transactions can be traced to the originator(s) or the recipient(s) of the transfer.

Transaction log: a sequential record of transactions that is stored on a device.

Transferability: in electronic money systems, the degree to which an electronic balance can be transferred between devices without interaction with a central authority.

White list: in a card-based system, a database containing the list of all authorised card numbers.

APPENDIX II

THE INTERNET

INTRODUCTIÓN

The purpose of this annex is to provide an understanding of the Internet and an overview of Internet payment schemes in existence and under

development. The Internet is constantly evolving, however, and any description will soon become outdated*.

OPERATION OF THE NETWORK

The Internet is a data infrastructure that connects computers via telecommunication networks. It originated in the 1960s and 1970s, when the United States Department of Defense Advanced Research Projects Agency (ARPA) funded a small group of computer programmers and electronic engineers to redesign the way computers were operated. This resulted in the creation of ARPANET, the first network of computers. Internet, the successor to ARPANET, was sponsored in the 1980s by the National Science Foundation and included tens of thousands of researchers and scholars in private industry and universities, connected to the network through their institutions' computer centres. It is estimated that by July 1995 the Internet consisted of 120,000 host computers, connecting 40,000,000 users through 70,000 networks.

Protocols and addresses

TCP (Transmission Control Protocol) and *IP* (Internet Protocol) can be considered the building blocks of the Internet. TCP and IP are communication protocols that control communication

* The source on which this annex is based is Security of Electronic Money, Report by the Committee on Payment and Settlement Systems and Group of Computer Experts of the Central Banks of the Group of 10 Countries (Basle, August, 1996).

between all connected computers. The protocols are designed to establish links between all types of computer and network. The information elements (called "packets") sent over the network usually contain the addresses of the receiver and the sender. A large set of data can be split into several packets, which might follow different communication routes over the Internet and be reconstituted by the receiving machine.

Computers on the Internet each have a unique address. The physical addresses are linked to logical names in a "name server", analogous to a telephone book. Addresses are issued by the Internet Assigned Numbers Authority *(IAN*A) under contract to the National Science Foundation. Currently the Information Sciences Institute of the University of Southern California is the executing office of IANA. Administrative tasks such as the issuing of addresses are delegated to Delegated Registries for certain domains or geographical areas.

The composition of the names used on the Internet illustrates the types of domain. The last part of the name is called the Top Level Domain Name *(TL*D). The TLD consists of two characters representing a country (using country codes conforming to ISO standard 3166) or three characters representing a certain domain ("com" for commercial, "gov" for the US Government, "edu" for educational institutions, "net" for Internet providers, etc.).

INTERNET PAYMENT SCHEMES AND THEIR PROVIDERS

As a result of the large number of initiatives to develop payment mechanisms for the Internet, it would be impossible to describe the Internet payment schemes and their providers in detail. In general, the following types of payment scheme are available or under development:

- credit card orders transmitted by electronic mail without encryption;
- the use of encryption software for credit card orders;

- an electronic "cheque" system, software that permits users to create what are intended to be electronic equivalents of paper cheques that can be transmitted to retailers over the Internet and result in funds being transferred through the traditional clearing infrastructure from an existing bank account;
- electronic "notes", which are issued in exchange for prepayment by customers and are often promoted as a means of making very small-value payments; and,
- home-banking services, in which the Internet is used as the transport network for payment orders and for the retrieval of sensitive customer information.

There are a number of different types of payment scheme provider on the Internet. Some banks and other financial institutions offer home-banking or payment facilities to their customers. In addition to home banking, banks can also offer more innovative payment systems such as those using electronic "notes", although such developments are not widespread to date. Some groups of retailers offer Internet shopping "malls" and payment facilities to their members. Consumers who register as a user or a member are able to pay for the products offered by the merchant members. Other payment system operators offer diverse schemes. Services range from encryption of credit card numbers to provision of an Internet interface for home-banking software. Third-party processing agencies provide facilities for payments using existing credit cards or bank accounts.

A number of universities and research laboratories have developed their own Internet payment schemes. Some of these have been developed for research purposes only; others are being tested in small pilot schemes. Often a major sponsor from the banking, payment or retail industry will be involved in such pilot schemes. Several industry consortia, including financial and non-financial organisations, are developing payment schemes for the Internet. Some aim to carry out pilot programmes of their systems in 1996.

INTERNET SECURITY

Security of protocols and servers

The TCP/IP protocol, which is the core component of the Internet, has been designed to provide a high level of resiliency with a minimum level of overhead network information in the messages. As a result the TCP/IP protocol does not provide for a high level of security. The following

measures have been aimed at providing additional security: (1) the development of an additional protocol (Netscape Secure Socket Layer) to establish encryption between Internet client and Internet server; (2) the development of an extension of the http language (**s-http**, secure http), which establishes a protocol by which an Internet client and an Internet server can negotiate the appropriate level of security before exchanging information; (3) an initiative by the IETF to extend the TCP/IP protocol to allow certain security functions.

Normally, servers on the Internet, also called "hosts", use a Unix operating system. As a result of the security design of Unix (in which a superuser has considerable control to perform specific read and write operations) and the fact that it is impossible to control all the existing superusers of the Internet servers, it must be assumed that communications on the Internet can be overheard, deleted and possibly altered.

Disclosure of information

It is fairly easy for certain experienced computer users ("hackers") connected to the network to intercept and read the flow of information involving other computers. Sophisticated software can be built to reside in the background of the application or operating system without the knowledge of the user. This software can be designed to intercept sensitive information such as passwords, PINs or credit card numbers, and send it automatically to a predetermined location on the Internet. Therefore, software transmitted over the Internet must be certified or checked to ensure that no unauthorised programs (known as "viruses") are present.

Unauthorised access

One of the major threats arising from the security limitations of the Unix-based operating systems on the Internet is unauthorised access to internal systems. Attempts at gaining such unauthorised access can be carried out by using stolen passwords, by impersonating a trusted user ("spoofing"), or by launching an attack from a host that is trusted by others. Software is readily available to analyse a specific network and to locate any security breaches. This software can, of course, also be used by hackers who may wish to attack a network. As a protection measure, all the communication between a computer (or an internal network of computers) and the Internet should be predefined and controlled. Such security measures are called *firewalls*.

Unavailability, unreliability and denial of service

There is no guarantee of service availability and continuity on the Internet. It cannot be assumed that messages will arrive at their destination without delay or corruption. It must be assumed that it is possible to overload a server with traffic in order to create a denial-of-service situation.

Security evaluation

Both protocols (TCP/IP) and components (mainly Unix-based servers) of the Internet have security limitations that make the Internet, by itself, an unsafe environment. It is therefore the responsibility of its users and product suppliers to ensure secure transfer of information or payment transactions over the Internet. Public key cryptography and digital signatures are the key technologies which provide for privacy and authentication. In fact, the use of these technologies (provided that keys are stored in a tamper-resistant manner) can be viewed tantamount to creating private networks over the public network.

APPENDIX III

SMART CARD SECURITY

INTRODUCTION

Currently, most payment cards still use a magnetic stripe to store consumer-related information. In the future, however, it is expected that extensive use will be made of integrated circuit (IC) cards for consumer payment systems, such as debit cards, credit cards and electronic purse systems. This annex provides a description of IC cards, the production and personalisation process and their security features.

IC cards can be categorised as smart cards or memory cards. A smart card has data-processing and storage functionality, whereas a memory card is used only for data-storage purposes. The first operational IC card systems for consumers (telephone cards in France) made use of memory cards. Currently, most systems use smart cards because of the data-processing functionality needed for computing, particularly cryptographic, purposes. Smart cards can be either of the contact type, which must be inserted into a reader when used, or of the contactless type, which must contain its own power source and operates remotely from the reader/writer. This annex focuses on the contact smart card, the device used in many electronic purse or stored-value card projects*.

SMART CARDS

A typical smart card is a plastic card in which an IC chip is embedded and on which eight contacts are placed. The physical and electronic

* The source on which this annex is based is Security of Electronic Money, Report by the Committee on Payment and Settlement Systems and Group of Computer Experts of the Central Banks of the Group of 10 Countries (Basle, August, 1996).

specifications generally follow ISO and IEC standards.A typical smart card chip consists of the following components:

- **CPU** (Central Processing Unit), which performs computation;
- **ROM** (Read-Only Memory), which stores the operating system and applications;
- **EEPROM** (Electronically Erasable and Programmable ROM), which stores the variable data such as the balance of the purse, cardholder data, etc.;
- **RAM** (Random Access Memory), which is used as the work area when the chip is processing; and
- **I/O** (Input/Output), which takes place through designated contact fields.

The price of a smart card depends on its data-storage and processing functionality. Smart cards with limited memory (8 Kbytes) and built-in symmetric encryption processors are currently available at a relatively low price (approximately US$ 5 if produced in large quantities). Smart cards that can also perform asymmetric cryptography have, in the past, been considered much more expensive and technically less reliable. In the course of 1996, a new generation of more reliable IC chips that contain a coprocessor to compute asymmetric cryptography are expected to become available at reasonable prices.

THE PRE-OPERATIONAL STAGES OF THE IC CARD LIFE CYCLE

The development and the production of IC cards is a very complex process, consisting of roughly the following phases: design, manufacturing and initialisation of the chip module; embedding of the chip module in the card; and personalisation. Many controls and measures are implemented to

Ensure that no single entity or person can obtain complete knowledge of the design of the chip, the cryptographic initialisation keys, or the initialisation or personalisation data. Separation of duties on a need-to-know basis is common during these early phases of the IC chip life cycle. This can be

achieved through cryptographic separation, physical separation, in which two or three employees are needed to produce or transport certain keys, or administrative measures, including internal controls.

