CHAPTER V

LEGAL RELATION OF E-BANKING IN INDIA

5.1. Introduction

Law cannot possibly be expected to keep pace with changes in technology. The recent debacle of virtual voyeurism has brought out, amongst other things, the inadequacy and vulnerability of the laws governing use of internet. Fixing liability, recording and reproducing evidence, ascertaining jurisdiction are problems which show little sign of easing. Concerns over security and misuse pertaining to e-banking activity have been mounting as more banks in India foray into electronic banking.\(^1\)

Though there was a message to banks that they should be formed for public good, since inception, banking has always been a commercial venture, the prime motive of banks being to enlarge profits. And lately adoption of new economic environment such as liberalisation, privatization and globalization has caused concern in banking sector. Indian banks have also undergone a sweeping change where deregulation, technological innovations and globalization are significantly affecting the banking services.\(^2\)

The emergence of internet banking has made many banks to rethink their Information Technology (IT) strategies in competitive markets. It is suggested that the banks that fail to respond to the emergence of internet banking in the

---

market are likely to lose customers and that the cost of offering internet banking services is less than the cost of keeping branch banking.\(^3\)

India has great prospect compared to other developing nations to leverage the potential of E-Banking and build a cash light economy. In addition to IT edge and relatively dense population, the Government of India (GOI) has clearly determined to achieve financial inclusion\(^4\) and is taking aggressive steps to see this happens.\(^5\) Rendering financial services to the un-served or poor through a market led approach is important for sustainability of financial inclusion.

There are many reforms and enrollment drives which have been undertaken by the Reserve Bank of India (herein referred as RBI) and GOI in matter of financial inclusion over the last decade. The RBI and GOI policy initiatives and reforms have considerably helped the development of E-Banking system.

The reforms include adoption of technology prototypes like smart cards, mobile based options, debit cards and credit cards. These facilities and advancement have given vent to more market driven environment, which is in fact, the future face of the Indian economy.

Adoption of new technology has resulted in risks\(^6\). The legal risk is one which arises from violation of, or non-conformance with laws, rules, regulations, prescribed practices, or when the legal rights and obligation of the


\(^4\) Financial inclusion or inclusive financing is the delivery of financial services at affordable costs to sections of disadvantaged and low-income segments of society.


\(^6\) Legal risk, security risk, market risk.
transaction are not based on well established norms. Given the relatively new nature of internet banking, rights and obligations in certain cases are uncertain and applicability of laws and rules is also ambiguous.

Other reason for legal risks is also uncertainty about the validity of agreements formed via electronic media and law relating to customers disclosure and privacy protection. A customer, who is inadequately informed about his rights and obligation, may not take proper precaution while using internet banking products or services, leading to disputed transactions, unwanted suits against the bank or other regulatory authority.

Legal risk is directly related to the electronic banking and they increase as and when its use is extended. They mainly stem from the uncertainty that exists in the legal and regulatory framework concerning E-Banking. In most countries an explicit regulating framework does exist and this is due to the experience they had in the sector of E-Banking. But the problem arises when there is no regulatory framework, where a banker offers its electronic services to other countries as well, and unified legal frame in international level does not exist.

Moreover, there is another legal risk which is relating to protection of the customers privacy. Bad use of the technology by the bank personnel or by exterior malignant intruders can expose a bank in a serious legal risk such as fraud, misrepresentation and misappropriation of funds. It is possible that the intruders acquire access in the databases of the banks and use the data of

---

7Law and Regulation of Electronic Finance and Internet Banking, 2007, in U.K., Electronic Fund Transfer Act, 1978, in U.S.A are few examples such regulations.

customers in order to commit fraud. In the enthusiasm of enhancing customer service, bank may link their internet site to other site also. This may cause legal complications and risk.

Further hackers may use the linked site to defraud a bank’s customer. If banks are allowed to play a role in authentication of systems such as acting as a Certification Authority, it will bring additional risk. With the introduction of E-banking, digital signatures are also recognized.

A digital certificate is granted by the certification authority which ensures that a given signature is, in fact, generated by a given signer. If any fraud takes place the certifying bank may become liable for financial losses incurred by the party who has relied on the digital certificate.

To cope with the risks on one hand and pressure of growing competition on the other has become inevitable to Indian banks. The banks have adopted several initiatives to curb the risk and also to play a safe in the competition world. The competition has been especially tough for the public sector banks (PSBs), as the newly established private sector and foreign banks have already sharpened their competitive edge.

Some of the proactive PSB’s have been striving hard to make their structures flexible enough to accommodate technological changes. To regulate the banking in India there are many statutes, which forms the legal framework such as Banking Regulation Act, 1949, The Reserve Bank of India Act,

---

9 Ibid at 170.
11 Act No. 10 of 1949.
E-Banking is an extension of traditional banking services with technology. As technology continues to advance, security measures also continue to improve and become more sophisticated. In 1994, Saraf Committee was appointed to study and recommend on technological issues relating to Electronic Fund Transfers (EFT). The following recommendations were made by the committee.