Design and manufacture of the IC chip

The chips that are being used in smart cards are produced mainly by a few large manufacturers. The technical characteristics of chips from these manufacturers determine the constraints within which electronic money suppliers and others must design the functionality of their IC chips. It should be noted that the manufacturers do not provide their technical design to potential customers; rather, they provide only the set of commands that the chip operating system can execute.

Organisations can choose between designing their own proprietary application code in close collaboration with the manufacturer and buying a standardised application that has already been designed by the manufacturer. The application code must be extensively tested before being converted into a "mask", which is the hardware specification that defines the physical and functional properties of the IC chip.

The production of chips takes places in several steps. Chips are first produced on a silicon wafer; then the wafer is sawn into smaller parts. The chips are mounted on separate modules, encapsulated with coatings and then tested, after which the test pins that are used during this phase are physically disabled.

As a final step in the production process, the chip module is initialised. The EEPROM is programmed to contain the directory and file structure. In addition, the most important cryptographic keys are loaded during this phase in order to provide control over the subsequent phases.

Embedding the chip module in the card

The process by which the chip module is mounted on the plastic carrier is called embedding. The company that performs the embedding function does not have access to the secret cryptographic keys with which the chip is protected, and therefore cannot tamper with the contents of the chip.

Personalisation

During the personalisation phase, the application on the chip is uniquely identified and the chip is loaded with all necessary personal and non-personal data and secret cryptographic keys. This process is divided into several steps and can also be designed to be performed by separate companies. The issuing company is present during all steps in this process, to control and supply thenecessary keys.

The personalisation of the smart card takes place in such a way that the personalization company cannot read the user data. The user data are encrypted by a key that has been loaded by the card-issuing organisation during the initialisation phase. This encrypted information is then decrypted by the card itself using the same secret key and stored in the appropriate records and files on the card.

SECURITY MEASURES

The countermeasures that can be taken to protect IC cards relate to different threats and vulnerabilities, such as analysing its design optically or electronically, manufacturing a fraudulent IC card, or changing the content of the IC chip (for example by increasing the balance).

Measures to prevent optical and physical analysis

Code in ROM is invisible: In the past, the ROM code was implanted on a chip with transistors that could be easily read optically. With advanced technology, the code is now usually implanted using the density of impurities in the transistors, and is protected by special coatings in order to prevent optical analysis.

Layout of chip is scattered :In earlier designs, the components of an IC chip such as the CPU, ROM, EEPROM, RAM and I/O were clearly separated on a chip, which made it easier to isolate each component from the others and analyse them separately. It is difficult to do so with an advanced IC chip, because the important components are scattered across different areas of the chip.

Double metal layer of wiring :Chip wiring laid out in a single layer may be relatively straightforward to analyse. With current advanced technology, however, the wiring is distributed between two layers, which makes analysis more difficult. The inclusion of "dummy" wiring in some chips is also intended to deliberately mislead potential attackers.

Measures to prevent electrical analysis

Low-frequency detector: Electrical analysis of IC chips is done by measuring the voltage and current of the wiring when the chip is working at very low frequency. With the current technology the chip is designed in such a way that it will not operate at low frequencies.

Scattered ROM/EEPROM data: The data stored in the ROM and EEPROM in a chip are stored in different physical locations on the chip, so that an attacker who reads the contents of ROM and EEPROM faces the task of determining which bits belong together.

Disabled test pins. The test pins of the chip, through which the chip is tested during the manufacturing process, are physically disabled so that they cannot be used to gain access to the inside of the chip. This is also referred to as "blowing the fuses".

Use of sensitive wiring :The wiring of a chip is designed to operate at a certain voltage. If an attacker used a voltage above the prescribed levels to analyse the contents of the chip, the wiring would burn and the information on the chip could not be recovered.

Measures to prevent the manufacture of fraudulent IC chips Small-scale technology

The utilisation of small-scale chip technology requires an investment of hundreds of millions of dollars in specialised equipment and extremely specialized expertise in order to manufacture an IC chip.

Proprietary operating systems: All chip operating systems are proprietary. Chip manufacturers generally provide a limited set of commands that the operating system will accept. They do not provide the source code.

Custom-made masks: Chip manufacturers and card issuers work closely together to establish the source code that will perform the specific application on the chip. This code is integrated into the mask, which is used to physically produce the chips. The code is known only to the manufacturer and developers.

Layout and keys during initialization: The further layout of the data and the master cryptographic keys are established and loaded during the initialisation phase and are known only to the card issuer or other owner of the application on the chip.

Encrypted personalization: Personalisation takes place by encrypting the user data under a cryptographic personalisation key that is known only to the owner of the application. This key is installed in the chip during initialisation.

Administrative and procedural controls: Administrative and procedural controls help ensure that no one person will be able to obtain all the information needed to fraudulently create a card.

Measures to prevent alteration of the contents of an IC chip

Electrical protection of EEPROM: A special protection layer protects the contents of the EEPROM from UV (ultraviolet) rays, X-rays and electromagnetic modification.

Commands for changing the contents of EEPROM: Changing the contents of the EEPROM requires several consecutive commands. The contents of the EEPROM cannot be altered unless the attacker can provide all the necessary commands in the proper order.

Control registers: For some data records stored in the EEPROM, a "hash" value is calculated and stored on the card in a control register. Access to the data records may only be allowed if the recomputed hash value is the same as the value in the control register.

EVALUATION OF IC CARD SECURITY MEASURES

To date, there have been no published reports of security breaches of smart cards, although some instances of tampering with simpler memory cards are known. Tampering with a chip would entail overcoming many physical and cryptographic barriers. This does not mean that the current security measures will continue to be sufficient in the future. As new techniques for attacking chips are developed, the current security measures may become obsolete and new ones will have to be adopted. In addition to new physical security measures, systems utilising IC cards should be designed to allow the security of the IC card to be upgraded, for example by implementing new or redundant algorithms.

Although not discussed in detail here, it should be stressed that considerable care must be taken to implement administrative and procedural security measures effectively. In view of the robustness of the technical security features of smart cards, an attack on administrative security during the manufacturing, distribution or issuing process (such as stealing ready-to-distribute cards, etc.) may constitute a greater risk.

APPENDIX IV

CRYPTOGRAPHY

INTRODUCTION

The use of cryptography is a very important security measure in the design of payment systems and message protocols. Cryptography (literally: secret writing) can be viewed as the application of mathematical theories to realise a certain level of security or secrecy. The application of cryptographic theories and functions can help achieve objectives such as confidentiality, data integrity and authentication. This annex describes the building blocks of cryptography as well as their application within payment systems. It is intended to provide an overview of the most important cryptographic algorithms and tools.*

GENERAL PRINCIPLES AND BUILDING BLOCKS

In this section, the general principles and terminology of cryptography are introduced and an overview of the most important cryptographic concepts is provided. These include encryption and decryption, one-way hash functions, challenge-response protocols with random numbers, digital signatures and key management.

Encryption and Decryption

Confidentiality of data can be achieved by applying encryption or encipherment techniques. Senders and receivers of information can agree on a certain method of encryption and decryption to ensure that their message is not understandable to others. The encryption and decryption processes will

* The source on which this annex is based is Security of Electronic Money, Report by the Committee on Payment and Settlement Systems and Group of Computer Experts of the Central Banks of the Group of 10 Countries (Basle, August, 1996).

require a mathematical function called an algorithm as well as keys,which are used to parameterise the encryption or decryption algorithm.

Symmetric and asymmetric algorithms

An algorithm is called *symmetric* if it uses the same key as both the encryption key and the decryption key. The use of such an algorithm depends on the key being safely stored by the sending and receiving parties. Compromising the encryption key would allow outsiders to decrypt the message. The Data Encryption Standard (DES) is an example of a symmetric algorithm. DES was adopted by the US Federal Government in 1977 and was developed by IBM under contract to the National Bureau of Standards, now called National Institute of Standards and Technology (NIST).

Another class of algorithms, called *asymmetric* algorithms, does not use the same key for encryption and decryption, but makes use of a pair of different but mathematically related keys. One key is kept secret by the creator of the key pair (the private key) and the other key is made known to the correspondents of the key creator. A message encrypted with one key of the pair can only be decrypted by the other key of the pair. It is not possible to deduce one key from the other. Thus, a message encrypted by the sender with the receiver's public key can only be decrypted by the receiver using its private key. The Rivest-Shamir-Adleman (RSA) algorithm is an example of an asymmetric algorithm.

Asymmetric algorithms can also be used to provide authentication. If a message or part of a message is encrypted using the sender's private key and it can be decrypted using the sender's public key, the message can be authenticated, or assumed to have been sent by the sender. As asymmetric public keys can be held by many parties who may not know the holder of the private key, a *certification authority* is sometimes used to distribute public keys and to certify their relationship to the holder of the private key.

Generally, symmetric algorithms (such as DES) can be executed faster than asymmetric algorithms (such as RSA) because asymmetric algorithms require more processing time and resources.

As a result, prices for computer hardware that can perform DES calculations are lower than those for hardware that can also execute the RSA algorithm. Consequently, those suppliers implementing encryption algorithms on IC chips concentrated first on implementing DES, but are now moving towards implementing RSA calculations.

Strength of encryption

The most desirable review of security algorithms consists of a public review by as many cryptographic experts as possible in order to analyse and detect any weaknesses in the design of the encryption method. If an encryption algorithm has withstood this review (cryptanalysis) for a considerable time, one can be reasonably sure that it does not contain secret "trapdoors" or undetected weaknesses. The use of public and extensively reviewed algorithms is therefore an important security principle, and one that is often applied by suppliers of electronic money systems.

The strength of the encryption should not be based on the secrecy of the applied algorithm, but on the fact that the secret and private encryption and decryption keys are known only to the sender or receiver of the message. It is therefore very important to store these keys safely and to use encryption and decryption keys of sufficient length.