1. Establishment of an EFT system, with the BANKNET communications network as its carrier.

2. Enactment of suitable legislation on the lines of the Electronic Funds Transfer law.

---

12 Act No. 2 of 1934.
13 Act No. 26 of 1881.
14 Act No. 9 of 1872.
15 Act No. 42 of 1999.
16 Act No. 68 of 1986.
17 Act No. 15 of 2003.
18 Act No. 18 of 1891.
19 Act No. 1 of 1872.
20 Act No. 45 of 1860.
22 Act No. 21 of 2000.
24 Headed by W.S Saraf, the committee was constituted to look into matters relating to technology issues relating to Payments System, Cheque Clearing and Securities Settlement in the Banking Industry.
25 A network jointly owned by the RBI and PSBs.
3. Magnetic Ink Character Recognition\textsuperscript{26} clearing is to be introduced.

4. Introduction of Electronic Clearing Service Credit for low value repetitive transactions such as interest, dividend, salary, pension payments and an Electronic Debit Clearing for payments to utility companies.

5. Large scale induction of computers and communication technology in service branches.

6. Promotion of a card culture, as well as enhanced training facilities.

Many of these recommendations were implemented by the RBI. In 1998, Narasimhan committee\textsuperscript{27} was formed which made certain recommendation for the implementation EFT in Indian banking sphere.

- Encryption on Public Switching Telephone Network (PSTN) lines.
- Admission of electronic files as evidence.
- Treating Electronic Funds Transfers on par with crossed cheques / drafts for purposes of Income Tax etc.
- Electronic Record keeping.
- Provide data protection.
- Implementation of digital signatures.
- Clarification on payment finality in case of EFT.

\textsuperscript{26}Magnetic Ink Character Recognition. It is a character recognition technology used by the majority of banks on their cheques. The technology uses magnetic ink for printing the code, which is usually present at the bottom of the cheque.

\textsuperscript{27}Headed by M. Narasimham, this committee was formed by the RBI to make suggestion in banking sector in India.
The *Information Technology Act, 2000* (herein after referred as IT Act, 2000) has attempted to address a number of E-Commerce regulatory issues. The law was amended in 2008 based on the recommendation of the ‘Working Group on Internet Banking’ which examines three thrust areas such as technology and security issues, legal issues and regulatory and supervisory issue. Some of the recommendations have been addressed in the IT amended Act, 2008. It is the legal department in the bank which is entrusted with the function to advice the business groups on the legal issues arising out of the use of IT.

**5.2. Law Relating to E-Banking in India**

Law relating to banking in India has undergone sweeping changes after the advent of technology. The changes have been made due to revolution in banking sector worldwide. To meet the international standard in service the transformation was necessary. There are amendments carried to the existing laws to meet the needs of the technology in banking.

**5.2.1. Reserve Bank of India Act, 1934**

In 1995, the Reserve Bank had set up the Committee for Proposing Legislation on Electronic Funds Transfer and other Electronic Payments. Based on the recommendation, the *Reserve Bank of India Act, 1934* (herein after referred as RBI Act, 1934) was amended to include electronic banking operation. A new clause to section 58, sub-section 2 of the Act, relating to the

---

28 This Committee was headed by Shri S.R.Mittal as chairman in 2001 to look at the working of internet banking in India and make required recommendations.
29 Shere Committee on Electronic Fund Transfer and Electronic Payment.
30 Section 58 (2) (pp) of the RBI Act.
regulation of funds transfer through electronic means between banks, i.e transactions like Real Time Gross Settlement (RTGS) and National Electronic Funds Transfer (NEFT) and other funds transfer was inserted, to facilitate such EFTs and ensure legal admissibility of documents and records. RBI encouraged electronic payment system has introduced Electronic Clearing Service (ECS) and EFT system in 1995, the RTGS system in 2004, NEFT system in 2005 and Cheque Truncation System (CTS) in 2008.

ECS is an electronic mode of payment / receipt for transactions that are repetitive and periodic in nature. ECS is used by institutions for making bulk payment of amounts towards distribution of dividend, interest, salary, pension, or for bulk collection of amounts towards telephone / electricity / water dues, cess / tax collections, loan installment repayments, periodic investments in mutual funds, insurance premium and other receipts.

Essentially, ECS facilitates bulk transfer of money from one bank account to many bank accounts or vice versa. ECS and EFT was introduced in the year 1995, RTGS was introduced in 2004 and NEFT was introduced in 2005 by amending RBI Act.

System of truncation of cheques was also recognized by the RBI. Truncation is the process of stopping the flow of the physical cheque issued by a drawer to the drawee branch. The physical instrument will be truncated at some point en-route to the drawee branch and an electronic image of the cheque would be sent to the drawee branch along with the relevant information.
like the MICR\textsuperscript{31} fields, date of presentation, presenting banks etc. Thus with the implementation of cheque truncation, the need to move the physical instruments across branches would not be required, except in exceptional circumstances. This would effectively reduce the time required for payment of cheques and the associated cost of transit and delay in processing, thus speeding up the process of collection or realization of the cheques. CTS was introduced in 2008.