To assess the strength of encryption algorithms, it can be assumed that the algorithm and the ciphertext are known to an outsider. An outsider could try to discover the plaintext by testing all possible decryption keys. This type of attack is known as a *brute-force attack* or an *exhaustive key search*. The amount of processing resources needed to discover the correct decryption key through a brute-force attack for a given algorithm and a given key length can be calculated relatively easily.

A group of cryptographic experts recently concluded that technology currently available makes brute-force attacks against symmetric cryptographic systems with small key lengths both fast and cheap.To provide adequate protection against the most serious threats, such as well-funded commercial enterprises or government intelligence agencies, key lengths of at least 90 bits are recommended for newly deployed systems. It is estimated that this key length will be adequate for the next 20 years. As far as asymmetric cryptographic systems are concerned, similar estimates are available, indicating that key lengths of 512 bits should be replaced by longer keys (768, 1,024 or 2,048 bits).

It should be noted, however, that key length itself is not a guarantee of a safe system. The complete spectrum of security measures (organisational, procedural and technical measures) will determine the security of a given system. The necessary key length will depend critically on the context in which the information must be secured. It is, therefore, not appropriate to presume that a system that applies the RSA algorithm with a key length of 768 bits is safer than a system for which a key length of 512 bits has been chosen.

Furthermore, developments within cryptography are directed not only at new algorithms but also at cryptanalysis of algorithms, an area in which significant improvements can be expected in the years to come. In particular, progress with respect to so-called differential and linear cryptanalysis could force system designers to re-evaluate the key management schemes and to update the security of the systems.

One-way hash functions

A one-way hash function is a means by which a receiver of a message can verify that the message content has not been changed. The sender of the message uses the message text and the one-way hash function to generate a hash value. The receiver of the message repeats this action and compares the received hash value and the calculated hash value. If they are the same, it can be assumed that the message content has not been changed.

An essential characteristic of a one-way hash function is that it can only be computed in a single direction and cannot be reversed. Furthermore, it may not generate the same hash value for different messages. In order to limit the risk of generating the same hash value for different messages, an appropriate hash function and an appropriate length of the hash value (for example 128 bits) must be selected. Hash functions are also subject to public review by cryptographers and are treated in the same manner as encryption algorithms. Well-known hash functions include Message Digest 5 (MD-5) and the Secure Hash Algorithm (SHA).

Through the combination of a hash function with the use of cryptographic keys, only parties that possess the appropriate cryptographic key can be permitted to verify the hash value.

Challenge-response protocols

Challenge-response protocols are used to establish whether two entities involved in communication are indeed genuine entities and can thus be allowed to continue communication with each other. One entity would challenge the other with a random number on which a predetermined calculation must be performed, often including a secret or a private key. In order to be able to generate the correct result for the computation, the other device must possess the correct private key and therefore can be assumed to be authentic.

The use of random or unpredictable numbers presents an attacker with an extra barrier, because past challenge and response values are not useful. The attacker will not be able to fraudulently authenticate a device by replaying an earlier recorded response because every response depends on a random input.

Digital signatures

A digital signature is a string of data, cryptographically generated, which authenticates both the sender and the contents of the message. Public key algorithms can be applied to provide digital signatures. Digital signatures in an asymmetric cryptosystem typically consist of encrypting a message or part of a message with a private key. Any recipient having the corresponding public key will be able to decrypt the ciphertext. Because the ciphertext can only be created using the private key known only to the sender, the recipient will have proof authenticating the sender of the message.

One use of digital signatures would consist in both parties performing the above procedure, thereby preventing denial, or repudiation, of messages after the event by either party. Depending on the system design, it might also be appropriate to include the time and date in the message. It is also possible for information to be time-stamped and digitally signed by a third party, thus attesting that the document existed at the stated time.

Digital signatures are not necessarily based on the mathematical problem of factoring. Signature schemes can also be based on other mathematical principles, such as the discrete logarithm problem.

Key management

Payment systems employing symmetric cryptography that use a single system-wide cryptographic key for encryption, decryption and authentication purposes would be vulnerable to attackers, who would only have to discover the single key to manipulate any aspect of the system.

Designers of payment systems, therefore, abide by certain key-management practices that have been established in international standards on key management, such as ISO standards 10202, 11166 and 11568.

As a principle of sound key management, cryptographic keys are only used for one specific function. A load transaction is secured by a special load key, a purchase transaction is secured by a purchase key, a collect transaction is secured by a collect key, etc. Furthermore, keys are unique to a card or terminal, so that the compromising of a card or terminal key would contain the security breach primarily to this individual level. These card-specific keys are created by a process called *key derivatio*n. This process typically takes place during personalization of the card and can be applied to generate all the card-specific keys (card load key, card purchase key, etc.).

In order to calculate a card-specific load key, for example, an arithmetic function is typically used that combines the system master key for load transactions with the card-specific identification number, for example the IC's serial number. The resulting value is used as the card-specific load key, which is stored in the IC chip. Whenever this particular card performs an online load transaction, the issuing bank reads the serial number of the IC card and recalculates the card's load key. In that way, both sides of the communication channel share the same individual key during the load transaction.

In addition to the use of derived keys, *session keys* are used as unique keys for every communication session. Session keys are special types of derived key that are based on the card's unique purchase keys, in combination with the transaction number of the card. The transaction number is derived from the card's transaction counter, which automatically increases for each transaction performed during the life of the card. A terminal holding the appropriate cryptographic key that receives the card's transaction number can recalculate the session key and use that key during a purchase transaction. The existence of these keys is limited to one session or transaction. New transactions will result in session keys with different values. The interception or possession of a session key will therefore not benefit an attacker for future use.

CRYPTOGRAPHY IN PAYMENT SYSTEMS

Applying cryptography to implement a secure payment system requires not only decisions with respect to the type of algorithms used but considerations regarding key management and key storage as well. Although these subjects are described separately, they are highly interdependent.

Use of algorithms and functions

The cryptographic principles and building blocks described above are used to achieve security goals such as confidentiality, data integrity and authentication. *Confidentiality* is typically achieved by using DES as the encryption method. Although it can also be done by applying asymmetric algorithms, owing to performance and price considerations the symmetric algorithms are generally preferred.

DES is also referred to as single-DES, to distinguish it from triple-DES. Triple-DES encryption consists of three consecutive operations (encryption; decryption; encryption) in which two

DES keys are used (or a double-length DES key). Triple-DES has been developed in response to the increasing processing capabilities of computers and ensures that an exhaustive key search would still demand a considerable amount of resources.

Several governments have established strict rules with respect to the commercial use and, in some cases, export of encryption algorithms, whether hardware or software-based. The main goal of these rules is to prevent the availability of powerful bulk-encryption processing capabilities, as these could be used for criminal purposes. As a result of these rules, the implementation of encryption in payment systems is often restricted to financial data only.

Data *integrity* and *authentication* (including non-repudiation) are achieved by using DES, triple-DES and public key algorithms such as RSA, and by applying well-known hashing and MAC algorithms, such as MD-5, SHA-1 and RSA.

Safe storage of secret keys

In addition to choosing appropriate cryptographic algorithms, payment system designers must ensure that secret and private cryptographic keys are stored safely and that tampering or eavesdropping will be detected or will result in the destruction of the remaining data. In practice, these keys are stored in security modules in host computers, payment terminals and payment modules, and on the IC chip.

Key management

Experience with key management is common amongst many payment system designers and operators as a result of their experience in executing and designing key management for point-of-sale environments. The relevance of sound key-management principles lies in the creation of extra barriers to attackers. For example, periodic changes of security keys (or different generations of keys) limit the usefulness of particular keys that an attacker might derive from an exhaustive key search.

SECURITY ASSESSMENT

It can be stated that, in theory, cryptography allows payment systems to be designed in a safe, secure and fleckless way. In order to breach the security of those systems, an attacker would need to steal the keys, to try all combinations of possible keys in sequence, or to apply the results of cryptanalysis using the discovered weaknesses or characteristics of the algorithms to break the algorithm. Depending on the key size used, the amount of time needed to succeed in such an attack can be calculated.

In symmetric cryptosystems, it would take a substantial effort to break a system with 56 bit keys such as DES, but this can be accomplished quite easily with special hardware. The cost of the special hardware is not insignificant, but is certainly not beyond the means of organised criminals, major companies and governments. Keys with 64 bits can probably be broken by major governments, and will be within the reach of organised criminals, major companies and other governments within a few years. Keys with 80 bits may become vulnerable in the near future. Keys with 128 bits will probably remain resistant to brute-force attacks for the foreseeable future.

The key lengths used in asymmetric cryptography are usually much longer than those used in symmetric ciphers. With asymmetric algorithms, the problem is not to determine the correct key, but to derive the matching secret key from the public key. In the case of RSA, this is equivalent to factoring a large integer that has two large prime factors. In the case of some other cryptosystems, the problem is equivalent to computing the discrete logarithm modulo for a large integer (which is believed to be roughly comparable to factoring). Other cryptosystems are based on yet other techniques.

For an RSA cryptosystem, a 256 bit modulus is easily factored by a computer user with average experience and resources. Keys with 384 bits can be broken by university research groups or companies; 512 bit keys are within the reach of major governments. Keys with 768 bits are probably not secure in the long term. Keys with 1,024 bits and more should be secure for a number of years unless major algorithmic advances are made in factoring; keys of 2,048 bits are considered by many to be secure for decades.

In practice, cost considerations will lead to design decisions with respect to the choice and application of certain cryptographic safeguards. These design decisions are not aimed at achieving the highest theoretical level of security, but at providing a level of security such that the cost of attacking a system will substantially exceed the possible financial gain to an attacker. The Task Force has not observed essentially different opinions among suppliers on issues such as the weaknesses and- 64 –strengths of particular algorithms, necessary key lengths for symmetric and asymmetric algorithms, and the best key-management practices.