Working group\textsuperscript{32} was constituted headed by Shri. G. Gopalakrishnan to study frauds due to electronic banking which gave its report. In the Report the committee has highlighted the danger of compliance or checklist type of mindset and called for dynamic and proactive assessment of various threats and their mitigation. One of the important aspects is the focus on “information security awareness”, as it is acknowledged that people often represent the weakest link in the security chain. In addition, the Report has called for enhancing the use of technology for identifying anomalous e-banking transactions, effective analysis of audit trails and logs, enhancing audit processes through the use of computer assisted audit tools, identifying vulnerabilities in systems and networks and using application systems for carrying out critical business processes involving financial/regulatory/legal and customer related implications rather than through manual methods or through spreadsheets.

\textsuperscript{31}\textit{Supra note 25.}

\textsuperscript{32}\textit{Gopalakrishnan Committee on Cyber Frauds. This group was headed by Shri G. Gopalkrishnan which recommended on Information Security, Electronic Banking, Technology Risk Management and Tackling Cyber Fraud.}
Meanwhile RBI has issued guidelines on Security Issues and Risk mitigation measures related to Card Present (CP) transactions. The highlights of this circular is measure has been taken to secure Card Not Present (CNP) transactions, making it mandatory for banks to put in place additional authentication/validation for all on-line recurring transactions based on information not available on the credit/debit/prepaid cards. Accordingly, banks and other stakeholders are directed to initiate immediate action for accomplishing the following tasks within the time indicated. Implementation of improved fraud risk management practices and securing the technology infrastructure were the task assigned to the commercial banks in India. The target time given for the completing of the task was September, 2012. With the Banking Laws Amendment Act, 2012, RBI is empowered to call for any information and cause inspection of business of any ‘associate enterprise’ of a bank. This has provided legal framework for setting up a Bank Holding Companies and paves the way for issue of new bank licenses.\(^3\) RBI has been issuing guidelines to the commercial banks on IT, electronic banking and technological risk management and cyber frauds.\(^4\)

### 5.2.2. Banking Regulation Act, 1949

The Act originally came into force on 16\(^{th}\) March, 1949 and it was known as Banking Companies Act, 1949. It was amended was renamed as Banking

\(^{3}\)As many as 26 firms, including top corporate houses like Tata Sons, L&T, Reliance Group, Adiya Birla Nuvo, Bajaj, Shriram and Religare, have sought banking licence. In the past 20 years, the RBI has licensed 12 banks in the private sector in two phases. Ten banks were licensed on the basis of guidelines issued in January 1993. Two were issued in 2001. News in Deccan Herald on September 4, 2013, Hubli-Dharwad Ed., p. 12.

(Acquisition and Transfer of Undertaking) Act, 1969\textsuperscript{35} and the original Act was extended to the cooperative banks from 1966 and is simply called as B.R.Act, 1949. The objectives of the Act are, to safeguard the interest of depositors, to develop banking institutions on sound lines and to attain the monetary and credit system to the larger interests and priorities of the nation.

Amendment has been brought to the original legislation as regards acquiring of shares. An approval may be granted by the RBI if it is satisfied that the shares are acquired in the interest of public, or the in the interest of banking policy or to prevent the affairs of any banking company being conducted in manner detrimental to public interest or companies interest, or in the interest of the emerging trends in banking and international practices, or in the interest of banking and financial system in India.

The applicant is the proper person to acquire shares or voting rights and no other person has such right.\textsuperscript{36} The voting right given under the law has immense power to the shareholders to control the banking business of the company.

The RBI has exclusive power to issue, accept or reject application for licence to carry on banking business. The RBI shall establish a Fund to be called the “Depositor Education and Awareness Fund”\textsuperscript{37} The salient features of the Banking Laws (Amendment) Act, 2012\textsuperscript{38} are-

1. Regulatory power to supersede board of banks

\textsuperscript{35} Act No. 5 of 1970.
\textsuperscript{36} Section 4 of the B.R.Act, 1969.
\textsuperscript{37} Section 26 (A) of Banking Law Amendment Act 2012.
\textsuperscript{38} Act No. 4 of 2013.
Under the *Banking Regulation Act, 1949* (herein after referred as B R Act, 1949) the RBI could remove a director or any other officer of the bank. RBI is empowered to supersede the board of directors of a bank for up 12 months if it feels that the board is not working in the interest of shareholders and depositors’. In case the bank is not working in the interest of the shareholders or depositors, RBI shall carry on the business of the bank by appointing an administrator during the period. RBI now being armed with powers to supersede the Board, it can now effectively influence and regulate management of banks. To limit arbitrary exercise of power by the RBI, the Act provides for consultation with the Indian Government.

2. Inspect associate enterprises

The Act empowers the RBI to call for any information and cause inspection of business of any ‘associate enterprise’ of a bank. This should provide legal framework for setting up of Bank Holding companies and pave the way for issue of new bank licenses. Associate enterprises could be a holding company or subsidiary company\(^{39}\) of the bank, a joint venture, an enterprise which controls the composition of the Board of Directors of the bank, an enterprise which influences the bank in taking financial decision or an enterprise which obtains economic benefits from the activities of the bank.

RBI may not be able to call for information from 'associate enterprises' incorporated outside India of foreign banks. However, the Indian branches and Indian associate enterprises of a foreign bank will fall under the RBI purview.