Although from a theoretical as well as a practical point of view it is possible to design sufficiently safe payment systems, it is critical to evaluate the actual execution of the security measures, in addition to the design of the systems. Such evaluations must take place periodically, as advances in cryptanalysis might expose weaknesses in the applied algorithms over time. Furthermore, it must be stressed that not only technical and cryptographic issues are a concern in these evaluations. The organisational and procedural design choices and execution of procedures must also be considered.

APPENDIX V

UNCITRAL MODEL LAW ON INTERNATIONAL CREDIT TRANSFERS

UNITED NATIONS 1994

CONTENTS

UNCITRAL Model Law on International Credit Transfers

CHAPTER I. GENERAL PROVISIONS[1]

Article 1. Sphere of application[2]

(1) This law applies to credit transfers where any sending bank and its receiving bank are in different States.

(2) This law applies to other entities that as an ordinary part of their business engage in executing payment orders in the same manner as it applies to banks.

(3) For the purpose of determining the sphere of application of this law, branches and separate offices of a bank in different States are separate banks.

Article 2. Definitions

For the purposes of this law:

(a) "Credit "means the series of operations, beginning with the originator's payment order, made for the purpose of placing funds at the disposal of a beneficiary. The term includes any payment order issued by the originator's bank or any intermediary bank intended to carry out the originator's payment order. A payment order issued for the purpose of effecting payment for such an order is considered to be part of a different credit ;

(b) "Payment order" means an unconditional instruction, in any form, by a sender to a receiving bank to place at the disposal of a beneficiary a fixed or determinable amount of money if

(i) the receiving bank is to be reimbursed by debiting an account of, or otherwise receiving payment from, the sender, and

(ii) the instruction does not provide that payment is to be made at the request of the beneficiary.

Nothing in this paragraph prevents an instruction from being a payment order merely because it directs the beneficiary's bank to hold, until the beneficiary requests payment, funds for a beneficiary that does not maintain an account with it;

(c) "Originator" means the issuer of the first payment order in a credit ;

(d) "Beneficiary" means the person designated in the originator's payment order to receive funds as a result of the credit;

(e) "Sender" means the person who issues a payment order, including the originator and any sending bank;

(f) "Receiving bank"means a bank that receives a payment order;

(g) "Intermediary bank" means any receiving bank other than the originator's bank and the beneficiary's bank;

(h) "Funds" or "money" includes credit in an account kept by a bank and includes credit denominated in a monetary unit of account that is established by an intergovernmental institution or by agreement of two or more States, provided that this law shall apply without prejudice to the rules of the intergovernmental institution or the stipulations of the agreement;

(i) "Authentication" means a procedure established by agreement to determine whether a payment order or an amendment or revocation of a payment order was issued by the person indicated as the sender;

(j) "Banking day" means that part of a day during which the bank performs the type of action in question;

(k) "Execution period" means the period of one or two days beginning on the first day that a payment order may be executed under article 11(1) and ending on the last day on which it may be executed under that article;

(l) "Execution", in so far as it applies to a receiving bank other than the beneficiary's bank, means the issue of a payment order intended to carry out the payment order received by the receiving bank;

(m) "Interest" means the time value of the funds or money involved, which, unless otherwise agreed, is calculated at the rate and on the basis customarily accepted by the banking community for the funds or money involved.

Article 3. Conditional instructions

(1) When an instruction is not a payment order because it is subject to a condition but a bank that has received the instruction executes it by issuing an unconditional payment order, thereafter the sender of the instruction has the same rights and obligations under this law as the sender of a payment order and the beneficiary designated in the instruction shall be treated as the beneficiary of a payment order.

(2) This law does not govern the time of execution of a conditional instruction received by a bank, nor does it affect any right or obligation of the sender of a conditional instruction that depends on whether the condition has been satisfied.

Article 4. Variation by agreement

Except as otherwise provided in this law, the rights and obligations of parties to a credit may be varied by their agreement.

CHAPTER II. OBLIGATIONS OF THE PARTIES

Article 5. Obligations of sender

(1) A sender is bound by a payment order or an amendment or revocation of a payment order if it was issued by the sender or by another person who had the authority to bind the sender.

(2) When a payment order or an amendment or revocation of a payment order is subject to authentication other than by means of a mere comparison of signature, a purported sender who is not bound under paragraph (1) is nevertheless bound if

(a) the authentication is in the circumstances a commercially reasonable method of security against unauthorized payment orders, and

(b) the receiving bank complied with the authentication.

(3) The parties are not permitted to agree that a purported sender is bound under paragraph (2) if the authentication is not commercially reasonable in the circumstances.

(4) A purported sender is, however, not bound under paragraph (2) if it proves that the payment order as received by the receiving bank resulted from the actions of a person other than

a) a present or former employee of the purported sender, or
b) a person whose relationship with the purported sender enabled that person to gain access to the authentication procedure.

The preceding sentence does not apply if the receiving bank proves that the payment order resulted from the actions of a person who had gained access to the authentication procedure through the fault of the purported sender.

(5) A sender who is bound by a payment order is bound by the terms of the order as received by the receiving bank. However, the sender is not bound by an erroneous duplicate of, or an error or discrepancy in, a payment order if

(a) the sender and the receiving bank have agreed upon a procedure for detecting erroneous duplicates, errors or discrepancies in a payment order, and

(b) use of the procedure by the receiving bank revealed or would have revealed the erroneous duplicate, error or discrepancy.

If the error or discrepancy that the bank would have detected was that the sender instructed payment of an amount greater than the amount intended by the sender, the sender is bound only to the extent of the amount that was intended. Paragraph (5) applies to an error or discrepancy in an amendment or a revocation order as it applies to an error or discrepancy in a payment order.

(6) A sender becomes obligated to pay the receiving bank for the payment order when the receiving bank accepts it, but payment is not due until the beginning of the execution period.

Article 6. Payment to receiving bank

For the purposes of this law, payment of the sender's obligation under article 5(6) to pay the receiving bank occurs

(a) if the receiving bank debits an account of the sender with the receiving bank, when the debit is made; or

(b) if the sender is a bank and subparagraph (a) does not apply,

(i) when a credit that the sender causes to be entered to an account of the receiving bank with the sender is used or, if not used, on the banking day following the day on which the credit is available for use and the receiving bank learns of that fact, or

(ii) when a credit that the sender causes to be entered to an account of the receiving bank in another bank is used or, if not used, on the banking day following the day on which the credit is available for use and the receiving bank learns of that fact, or

(iii) when final settlement is made in favour of the receiving bank at a central bank at which the receiving bank maintains an account, or

(iv) when final settlement is made in favour of the receiving bank in accordance with

a.provides for the settlement of obligations among participants either bilaterally or the rules of a funds system that multilaterally, or

b. a bilateral netting agreement with the sender; or

(c) if neither subparagraph (a) nor (b) applies, as otherwise provided by law.

Article 7. Acceptance or rejection of a payment order by receiving bank other than the beneficiary's bank

1) The provisions of this article apply to a receiving bank other than the beneficiary's bank.
2) A receiving bank accepts the sender's payment order at the earliest of the following times:
   a) when the bank receives the payment order, provided that the sender and the bank have agreed that the bank will execute payment orders from the sender upon receipt;
   b) when the bank gives notice to the sender of acceptance;
   c) when the bank issues a payment order intended to carry out the payment order received;

d) when the bank debits an account of the sender with the bank as payment for the payment order; or

e) when the time for giving notice of rejection under paragraph (3) has elapsed without notice having been given.

(3) A receiving bank that does not accept a payment order is required to give notice of rejection no later than on the banking day following the end of the execution period, unless:

(a) where payment is to be made by debiting an account of the sender with the receiving bank, there are insufficient funds available in the account to pay for the payment order;

(b) where payment is to be made by other means, payment has not been made; or

(c) there is insufficient information to identify the sender.

(4) A payment order ceases to have effect if it is neither accepted nor rejected under this article before the close of business on the fifth banking day following the end of the execution period.

Article 8. Obligations of receiving bank other than the beneficiary's bank

(1) The provisions of this article apply to a receiving bank other than the beneficiary's bank.

(2) A receiving bank that accepts a payment order is obligated under that payment order to issue a payment order, within the time required by article 11, either to the beneficiary's bank or to an intermediary bank, that is consistent with the contents of the payment order received by the receiving bank and that contains the instructions necessary to implement the credit in an appropriate manner.

(3) A receiving bank that determines that it is not feasible to follow an instruction of the sender specifying an intermediary bank or funds system to be used in carrying out the credit , or that following such an instruction would cause excessive costs or delay in completing the credit , shall be taken to have complied with paragraph (2) if, before the end of the execution period, it inquires of the sender what further actions it should take.

(4) When an instruction is received that appears to be intended to be a payment order but does not contain sufficient data to be a payment order, or being a payment order it cannot be executed because of insufficient data, but the sender can be identified, the receiving bank shall give notice to the sender of the insufficiency, within the time required by article 11.

(5) When a receiving bank detects that there is an inconsistency in the information relating to the amount of money to be transferred, it shall, within the time required by article 11, give notice to the sender of the inconsistency, if the sender can be identified.

Any interest payable under article 17(4) for failing to give the notice required by this paragraph shall be deducted from any interest payable under article 17(1) for failing to comply with paragraph (2) of this article.

(6) For the purposes of this article, branches and separate offices of a bank, even if located in the same State, are separate banks.

Article 9. Acceptance or rejection of a payment order by beneficiary's bank

(1) The beneficiary's bank accepts a payment order at the earliest of the following times:

(a) when the bank receives the payment order, provided that the sender and the bank have agreed that the bank will execute payment orders from the sender upon receipt;

(b) when the bank gives notice to the sender of acceptance;

(c) when the bank debits an account of the sender with the bank as payment for the payment order;

(d) when the bank credits the beneficiary's account or otherwise places the funds at the disposal of the beneficiary;

(e) when the bank gives notice to the beneficiary that it has the right to withdraw the funds or use the credit;

(f) when the bank otherwise applies the credit as instructed in the payment order;

(g) when the bank applies the credit to a debt of the beneficiary owed to it or applies it in conformity with an order of a court or other competent authority; or

(h) when the time for giving notice of rejection under paragraph (2) has elapsed without notice having been given.

(2) A beneficiary's bank that does not accept a payment order is required to give notice of rejection no later than on the banking day following the end of the execution period, unless:

(a) where payment is to be made by debiting an account of the sender with the beneficiary's bank, there are insufficient funds available in the account to pay for the payment order;

(b) where payment is to be made by other means, payment has not been made; or

(c) there is insufficient information to identify the sender.

(3) A payment order ceases to have effect if it is neither accepted nor rejected under this article before the close of business on the fifth banking day following the end of the execution period.

Article 10. Obligations of beneficiary's bank

(1) The beneficiary's bank is, upon acceptance of a payment order, obligated to place the funds at the disposal of the beneficiary, or otherwise to apply the credit, in accordance with the payment order and the law governing the relationship between the bank and the beneficiary.

(2) When an instruction is received that appears to be intended to be a payment order but does not contain sufficient data to be a payment order, or being a payment order it cannot be executed because of insufficient data, but the sender can be identified, the beneficiary's bank shall give notice to the sender of the insufficiency, within the time required by article 11.

(3) When the beneficiary's bank detects that there is an inconsistency in the information relating to the amount of money to be transferred, it shall, within the time required by article 11, give notice to the sender of the inconsistency if the sender can be identified.

(4) When the beneficiary's bank detects that there is an inconsistency in the information intended to identify the beneficiary, it shall, within the time required by article 11, give notice to the sender of the inconsistency if the sender can be identified.

(5) Unless the payment order states otherwise, the beneficiary's bank shall, within the time required for execution under article 11, give notice to a beneficiary who does not maintain an account at the bank that it is holding funds for its benefit, if the bank has sufficient information to give such notice.

Article 11. Time for receiving bank to execute payment order and give notices

(1) In principle, a receiving bank that is obligated to execute a payment order is obligated to do so on the banking day it is received. If it does not, it shall do so on the banking day after the order is received. Nevertheless, if

(a) a later date is specified in the payment order, the payment order shall be executed on that date, or

(b) the payment order specifies a date when the funds are to be placed at the disposal of the beneficiary and that date indicates that later execution is appropriate in order for the beneficiary's bank to accept a payment order and execute it on that date, the order shall be executed on that date.

(2) If the receiving bank executes the payment order on the banking day after it is received, except when complying with subparagraph (a) or (b) of paragraph (1), the receiving bank must execute for value as of the day of receipt.

(3) A receiving bank that becomes obligated to execute a payment order by virtue of accepting a payment order under article 7(2)(e) must execute for value as of the later of the day on which the payment order is received and the day on which

(a) where payment is to be made by debiting an account of the sender with the receiving bank, there are sufficient funds available in the account to pay for the payment order, or

(b) where payment is to be made by other means, payment has been made.

(4) A notice required to be given under article 8(4) or (5) or article 10(2), (3) or (4) shall be given on or before the banking day following the end of the execution period.

(5) A receiving bank that receives a payment order after the receiving bank's cut-off time for that type of payment order is entitled to treat the order as having been received on the next day the bank executes that type of payment order.

(6) If a receiving bank is required to perform an action on a day when it does not perform that type of action, it must perform the required action on the next day it performs that type of action.

(7) For the purposes of this article, branches and separate offices of a bank, even if located in the same State, are separate banks.

Article 12. Revocation

(1) A payment order may not be revoked by the sender unless the revocation order is received by a receiving bank other than the beneficiary's bank at a time and in a manner sufficient to afford the receiving bank a reasonable opportunity to act before the later of the actual time of execution and the beginning of the day on which the payment order ought to have been executed under subparagraph (a) or (b) of article 11(1).

(2) A payment order may not be revoked by the sender unless the revocation order is received by the beneficiary's bank at a time and in a manner sufficient to afford the bank a reasonable opportunity to act before the later of the time the credit is completed and the beginning of the day when the funds are to be placed at the disposal of the beneficiary.

(3) Notwithstanding the provisions of paragraphs (1) and (2), the sender and the receiving bank may agree that payment orders issued by the sender to the receiving bank are to be irrevocable or that a revocation order is effective only if it is received earlier than the time specified in paragraph (1) or (2).

(4) A revocation order must be authenticated.

(5) A receiving bank other than the beneficiary's bank that executes, or a beneficiary's bank that accepts, a payment order in respect of which an effective revocation order has been or is subsequently received is not entitled to payment for that payment order. If the credit is completed, the bank shall refund any payment received by it.

(6) If the recipient of a refund is not the originator of the credit, it shall pass on the refund to its sender.

(7) A bank that is obligated to make a refund to its sender is discharged from that obligation to the extent that it makes the refund direct to a prior sender. Any bank subsequent to that prior sender is discharged to the same extent.

(8) An originator entitled to a refund under this article may recover from any bank obligated to make a refund hereunder to the extent that the bank has not previously refunded. A bank that is obligated to make a refund is discharged from that obligation to the extent that it makes the refund direct to the originator. Any other bank that is obligated is discharged to the same extent.

(9) Paragraphs (7) and (8) do not apply to a bank if they would affect the bank's rights or obligations under any agreement or any rule of a funds system.

(10) If the credit is completed but a receiving bank executes a payment order in respect of which an effective revocation order has been or is subsequently received, the receiving bank has such rights to recover from the beneficiary the amount of the credit as may otherwise be provided by law.

(11) The death, insolvency, bankruptcy or incapacity of either the sender or the originator does not of itself operate to revoke a payment order or terminate the authority of the sender.

(12) The principles contained in this article apply to an amendment of a payment order.

(13) For the purposes of this article, branches and separate offices of a bank, even if located in the same State, are separate banks.

CHAPTER III. CONSEQUENCES OF FAILED, ERRONEOUS OR DELAYED CREDIT TRANSFERS

Article 13. Assistance

Until the credit is completed, each receiving bank is requested to assist the originator and each subsequent sending bank, and to seek the assistance of the next receiving bank, in completing the banking procedures of the credit .

Article 14. Refund

(1) If the credit is not completed, the originator's bank is obligated to refund to the originator any payment received from it, with interest from the day of payment to the day of refund. The originator's bank and each subsequent receiving bank is entitled to the return of any funds it has paid to its receiving bank, with interest from the day of payment to the day of refund.

(2) The provisions of paragraph (1) may not be varied by agreement except when a prudent originator's bank would not have otherwise accepted a particular payment order because of a significant risk involved in the credit .

(3) A receiving bank is not required to make a refund under paragraph (1) if it is unable to obtain a refund because an intermediary bank through which it was directed to effect the credit has suspended payment or is prevented by law from making the refund. A receiving bank is not considered to have been directed to use the intermediary bank unless the receiving bank proves that it does not systematically seek such directions in similar cases. The sender that first specified the use of that intermediary bank has the right to obtain the refund from the intermediary bank.

(4) A bank that is obligated to make a refund to its sender is discharged from that obligation to the extent that it makes the refund direct to a prior sender. Any bank subsequent to that prior sender is discharged to the same extent.

(5) An originator entitled to a refund under this article may recover from any bank obligated to make a refund hereunder to the extent that the bank has not previously refunded. A bank that is obligated to make a refund is discharged from that obligation to the extent that it makes the refund direct to the originator. Any other bank that is obligated is discharged to the same extent.

(6) Paragraphs (4) and (5) do not apply to a bank if they would affect the bank's rights or obligations under any agreement or any rule of a funds system.

Article 15. Correction of underpayment

If the amount of the payment order executed by a receiving bank is less than the amount of the payment order it accepted, other than as a result of the deduction of its charges, it is obligated to issue a payment order for the difference.

Article 16. Restitution of overpayment

If the credit is completed, but the amount of the payment order executed by a receiving bank is greater than the amount of the payment order it accepted, it has such rights to recover the difference from the beneficiary as may otherwise be provided by law.

Article 17. Liability for interest

(1) A receiving bank that does not comply with its obligations under article 8(2) is liable to the beneficiary if the credit is completed. The liability of the receiving bank is to pay interest on the amount of the payment order for the period of delay caused by the receiving bank's non-compliance. If the delay concerns only part of the amount of the payment order, the liability shall be to pay interest on the amount that has been delayed.

(2) The liability of a receiving bank under paragraph (1) may be discharged by payment to its receiving bank or by direct payment to the beneficiary. If a receiving bank receives such payment but is not the beneficiary, the receiving bank shall pass on the benefit of the interest to the next receiving bank or, if it is the beneficiary's bank, to the beneficiary.

(3) An originator may recover the interest the beneficiary would have been entitled to, but did not, receive in accordance with paragraphs (1) and (2) to the extent the originator has paid interest to the beneficiary on account of a delay in the completion of the credit . The originator's bank and each subsequent receiving bank that is not the bank liable under paragraph (1) may recover interest paid to its sender from its receiving bank or from the bank liable under paragraph (1).

(4) A receiving bank that does not give a notice required under article 8(4) or (5) shall pay interest to the sender on any payment that it has received from the sender under article 5(6) for the period during which it retains the payment.

(5) A beneficiary's bank that does not give a notice required under article 10(2), (3) or (4) shall pay interest to the sender on any payment that it has received from the sender under article 5(6), from the day of payment until the day that it provides the required notice.

(6) The beneficiary's bank is liable to the beneficiary to the extent provided by the law governing the relationship between the beneficiary and the bank for its failure to perform one of the obligations under article 10(1) or(5).

(7) The provisions of this article may be varied by agreement to the extent that the liability of one bank to another bank is increased or reduced. Such an agreement to reduce liability may be contained in a bank's standard terms of dealing. A bank may agree to increase its liability to an originator or beneficiary that is not a bank, but may not reduce its liability to such an originator or beneficiary. In particular, it may not reduce its liability by an agreement fixing the rate of interest.