---

\(^{39}\) Ex. Karnataka Grameena Vikas Bank is the subsidiary of Syndicate Bank.
of ‘associate enterprise’ and they may call for information. An associate enterprise (outside India) of a foreign bank which has a Wholly-Owned-Subsidiary (WOS) in India is covered under the Act.

3. Increase in voting rights

In a public sector bank (PSB), no shareholder (except the Central Government) shall exercise voting rights in excess of one percent of the total voting rights of all the shareholders.

Further, the preference share holder (except the Central Government) also has an embargo on the voting rights up to one percent of total voting rights of all the shareholders holding preference share capital only.

The Act raises the shareholders’ voting rights in a public sector bank from one percent to 10 percent. No shareholder, in a private sector bank, can exercise voting rights in excess of ten percent of the total voting rights of all the shareholders.

4. Conversion of a branch of a bank into Wholly Owned Subsidiary

Conversion of a branch of any bank into a Wholly Owned Subsidiary (WOS) or transfer of shareholding of a bank to its holding company is now exempt from stamp duty. These amendments would be beneficial for various stakeholders in the banking sector. While the banking regulator gets enhanced powers that will result in effective compliance of regulations, banks will be able to attract more investments to raise funds for business expansion and to meet capital norms.

This is a huge relief for foreign banks to convert their Indian branches into Indian WOS and expand their operations in India.
Accounts and audit\(^{41}\), is also very strict under the law. It is the auditor who should examine whether there is an effective system of obtaining confirmations/acknowledgement of debts periodically. For this purpose, the auditors should also review the branch audit reports. The auditor is expected to report on the following aspects of the recovery period, existence of a recovery policy, regular updating, monitoring and adherence, compliance with the RBI guidelines and system of monitoring of recovery from credit card dues in respect of credit cards issued.

The auditor is expected to give his observations on major frauds discovered during the year under the audit. The auditor is also expected to comment on the efficacy of the system and follow up on vigilance reports.\(^ {42}\) According to R.B.Burman Committee recommendation\(^ {43}\) the bank and financial institutions should conduct Information System Audit conforming to information system audit policy, which has been incorporated in the present system.

5.2.3. *Negotiable Instruments Act, 1881*

Under the *Negotiable Instruments Act, 1881*, cheque\(^ {44}\) includes electronic image of truncated cheque and a cheque in the electronic form. The definition of a cheque in electronic form contemplates digital signature with or without biometric signature\(^ {45}\) and asymmetric crypto system\(^ {46}\).

---

\(^{41}\) Section 29-33 of the B.R.Act, 1969.

\(^{42}\) Guidance note on Audit of Banks (Revised 2013), part IV, published by The Institute of Chartered Accountants of India, New Delhi, March 2013, p.56.

\(^{43}\) R.B.Burman Committee on Information System Security.

\(^{44}\) Section 6 of the NI Act, 1881.

\(^{45}\) A captured handwritten signature looks identical to a person’s original wet ink signature.

\(^{46}\) A cryptographic algorithm in which different keys are used to encrypt and decrypt a single message or block of stored information. One of the keys is kept secret and referred to as a private key; the other key can be freely disclosed and is called a public key.
Cheque truncation, loosely defined, is the process in which the physical movement of cheque within bank, between banks and clearing house is curtailed or eliminated, being replaced in whole or in part, by electronic records of their content, with or without images, for further processing and transmission.\textsuperscript{47}

The truncation of cheque in clearing has been given effect to and appropriate safeguards in this regard have been put forth in the guidelines\textsuperscript{48} issued from time to time. Cheque Truncation speeds up the process of collection of cheques resulting in better service to customers reduces the scope for clearing-related frauds or loss of instruments in transit, lowers the cost of collection of cheques, and removes reconciliation-related and logistics-related problems, thus benefitting the system as a whole.

The truncated cheque is an electronic image of the cheque. When it is presented for payment, the drawee bank is entitled to demand any further information regarding the truncated cheque from the bank holding the truncated cheque in case of any reasonable suspicion about the genuineness of the apparent tenor of instrument and if the suspicion is that of any fraud, forgery, tampering or destruction of the instrument,\textsuperscript{49} it is entitle to further demand the presentment of the truncated cheque itself for verification,\textsuperscript{50} provided that the truncated cheque so demanded by the drawee bank shall be retained by it, if

\begin{flushleft}
\textsuperscript{47} Supra note 36. \\
\textsuperscript{48} RBI/2012-13/444 DPSS.CO.CHD.No. 1622/04.07.05/2012-13. \\
\textsuperscript{49} Section 131 of the \textit{NI (Amendment and Miscellaneous Provisions) Act, 2002}. \\
\textsuperscript{50} Section 64 Sub-section 2 of the NI Act, 1881. 
\end{flushleft}
payment is made accordingly. This provision protects the paying banker who pays in good faith and without negligence.\textsuperscript{51}

Truncation of cheques can be done by the clearing house or the bank which collects the truncated version of the cheque. As per Section 81 of the NI Act, the banker who receives the payment is also supposed to retain the copy of the cheque even after payment has been done. Section 89 of the NI Act says that any distinction between the original cheque and the truncated image should be construed as material alteration.