Article 18. Exclusivity of remedies

The remedies in article 17 shall be exclusive, and no other remedy arising out of other doctrines of law shall be available in respect of non-compliance with articles 8 or 10, except any remedy that may exist when a bank has improperly executed, or failed to execute, a payment order (a) with the specific intent to cause loss, or (b) recklessly and with actual knowledge that loss would be likely to result.

CHAPTER IV. COMPLETION OF CREDIT

Article 19. Completion of credit

(1) A credit is completed when the beneficiary's bank accepts a payment order for the benefit of the beneficiary. When the credit is completed, the beneficiary's bank becomes indebted to the beneficiary to the extent of the payment order accepted by it. Completion does not otherwise affect the relationship between the beneficiary and the beneficiary's bank.

(2) A credit is completed notwithstanding that the amount of the payment order accepted by the beneficiary's bank is less than the amount of the originator's payment order because one or more receiving banks have deducted charges. The completion of the credit shall not prejudice any right of the beneficiary under the applicable law governing the underlying obligation to recover the amount of those charges from the originator.

Explanatory Note by the UNCITRAL Secretariat on the Model Law on International Credit Transfers

NOTES

Article Y Conflict of laws

(1) The rights and obligations arising out of a payment order shall be governed by the law chosen by the parties. In the absence of agreement, the law of the State of the receiving bank shall apply.
(2) The second sentence of paragraph (1) shall not affect the determination of which law governs the question whether the actual sender of the payment order had the authority to bind the purported sender.
(3) For the purposes of this article:
(a) where a State comprises several territorial units having different rules of law, each territorial unit shall be considered to be a separate State;
(b) branches and separate offices of a bank in different States are separate banks.

[2] This law does not deal with issues related to the protection of consumers.

[3] The Commission suggests the following text for States that might wish to adopt it:
If a credit was for the purpose of discharging an obligation of the originator to the beneficiary that can be discharged by credit the account indicated by the originator, the obligation is discharged when the beneficiary's bank accepts the payment order and to the extent that it would be discharged by payment of the same amount in cash.

Bibliography

BIBLIOGRAPHY

I. PRIMARY SOURCES

International and National Documents

Carblanc,Anne "Privacy Protection and Redress in the Online Environment: Fostering Effective Alternative Dispute Resolution", 22nd International Conference On Privacy and Personal Data Protection, (Venice,28-30September,2000),available at, http://www.oecd.org/dsti /sti/it/secur/prod /venice paper.pdf.

Clearing and Settlement Arrangement for Retail Payment in Selected Countries, 2000, Committee on Payment and Settlement System, available at http://www.bis.org/publ/cpss40.pdf.

Consultative Document on Customer Due Diligence for Banks, Basle Committee on Banking Supervision, 2001, available at http://www.bis.org/publ/bcbs77.pdf.

Critique of the 1994 EU Report on Repaid cards, 199 of 6, available at DRVSPACEics.com/docs/papers/1994_critique.html#cb_comp" competition between Nations.

Dandekar Committee on Legal Issues in Electronic Banking, available at http://www.bankersindia.com/committees/dandekar/committee.htm.

Draft Guide to Enactment of the UNCITRAL Model Law on Electronic Signature, A/CN. 9/WG.IV/wp.88, March 2001.

Draft Legal Guide on Electronic Funds Transfers: Report of the Secretary General (A/CN.9/266 and Add.1 and 2).

Draft Model Law on International Credit Transfers: Suggestions for the Final Review: Note by the Secretariat, (A/CN.9/367).

Electronic Commerce and the NII: Draft for Public Comments, available at http://iitfcat.nist.gov:94/doc/electronic_commerce.html>.

Electronic Commerce: The Challenges to Tax Authorities and Taxpayers, An Informal Round Table Discussion between Business and Government, Turku, Finland, 18th Nov. 1997, OECD, available at http://www.oecd.org/daf/fa/e-com/turku_e.pdf.

Electronic Funds Transfers, Report of the Secretary-General (A/CN.9/278).

Electronic Signature and Records: Legal Policy and Technical Consideration, Appendix G to the statement by the legislative and the policy making group of America Bar Association.

FATF Annual Report (1999-2000), available at, http:// www.oecd.org/fatf.

First Council Directive 77/780/ESC of 12th Dec. 1977 on the condition of the Laws, Regulation and Administrative Provisions Relating to the Taking up and pursuit of the Business of Credit Institution OJL. 322, 17th Dec. 1977.

Huges, Eric, "Address before the seminar in Law, Internet, and Society" at *Harvard Law school* (Apr. 1.1996). Reproduced from *Harvard Journal of Law and Technology*, Vol. 10, No. II, winter 1997.

ICC, General Usage of Internationally Digitally Insured Commerce (GUIDEC),available at,http://www.iccwbo.org/cust/html/guidec./20./.20living./.20 documents.htm

Implications for Central Banks of the Development of Electronic Money, BIS, (Basle, Oct. 1996), available at http://www.bis.org/publ/bisp01.pdf.

Jurisdiction Over Fraud Offences With a Foreign Element (1987), Law Commission, U.K., Para 2.7.

Legal Value of Computer Records: Report of the Secretary General (A/ CN.9/ 265).

Managing Change in Payments Systems, Policy Paper No. 4, Bank for International Settlements, Monetary and Economic Department, Basle, May 1998.

Narasimham- II Committee Report on Banking Sector Reforms, available at http://www.bankersindia.com/committiees/ Narasimham II Committee html.

OCED Guidelines for Consumer Protection in the context of Electronic Commerce, 1998, available at http://www.oecd.org/ news-and-events/release/ guidelines consumer. Pdf.

OECD Guidelines for the security of information systems, C (92) 188/ Final, November 1992.

OECD Guidelines on Cryptography Policy, 1997, available at, http://www.oecd.org/dsti/sti/it/ec/act/paris-ec/pdf/progrep-e.pdf.

OECD Guidelines on the Protection of Privacy and Trans Border Flows of Personal Data, available at http://www.oecd.org.

OECD Inventory of Approaches to Authentication and Certification in Global Networked Society, DSTI/ICCP/REG (98) REV 3, SEP 1998.

OECD, Electronic Commerce: A Discussion Paper on Taxation Issues, Directorate for Financial, Fiscal and Enterprise Affairs, Committee on Fiscal Affairs, October, 1998.

OECD, Improving Access to Bank Information for Tax Purposes, A Statement to the media by Gabriel Makhlouf, Chair of the Committee on Physical Affairs, April 2000.

OECD, Inventory of Controls on Cryptography Technology, DSTI / ICCP/REG (98) 4/Final, Jan 1999.

Planning of Future Work on Electronic Commerce: Digital Signatures, Certification Authorities and Related Issues, A/ CN.9/ WG IV/ WP. 71 31.

Report of the Working Group on International Payments on the work of its 18th Session, (Vienna, 5-16 December, 1988), (A/CN.9/318).

. Risk Management for Electronic Banking and Electronic money Activities, Basle Committee on Banking Supervision, (Basle, March 1998), available at, http://www.bis.org/publ/bcbs35.pdf

Saraf Committee Report on Technology Issues, available at http://www.bankersindia.com/committees/ saraf-committee,htm.

Scottish Law Commission Consultative Memorandum no. 68, para 3.9.

Security of Electronic Money, by the Committee on Payment and Settlement Systems and the Group of Computer Experts of the Central Banks of the Group of Ten Countries, (Basle, August 1996), available at, http://www.bis.org/publ/cpss18.pdf.

. Shere Committee on Electronic Fund Transfer (EFT), available at http://www.securities.com/pl/public/public98/RBI/publican/pub990717-7 html.

Speech by Gregor Heinrich, Session 9: "Establishing Payment Systems and Easing Logistical Problems", at the conference on "dismantling the Barriers to Global Electronic Commerce", Turku, Finland, 19-21, November 1997.

Survey of Electronic Money Developments, CPSS, May 2000, available at http://www.bis.org/publ/CPSS38.pdf.

The Forty Recommendations, Financial Action Task Force on Money Laundering, available at http:// www. oced.org/ fatf.

The G-10 Deputies Report on Electronic Money – Consumer Protection, Law Enforcement, Supervisory and Cross – border Issues, (Basle, April 1997), available at http://www.bis.org/publ/ gten 01.pdf.

The Report of the Consumer Electronic Payments Task Force (U.S.A), 1998, available at http://www.occ.treas.gov/money/ceptfrpt.pdf.

The Role of the Central Bank in the Growing Industry of Internet Payments, available at http://www.genocities.com/Wall Street/2486.

UNCITRAL Draft Model Law on Legal Aspects of Electronic Data Interchange and Related Means of Communication, (Annex II to Document A/ 50/ 17), together with a Draft Guide to Enactment (A/ CN.9/ 426), 1996.

UNCITRAL Model Law on Electronic Commerce, Guide to Enactment 1996, with additional article 5 bis as adopted in 1998, General Assembly Resolution 51/162 of 16th Dec. 1996.

UNCITRAL Model Law on International Credit Transfer (1992), United Nations 1994.

UNCITRAL Model Law on International Credit Transfers; Note by the Secretariat (A/CN.9/384).

UNCITRAL, Model Law On International Credit Transfers: Note by the secretariat, A/ CBN.9/ 384.

UNCTAD: Electronic Commerce: Legal Consideration; UNCTAD/ SDTE/BFB/1.

Vasudevan Committee Report on Technology Upgradation, available at http://www.securities.com/pl/public/public98/RBI/publican/pub990717-10 html.

Wassenaar Arrangement on Export Controls for Conventional Arms and Dual Use Goods and Technologies, 1996,available at http://www.wassenaar.org/

International Treaties and National Statutes

Bankers' Book Evidence Act, 1891.

Certifying Authorities Rules, 2000.