A material alteration is one which varies the rights, liabilities, or legal position of the parties ascertained by the deed in its original state or otherwise varies the legal effect of the instrument as originally expressed, or reduces to certainty some provision which was originally unascertained and as such void, or may otherwise prejudice the party bound by the deed as originally executed\textsuperscript{52}. In such cases it is obligatory on the part of the clearing house or the bank to ensure the correctness of the truncated image while transmitting the image.

The Supreme Court of India\textsuperscript{53} has opined that there should be early disposal of cases relating to dishonour of cheques, enhancing punishment for offenders, introducing electronic image of a truncated cheque and a cheque in the electronic form as well as exempting an official nominee director from prosecution under the NI Act, 1881. A certificate issued on the foot of the


\textsuperscript{52} Nathu Lal v. Gomti Kuar, AIR 1940 PC 160.

\textsuperscript{53} M/S. Mandvi Co-Op Bank Ltd. vs Nimesh B.Thakore, SLP (Crl.) No.3915/2006.
printout of the electronic image of a truncated cheque by the banker who paid the instrument, shall be *prima facie* proof of such payment.\textsuperscript{54} Where the cheque is an electronic image of a truncated cheque, any difference in apparent tenure of such electronic image and the truncated cheque shall be a material alteration and it shall be the duty of the bank or the clearing house, as the case may be, to ensure the exactness of the apparent tenure of electronic image of the truncated cheque while truncating and transmitting the image.\textsuperscript{55} Any bank or a clearing house which receives a transmitted electronic image of a truncated cheque, shall verify from the party who transmitted the image to it, that the image so transmitted to it and received by it, is exactly the same.

NI Act makes an obligation on the banks to make payment in due course\textsuperscript{56}. Section 131 of the *Negotiable Instruments (Amendment and Miscellaneous Provisions) Act, 2002*) has an explanation which states, ‘it shall be the duty of the banker who receives payment based on an electronic image of a truncated cheque held with him, to verify the *prima facie* genuineness of the cheque to be truncated and and any fraud, forgery or tampering apparent on the face of the instrument that can be verified with due diligence and ordinary care’. In case of dishonor of cheque, the period for giving notice of dishonour has been extended to 30 days instead of 15 days.\textsuperscript{58} Also any dispute in this

\textsuperscript{54}Section 81 of the *NI (Amendment and Miscellaneous Provisions) Act, 2002*.
\textsuperscript{55}Section 89, *Ibid*.
\textsuperscript{56}Section 10 of the NI Act, defines payment in due course which means payment made in accordance with the apparent tenor of the instrument in good faith and without negligence to any person in possession thereof under circumstances which do not afford a reasonable ground for believing that he is not entitled to receive payment of the amount therein mentioned.
\textsuperscript{57}Act No. 55 of 2002.
\textsuperscript{58}Section 138 of the *NI (Amendment and Miscellaneous Provisions) Act, 2002*. 
matter shall be resolved within 2 years (instead of 1 Year) from the date of institution of the suit.\textsuperscript{59}

Truncating cheques entails additional operational risks. Banks have to take adequate measures to ensure that all necessary safeguards are provided. It must be in consonance with the legal requirements and banking practice. While making payment especially of high value instruments under the system extra care has to be taken, otherwise the banker will become liable under section 131 of the NI Act. But a clearing house cannot be held liable for fraud or forgery, as they cannot open the truncated cheques.\textsuperscript{60} In all cases the banker should act judiciously and within the purview of the law.

\textbf{5.2.4. Bankers Books Evidence Act, 1891}

Amendment is carried even to the \textit{Bankers Books Evidence Act}, after the advent of E-Banking in India. Section 2 of the Act defines which books are ‘bankers books’. This includes ledgers, day-books, cash-books, account-books and all other records used in the ordinary business of the bank, whether these records are kept in written form or stored in a micro film, magnetic tape or in any other form of mechanical or electronic data retrieval mechanism, either onsite or at any offsite location including a back-up or disaster recovery site of both.\textsuperscript{61} And a printout of any entry in the books of a bank stored in a micro film, magnetic tape or in any other form of mechanical or electronic data\textsuperscript{62}

\textsuperscript{59} \textit{Ibid}.
\textsuperscript{60} N. V. Deshpande Group on Truncated cheques.
\textsuperscript{62} By Amendment Act No. 55 of 2002.
retrieval mechanism obtained by a mechanical or other process which in itself ensures the accuracy of such printout as a copy is admissible as evidence.⁶³

Certified copy⁶⁴ means books in written form and has an attestation as ‘true copy’ and printout or data stored in a floppy, disc, tape or any other electronic magnetic storage system. The printout shall have certificate of bank manager and computer in-charge person.⁶⁵ All these amendments have made the law applicable to cases relating to E-Banking when evidence is produced before the court of law or an arbitrator.