Conference Report on S.761, Electronic Signatures in Global and National Commerce Act- (House of Representatives- June 8, 2000), p.

Cyber Regulation Appellate Tribunal Rules, 2000.

E.C. Directive on a Common Framework for Electronic Signature, 1998, O.J. 98/C325/04(23/10/98).

E.C. Directive on the Legal Protection of Databases, 1996, Directive 96/9/EC,March1996,OJL77,1996,available at http://www2.echo.lu/legal/en/ipr/database/database.html.

E.C. Directive on the Protection of Consumer with respect to Distant Contracts, Directive 97/7EC, May 1997, OJL 144, 1997, available at http://europa.eu.int/comm/dg24/policy/developments/dist_sell/dist01_en.html.

E.C. Directive on the Protection of Individuals with regard to the Processing of Presonal Data and on the Free Movement of such Data, 1995, Directive 95 /46/EC, OJ23. 11.19.95 NOL.281, available at http://www.2echo.lu/legal/en/dataprot/directive/directive.html.

E.C.E-Commerce direcctive,1998,available at http://www.ispo.cec.be/ e-commerce/legal.html#legal.

E.C. Transparency Directive, 1998, 98/34/EC, June 98, OJL 204, 1998 as amended by the Directive 98/48/EC, July 1998, OJL 217, available at http://europa.eu.int/eur_lex/en/lif/dat/1998en_398L0048.html.

European Commission Proposal for a Directive on the Taking-up, the Pursuit and the Prudential Supervision of the Business of Electronic

Money Institution, 1998, available at, http://europa.eu.int/ISPO/e-commerce /legal/document/52000 ag 0008-en.pdf.

European Model EDI Agreement, 1994 O.J.L.338/98.

Income Tax Act, 1961.

Indian Contract Act, 1872.

Indian Evidence Act, 1872.

Indian Penal Code, 1860.

Information Technology (Procedure for Holding Enquiry and Imposing Penalties by Adjudicating Officer) Rules, 2000.

Information Technology Act, 2000.

Monopolies and Restrictive Trade Practices Act, 1969.

Negotiable Instruments Act, 1881.

Reserve Bank of India Act, 1934.

Singapore Electronic Transaction Act, 1998.

The Consumer Protection Act, 1986.

U.K. Computer Misuse Act, 1990.

U.K. Consumer Credit Act, 1974.

U.K. Data Protection Act, 2000.

U.K. Good Banking Code of Practice, 1999.

U.K. Money Laundering Regulations, 1993.

U.K. The Electronic Communications Act, 2000.

U.K. Unfair Terms in Consumer Contract Regulations, 1994.

U.S. Computer Fraud and Abuse Act.

U.S. Electronic Communications and Privacy Act, 1986.

U.S. Electronic Fund Transfer Act,1978, Regulation E and Regulation Z.

U.S. Fair Credit Billing Act, 1994.

U.S. Millennium Digital Commerce Act, 1999.

U.S. Uniform Commercial Code, 1995.

Unif.Unclaimed Property Act (1995), available at http://www.law.openn.edu./bll/ulc/fnact99/1905/uupa95.html.

II. SECONDERY SOURCES

Books

Alelio, Ellen d and Colli, John T, in Ruh (ed), *The Internet and Business: A Lawyers Guide to the Emerging Legal Issues*, (Steptoe & Johnson Publications, Washington, 1996).

Alelio, Ellen d', *"The Challenge of Information Privacy in the World of Cyber Banking, Electronic Banking Law and Commerce Report"*, (Glasser Legal Works, New York, June 1996).

Amor, Daniel, *The E-Business Revolution: Living and Working in an Inter-Connected World*, (Prentice Hall International Ltd, PTR, London, 1999).

Bajaj, Kamlesh K and Nag, Debjani, *E-Commerce: The Cutting Edge of Business*, (Tata McGraw Hill Publishing Company Ltd. New Delhi, 1999).

Brown, David, *Cyber Trends: Chaos, Power and Accountability in the Information Age*, (Dengein Books, London, 1997).

Campbell, Dennis (ed), *Law of International On-line Business: A Global Perspective*, (Sweet & Maxwell, London, 1998).

Creach, Kennith C, *Electronic Media Law and Regulation*, (Focal Press, 2000).

David, Kosiur, *Understanding Electronic Commerce*, Strategic Technology Series, (Microsoft, Washington, 1997).

Diwan, Parag and Sharma Sunil, *Electronic Commerce: A Manager's Guide to E-Business,* (Vanity Book International, New Delhi, 2000).

Ghosh, Anup K. *E-commerce Security: Weak Links, Best Defences*, (Wiley Computer Publishing, New York, 1998).

KalaKota, Ravi and Whinston, Andrew. B, *Frontiers of Electronic Commerce*, (Addision-Wesley, Massachusetts, 2000).

Kalakota, Ravi and Whinston, Andrew, *Electronic Commerce: A Manager's Guide*, (Addision-Wesley, Massachusetts, 1997).

Kamath, Nandan, *Law Relating to Computers Interest and E-commerce*, (Universal Publishing Company Pvt. Ltd. Delhi 2000).

Kaushik, P.D, *Global Electronic Commerce: Implications for India*, (Rajiv Gandhi Institute for Contemporary Studies, RGICS International Economic Relations Series, No. 2, New Delhi, 1999).

Liyod, Ian J, *Information Technology Law*, 3rd ed., (Butterworths, London, 2000).

Mattan, Rahul, *Law Relating to the Computer and the Internet,* (Butterworths, New Delhi, 2000).

Mittal, D.P, *Law of Information Technology (Cyber Law),* (Taxmann's, New Delhi, 2000).

Murphy, Peter, *A Practical Approach to Evidence*, (London, 1988).

Narayan, Asit and Thakur, L.K, *Internet Marketing E-Commerce and Cyber Laws*, (Authors Press, New Delhi, 2000).

Rahman, Syed Mahburbur and Raisanghani, Mahesh S, *Electronic Commerce: Opportunities and Challenges,*(eds), (Idea Group Publishing, Hershey,USA, 2000)

Read, Chris, *Internet law:Text and Materials,* (Butterworths, London, 2000).

Richard, Y. Wang, *Information Technology in Action: Trends and Perspectives,* (PTR Pretence Hill, New Jersey, 1993).

Schneider, Gary P. and Perry, James T, *Electronic Commerce*, (Thomson Learning, Cambridge, 2000).

Shaw, Michael, Blanning, Robert, Strader, Troy and Whinston, Andrew (eds), *Handbook on Electronic Commerce*, (Springer,New York, 2000),

Singleton, Susan and Halbstern, Simon, *The Law, Business and the Internet,* (Tolley's, Great Britain, 1999).

Silver, Michael de Kare, *E-shock: The Electronic Shopping Revolution: Strategies for Retailers and Manufacturers*, (Macmillan Business, London, 1999).

Treese, G.Winfield and Stewart, Lawrence C, *Designing Systems for Internet Commerce*, (Addison Wesley Longman.Inc. Massachusetts, April 1998).

Westland, J. Chrisotpher and Clark, Theodore H.K, *Global Elcetronic Commerec: Theory and Case Studies* (The MIT Press, Massachusetts, 1999).

York Stephen and Chia Ken (eds), *E-Commerce: A Guide to the Law of Electronic Business*, (Butterworths, London, 1999).

Articles

Adams, Lee S. and Martz, David J, "Developments in Stored Value Cards and Cyber Banking", *The Business Lawyer*, Vol. 54, May 1999 p. 1382.

American Bar Association, *Achieving Legal and Business Order in Cybserspace: Jurisdictional Issues Created by the Internet* (July 2000), available at www.abanet.org/buslaw /cyber.

Bansal, Praveen, Smart Cards Come of Age, *The Banker* (Special anniversary issue), Vol. 151, No. 819, January 2001, pp. 127-128.

Bindra, P.S, *IT Implementation in Banking-Legal Implications*, available at http://www.securities.com.pl/public/public98/RBI/publican/pub 981222-2.html.

By The Task Force on Stored Value Cards, "A Commercial Lawyers Take on the Electronic Purse: An Analysis of Commercial Law Issues Associated with Stored Value Cards and Electronic Money", *The Business Lawyer* Vol. 52, Feburary, 1997, pp. 653-727.

Caden, Mark L and Lucas Stephanie E, Accidents on the Information Super Highway, Online Liability and Regulation, available at http://www.richmond.edu/jolt/v2i1/caden_lukas.html.

Chron, S.F, " Possible Defect in Smart Cards", *Scientists*, Sep. 26, 1996, at B2.

Cipparone, Mauro, Internet Banking Services vs. Proprietary Solutions: Why the Internet is Deemed to Succeed, available at http://www.geocities.com/WallStreet/2486.

Cipparone, Mauro, *The Role of the Central Bank in the Growing Industry of Internet Payments*, p. 3, available at http://www.geocities.com/wall street/2486.

Clark, Andrew and Hunter, Mark, Creating A Cleaner Industry, *The Banker*, Vol. 150, No. 890, April 2000, pp. 88-90.

Connolly, Brain, Digital Commerce Gaining Currency, *INTELLECTUAL CAPITOL* available at, http://www.intellectualcapitol.com/.

Corwin, Philip S, "Encryption: From Obscurity to Political Controversy", *American Banker, Future Banking*, May 20, 1996 at 8A.

Cotterill, Nigel, Secrecy Laws Under Assault, *The Banker*, Vol. 150. No. 894, August 2000, pp. 62-65.

Crede, Andreas, Electronic Commerce and the Banking Industry: The Requirement and Opportunities for New Payment Systems Using the Internet, available at http://www.ascuse.org/jemc/vol1/issue3/crede.html.

Cuevas, Jackie, The Internet Banking Horizon: Bleak or Bright for Community Banks? Available at http://www.qup.com.

Desai Nishith, Legal and Policy Framework for E-Commerce in India, available at http://www.giic.org/pubs/indiawhitepaper.pdf.