5.2.5. Prevention of Money Laundering Act, 2002

Money laundering is the practice of engaging in financial transactions in order to conceal the identity, source, and/or destination of money, and is a main operation of the underground economy. Money laundering⁶⁶ is defined as the conversion or transfer of property, knowing that such property is derived from serious crime, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in committing such an offence or offences to evade the legal consequences of his action, and the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from serious crime. In other words, the source of illegally obtained funds is obscured through a succession of transfers and deals in order that those same funds can eventually be made to appear as legitimate income.

⁶⁴ Section 2 Sub Clause 8, Ibid.
⁶⁵ Inserted by an amendment in 2003.
Every financial institution is charged with the responsibility of developing policies and procedures to combat money laundering, which includes the duty to be aware of trends and adaptations in the methods by which money laundering is carried out. The most difficult aspect of this responsibility is a financial organisation’s ability to anticipate new criminal behaviour and to proactively implement protocols before the criminal behaviour occurs.67

Bankers play the most prominent role and without their connivance the operation on money laundering cannot be curtailed. Development of new high-tech coupled with wire transfer of funds has further aggravated the difficulties to detect the movement of slush funds.68

As internet banking transactions are conducted remotely, banks may find it difficult to apply money laundering rules for some forms of electronic payments.

Thus, banks expose themselves to the money laundering risk. This may result in legal sanctions for non-compliance with ‘know your customer’ (KYC) rules. Every banking company, financial institution and intermediary, as the case may be, is required to maintain a record of transactions as prescribed by the rules70 and furnish information to the director within time prescribed71

67Virender Singh Solanki, *loc. cit.*
69KYC is a term used for customer identification process. It involves making reasonable efforts to determine true identity and beneficial ownership of accounts, source of funds, the nature of customer’s business, reasonableness of operations in the account in relation to the customer’s business, etc which in turn helps the banks to manage their risks prudently. The objective of the KYC guidelines is to prevent banks being used, intentionally or unintentionally by criminal elements for money laundering.
under the law.\textsuperscript{72} The principal officer of the financial institution should furnish the information in writing or by fax or e-mail to the director. The records to be maintained by such entities are set forth in rule 3 of PMLR. Such records include record of cash transactions of value more than ten lakhs or its equivalent in foreign currency. Integrally connected cash transaction which takes place within one month, of any forged or counterfeit note,\textsuperscript{73} or there is any suspicious transactions should also be reported every month before 15\textsuperscript{th} day of the succeeding month. Such records are to be maintained by the financial institutions for ten years from the date of the transaction.\textsuperscript{74} The financial institution is also required to maintain the records and identity of their clients.\textsuperscript{75}

The financial institution is required to formulate and implement a client identification programme and for this they may have their own additional requirements to determine the identity of the clients. A copy of the said identification programme is required to be forwarded to the director. The above provision needs to be appreciated, though they are procedural in nature, it leads to maintenance of records and reporting of transactions which helps in tracking frauds, forgeries and money laundering and the persons involved in such transactions.

\textsuperscript{72} Section 12(1) states ‘Every banking co-, financial institution and intermediary shall maintain a record of all transactions, the nature and value of which may be prescribed, whether such transactions comprise of a single transaction or a series of transactions integrally connected to each other and where such series of transaction take place within a month furnish information of transaction referred, to the director within such time as may be prescribed, and to verify and, maintain the records of the identity of all its clients, in such a manner as may be prescribed’.

\textsuperscript{73} Information of forged or counterfeit coins to be submitted with seven days of such occurrence of the transaction.

\textsuperscript{74} Rule 6 of the PMLR, 2005.

\textsuperscript{75} Rule 9, \textit{Ibid.}
The law is a penal law. It imposes penalty for every failure. This penalty may in addition to penalties imposed by other laws. The officer incharge of and responsible to the conduct of the business shall be liable to be prosecuted and punished under this Act.\(^{76}\) It is therefore clear that such entities should have a robust system of keeping track of the transactions of the nature referred in the Act and the Rule and report the same within the prescribed period to the authority concerned. The fear to the financial institution is not just penalty, but reputation risk of the entity.

**5.2.6. Information Technology Act, 2000**

This is the pivotal legislation dealing with crimes committed due to technology in India. Technological innovation in general and IT applications in particular, have had a major effect in banking and finance.

The technology and security standards are of prime important as the entire base of Internet banking rests on it. If the technology and security standards are inadequate, then Internet banking will not provide the desired results and will collapse ultimately.\(^{77}\) The adoption of firm’s available new technology has been recognized as an important part of the overall process of technological change.\(^{78}\) Information security is concerned with the protection of three characteristics of information, confidentiality, integrity and availability through the use of technical solutions and managerial actions.\(^{79}\)

\(^{76}\) Section 70 of the PMLA, 2002.


\(^{79}\) Aaron M. French, *op. cit.*, p.3.
amended in 2008\textsuperscript{80} enlarging definitions, introducing the concept of electronic signature, creating new offences, and many more things. IT Act, 2000 had only two sections\textsuperscript{81} dealing with computer related offences generally.

The amended Act provides for a stronger data protection measures as well as strengthening the general framework against cyber crimes. There are certain issues which are inherent in the very nature of crimes committed by using IT which are specifically applicable to banker and customer. They are anonymity in cyberspace, the issue as to jurisdiction, the question of reliability and procuring of evidence and the issue of non-reporting of cyber crimes to authorities due to the bad publicity to the business.

The issues that are specific to banker and customer, apart from the above, are enlisted below-

1. Intermediary- From times immemorial banker and customer relationship consisted of multiple roles such as debtor and creditor, agent and principal, bailor and bailee, trustee and beneficiary, which were called as general and special relationship between banker and customer. With the innovation in technology and adoption of it by the banker has created a new role to the banker as ‘intermediary’ and in certain respect as a ‘data/information owner’.

The definition of ‘intermediary’ under IT Act, 2000, means ‘any person who on behalf of another person receives stores or transmits that message or provides any service with respect to that message’.\textsuperscript{82} Though the banks are not directly referred to in the definition, the term is very wide to cover the banker,

\begin{flushright}
\textsuperscript{80} Act No. 13 of 2008.  \\
\textsuperscript{81} Section 43 and 60 of the IT Act, 2000.  \\
\textsuperscript{82}Section 2(1)(w), \textit{Ibid}.  
\end{flushright}
as the banker receives payments on behalf of the customers by receiving electronic messages. The same procedure applies for making payments on behalf of the customer which are normal activities of the banker.

This renders them as intermediaries. Further, the definition also covers any person who provides any service with respect to such messages/records, in which case it is possible that banks may fall within the definition of the term ‘intermediary’.

The definition was amended in 2008. The amended definition reads intermediaries as ‘intermediary with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes’\(^{83}\). The amendment does not really change the position of banks as intermediary but now even electronic records maintenance and transmission makes banks as intermediaries for E-Banking.

The IT Act places some responsibilities on intermediaries such as secure the E-Transactions, password and pay with due diligence. In *Sanjay Kumar Kedia v. Central Bureau and Anr*,\(^{84}\) Supreme Court held that the service providers (intermediaries) are not liable for act done with due diligence. Whatever it is, uncertainty whether banker is an intermediary or not is not in the interest of the

---


\(^{84}\)(2008) 2 SCC 294.
customer. Only thing is banker should act judiciously in case of E-Banking transaction.

2. Encryption\textsuperscript{85}-The Central Government may, for securing the use of the electronic medium and for promotion of E-governance and E-commerce, prescribe the modes or methods for encryption\textsuperscript{86}. This is because any data which is transferred online is subject to the risk of being intercepted and misused. Encrypting data before transferring it over the internet will go a long way in safeguarding against such interception. But such interception will not be of any use unless it is decrypted. If encryption of data is adopted by internet service providers, it will be helpful in protecting the customers’ privacy and also protection of all other data’s. Internet Service Provider licence restricts the level of encryption for individuals, groups or organizations. For banks RBI has stipulated a Secure Sockets Layer (SSL)\textsuperscript{87}.

3. Data Protection- Data Protection refers to the set of privacy laws, policies and procedures that aim to minimize intrusion into ones privacy caused by the collection, storage and dissemination of personal data. Personal data generally refers to the information or data which relate to a person who can be identified from that information or data whether collected by any Government or any private organization or an agency.

   IT Act imposes civil and criminal liability on a body corporate who is possessing, dealing or handling any sensitive personal data or information, and

\textsuperscript{85}Encryption is the process of encoding messages (or information) in such a way that third parties cannot read it, but only authorized parties can.

\textsuperscript{86}Section 84A of the IT Act, 2000.

\textsuperscript{87}SSL stipulated by RBI for banks is SSL/128 bit as minimum level of security as per RBI’s report 2001.
is negligent in implementing and maintaining reasonable security practices resulting in wrongful loss or wrongful gain to any person, then such body corporate may be held liable to pay damages to the person so affected\textsuperscript{88}.

It is important to note that there is no upper limit specified for the compensation that can be claimed by the affected party in such circumstances. It is in the discretion of the court to grant compensation to the victim. The Act prescribes the punishment if any person who, in pursuance of the powers conferred under the IT Act, 2000, has secured access to any electronic record and information without the consent of the person concerned discloses such information to any other person, then he shall be punished with imprisonment upto two years or with fine upto one lakh or with both\textsuperscript{89}. Section 72A on the other hand provides the punishment for disclosure by any person, including an intermediary, in breach of lawful contract.

The purview of Section 72A is wider than section 72 and extends to disclosure of personal information of a person (without consent) while providing services under a lawful contract and not merely disclosure of information obtained by virtue of powers granted under IT Act, 2000. As of now, the issue of data protection is generally governed by the contractual relationship between the parties, and the parties are free to enter into contracts to determine their relationship defining the terms personal data, personal sensitive data, data which may not be transferred out of or to India and mode of

\textsuperscript{88} Section 43A of the IT Act, 2000.
\textsuperscript{89} Section 72 of the IT Act, 2008.
handling the same. Many a time the data is leaked or fraud is carried with the help of employee of the bank also.

Internal threats can stem from three areas: the application development department, the infrastructure, and the data center. Despite the risk of internal threats, it is highly believed that threats from employees are largely unintentional. Threats from the employees results in misappropriation and embezzlement of funds.