Dischter, Mark S. and Burkhardt, Michael S, Electronic Interaction in the Work Place: Monitoring, Retrieving, and Storing Employee Electronic Communications in the Workplace available at http://www.mlb.com/speech1.html.

Dunne, Michael J and Mussacchio, Anna L, Jurisdiction over the Internet, *The Business Lawyer*, Vol. 54, November 1998, pp. 385-401.

Electronic Money and its Legal Impact, available at, http://www .loasbridge.533.net/e-money-html.

"Electronic Money: So Much for the Cashless Society", *The Economist*, Nov. 26, 1994, at 21.

Field, Richard L, U.S. Consumer Protections Proposed for Stored-Value Cards, available at http://www.gpo.gov/su-doc/aces/aces140.html.

Freeling, Kenneth A. and Wiggins, Ronald E, States Develop Rules for Using Digital Signatures, available at http://www.lix.com/ internet/ 1020esig.html.

Galvin, Andrew, “The Legal Nature of Stored Value Card Transactions”, *Journal of Banking, Finance, Law, and Practice* vol.10, No. 1, 1999, pp.54-65.

Garcia, D, Linda, Networked Commerce: Public Policy Issues in a Deregulated Communication Environment, *The Information Society*, Vol. 13, No. 1, January-March 1997.

Garnett, Richard, Are Foreign Internet Infringers Beyond the Reach of the Law?, *UNSW Law Journal*, Vol. 23, No. 1, 2000, pp. 105-126.

Goldman, Nahum, The City Bank Affair: A Purely Russian Crime? available at http://www.ARRAYdev.com/JIBC/

Goldsworthy, Mary Anne, Smart Card Ends Plastic Proliferation, available at http://www-cec.buseco.monash.edu.au/

Grabbe, J. Orlin, Internet Payment Schemes: Part 3, available at http://www.Zotatimes.com.

Greenspan, Alan, Regulating Electronic Money, available at http://www.cato.org/pubs/policy_report/c10r.19n2-1.html.

Greguras, Fred M, Global Electronic Commerce, *Find Law for Legal Professionals*, available at http://www.findlaw.com.

Halbe, Anand, How to Build a Safe Network, *Computers Today*, September 1, 1999, pp. 60-62.

Hardy, Trotter, The Ancient Doctrine of Trespass to Websites, available at http:// www.wm.edu/law/publications/jol/hardy.html.

Hoffman, Donna L, and Novack, Thomas P, A New Marketing Paradigm for Electronic Commerce, *The Information Society*, Vol. 13, No. 1, January-March 1997.

Jones, Chris, End to End Internet Security Still Depends on Encryption Apps, *Info World*, Vol.19, No.14, April 7, 1997.

Kanvisser, Jashua B., "Coins, Notes, And Bits: The Case for Legal Tender on the Internet", *Harvard Journal of Law and Technology,* Volume 10. No. 2, Winter 1997.

Katz, Paul R, Electronic Documents and Digital Signatures: Changing the Way Business is Conducted and Contracts are Formed, *Find Law for Legal Professionals*, available at http://www.findlaw.com.

Kaur, Kavita, Cheques and Balances, *Computers Today*, August 15, 1999, pp. 140-141.

Keen, Peter, Designing Privacy for your E-business, *PC Magazine*, Vol. 19, No. 11, June 6, 2000, pp. 132-136.

Lumb, Pramod Kumar, Digital Signature Identity Assured, *Computers Today*, Vol. 16, No. 199, March, 2000, pp. 92-93.

Lupton Everett, Comment, The Digital Signature: Your Identity by Numbers, Fall 1999, at http:// www.richmond.edu/jolt/v6i2/ note 2.html.

Machinotogh, Kerry Lynin, "How to Encourage Global Electronic Commerce: The Case for Private Currencies on the Internet", *Harvard Journal of Law & Technology*, vol. 11, 3, Summer 1998, pp-749.

Maduegbuna, Samuel O, The Effects of Electroniv Banking Techniques on the Use of Paper-based Payment Mechanisms in International Trade, Journal of Business Law, 1994, pp.338-362.

Maher, Marcus, Note, International Protection of US Laws Enforcement Interests in Cryptography, available at, <http:// www.richmond..edu/jolt/maher.html>

Martin, Dave, Digital Proof of Identity, *The Banker* (Special anniversary issue), Vol. 151, No. 819, January 2001, pp. 116-117.

McCarthy, Paul, The Future is Mobile, *The Banker* (Special anniversary issue), Vol. 151, No. 819, January 2001, pp. 118-119.

McGregor, Heather, Law on a Boundless Frontier: The Internet and International Law, *Kentucky Law Journal,* Vol. 88, No. 4, 1999-2000, pp. 967-986.

Morris Niger, Cotterill, "Secrecy Laws Under Assault", *The Banker*, Volume 150, No-894, August 2000.

Motial, S.S, Electronic Commerce: The Promises and the Security Risks-An Overview, *Telematics India*, May 1999, pp.73-75.

Muller, John D, Selected Developments in the Law of Cyberspace Payments, *The Business Lawyer*, Vol. 54, November 1998, pp. 403-441.

Murray, David, Internet Banking and Commerce: Security, available at http://www.thumper.vmeng.com/pub/rah/.

Nehf, James P, Borderless Trade and the Consumer Interest: Protecting the Consumer in the Age of E-Commerce, *Columbia Journal of Transnational Law*, Vol. 38, 1999, pp. 457-465.

Netke, Shirish, E-Com Shadows, *Computers Today*, January 15, 2000, pp. 101-106.

Penny, Lunt, Payments on the Net: How many? How safe? *ABA Banking Journal*, November 1, 1998.

Perritt, Henry H. Jr, The Internet is Changing the Public International Legal System, *Kentucky Law Journal,* Vol. 88, No. 4, 1999-2000, pp. 885-955.

Pinsky, Lawrence, Digital Signatures: A Sign of the Times, at <http://ww.Isus.edu/classes/csc/spring98/March24/GORYDETL html>

Purkayastha, Arindan Das, Cryptosystems: The Key to Security, *Computers Today*, Vol. 16, No. 198, 1-15 March, 2000, pp. 82-85.

Radigan, Joseph, "Locking up: The Money Monopoly", *U.S. Banker*, Jan. 1997, pp. 26.

Raipuria, Kalyan, Electronic-Commerce: Opportunities for Indian Exports, *Economic and Political Weekly*, Vol. 35, August 26- September 1, pp. 3260-3265.

Rupley, Sebastian, E-Business, *PC Magazine*, Vol. 19, No. 15, September 1, 2000, pp. 140-143.

Ryder, Rodney D, Internet Banking: The Legal Challenges, *Computers Today*, Vol. 16, No. 202, 1-15 May, 2000, pp. 58-60.

Scarrott, Paul, "Banking in a Mobile World", *The Banker Supplement*, April 2000, p. 16.

Scott, Kennith E, Electronic Commerce Revisited, *Stanford Law Review*, Vol. 57, No. 5, May 1999, pp. 1333-1342.

Seitz, Juergen and Stickel, Eberhard, Internet Banking – An overview, pp. 4-12, available at, www.arraydev.com/commerce/JIBC/9801-8/htm.

Sergeant, Carol, E-Banking – Risks and Responses. 2000 available at, www.fsa.gov.uk/pubs/speeches/sp46.html.

Shapiro, Andrew L, Privacy for Sale, Peddling Data on the Internet, *NATION*, Vol. 264, No.24, June 23, 1997.

Sifers, Randell W, "Regualting Electronic Money in Small Value Payment Systems: Telecommunication Law as a Regulatory Model", *Federal Communications Law Journal,* April 1997, p.719.

Singh, Ranjit, E-Commerce: Into the Age of Borderless Markets, *Telematics India*, May, 1999, pp. 6-11.

Spencer, Peter, Through the Glass Window, The Banker (Supplment, April 2000, pp. 6-8.

Stewart, C. David, The Future of Digital Cash on the Internet, available at http://www.global-concepts.com/

Stewart, David C., The Future of Digital Cash on the Internet, available at, http://www.global.concepts.com.

Sundaram, Chander, A New Chapter for Electronic Commerce in India, *The Economic Times*, Bangalore, March 25, 1998.

Thomson, Paul and Randall Bernard, Privates on Parade, *The Banker*, Vol.150, No. 889, March 2000, pp. 98-99.

Tucker, Michael Jay, The New Money: Transactions Pour Across the Web, *Datamation*, Vol. 43, No. 4, April 1997.

Tynan, Daniet, "Privacy 2000 In Web We Trust?" *PC World*, Vol. 18, No. – 6, June 2000, p. 107.

Tyree, Alan L, "Regulating the Payment System – Part I", *Journal of Banking and Finance Law and Practice,* Vol. 10, No.1, March 1999 pp. 66-68.

Tyree, Alan L, "Virtual cash – Payments on the Internet – Part I", *Journal of Banking and Finance Law and Practice*, Vol. 7, 1996, pp. 35-38, available at http://www.law.usyd.edu.au/~alant/netplay.html.

Tyree, Alan L, *Virtual Cash – Part – II,* available at http://www.law.usyd.edu.au/~alant/netpay2.html.

Unnithan, Chandana R, and Swatman, Paula, M.C, E-Business Adaption: A comparison Australian and Indian Experiences in Internet Banking, available at, http://mis.deakin.edu.au/research/wprking_papers_2001/2001-06-unnithan.pdf.

Vartanian, Thomas. P, The Future of Electronic Payments: Roadblocks and Emerging Practices, available at http://www.ffhsj/bancmail/bancpage.htm

Wlatham, Tony, Managing Your Online Identity, *Computers Today*, September 1, 1999, pp. 64-66.

Young, Kung, WAP Fever: Have You Got It?, *The Banker*, Vol. 150, No. 890, April 2000, pp. 20-26.