4. Computer related offences and Penalty/Punishment -The IT Act, 2000 as amended, exposes the banks to both civil and criminal liability. The civil liability could consist of exposure to pay damages by way of compensation upto five crores under the amended IT Act before the Adjudicating Officer and beyond five crores in a court of competent jurisdiction.

There could also be exposure to criminal liability to the top management of the banks given the provisions of Chapter XI of the amended IT Act and the exposure to criminal liability could consist of imprisonment for a term which would extend from three years to life imprisonment as also fine. Phishing is one such offence which is covered.

---

90 Aaron M French, *loc. cit.*
92 Section 43-45 of the IT Act, 2008.
95 Phishing is the act of attempting to acquire information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication.
5. Bank’s to be licensed as Certifying Authority-Banks shall be allowed to apply for a license to issue digital signature certificate\(^{96}\) and function as certifying authority for facilitating Internet banking and that Reserve Bank of India shall issue the licence under clause (o) of Section 6(1) of the Banking Regulations Act, 1949.

The authentication of electronic records for the purposes of Internet banking should be in accordance with the provisions of the Act. The electronic records duly maintained for the purposes of Internet banking would be recognized as legally valid and admissible.

The digital signature\(^{97}\) affixed in a proper manner would satisfy the requirement of signing of a document for the purposes of Internet banking. A digital signature meeting the specified requirements would be deemed to be a secured digital signature for carrying out Internet banking transactions.

Digital signatures share some interesting features with legal signatures in the sense that they can be fairly readily and intimately related to an individual and they serve to authenticate digital content with a high degree of assurance. Any kind of paper work, which is required to be filed in the government offices or its agencies, would be deemed to be duly filed if it is filed in the prescribed electronic form.

---

\(^{96}\) Section 21 of the IT Act, 2000.

\(^{97}\) A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, such that the sender cannot deny having sent the message (authentication and non-repudiation) and that the message was not altered in transit (integrity). Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering.
Thus the paper formalities can be effectively substituted with electronic filings for Internet banking purposes. The records are maintained in electronic form. And then each bank can also publish rules, regulations, order, bye-laws, notification or any other matter pertaining to its business in electronic format.

If electronic record is sent by the originator or by his agent or by an information system programmed by or on behalf of the originator to operate automatically, then the electronic record shall be attributed to the originator. The requirement of acknowledgement of documents sent for the purposes of Internet banking is adequately safeguarded by the Act. The Internet banking may require to determine the time and place of dispatch and receipt of electronic records. The Internet banking would require the secured electronic records for its proper working. Where any security procedure has been applied to an electronic record at a specific point of time, then such record shall be deemed to be a secure electronic record from such point of time to the time of verification.

The CG has the power to prescribe the security procedures to give effect to the provisions of the Act, having regard to the commercial circumstances prevailing at the time when the procedure was used. Thus, the CG can specify safety measures and security procedures for Internet banking under the provisions of the Act. The Controller of Certifying Authorities can issue licenses to the Certification Authority under the IT Act, 2000. The Certifying

---

98 Section 66, 70, 72 of the IT Act.
99 Ashok Shankarrao Pawar & Sunita J. Rathod, op. cit., p.159.
Authority is assisted by the Registration Authority, which is created at the level of the organizations subscribing to the services of the Certifying Authority.

The Reserve Bank would function as a Registration Authority for the proper functioning of Internet banking. Thus, the IT Act, 2000 has laid down the basic legal framework conducive to the Internet banking in India. It must be noted that the object of the Act is to facilitate e-commerce and e-governance, which is essential for the functioning of the internet banking.

Table showing Offences and Punishment under IT Act, 2008 with regards to crimes against Electronic Banking

<table>
<thead>
<tr>
<th>Section</th>
<th>Particulars</th>
<th>Punishment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Section 43</td>
<td>If a person without the permission of the owner or anyone in charge of a computer system or network, secures access to such computer, downloads, copies or extracts data stored therein, introduces viruses or contaminants into the system, damages and/or disrupts the computer system, denies access to a person authorised to access the computer, tampers with the computer system, destroys, deletes or alters information in a computer system,</td>
<td>He shall be liable to pay damages by way of compensation to the person so affected.</td>
</tr>
<tr>
<td>Section 66B</td>
<td>Receiving a stolen computer resource.</td>
<td>Up to 3 years imprisonment, fine up to Rs 1 lakh or both.</td>
</tr>
<tr>
<td>Section</td>
<td>Description</td>
<td>Punishment</td>
</tr>
<tr>
<td>----------</td>
<td>--------------------------------------------------</td>
<td>-------------------------------------------------</td>
</tr>
<tr>
<td>66C</td>
<td>Identity theft.</td>
<td>Up to 3 years imprisonment, fine up to Rs 1 lakh.</td>
</tr>
<tr>
<td>66D</td>
<td>Cheating by impersonation</td>
<td>Up to 3 years imprisonment, fine up to Rs 1 lakh.</td>
</tr>
<tr>
<td>66E</td>
<td>Violation of privacy, video voyeurism.</td>
<td>Up to 3 years imprisonment, fine up to Rs 2 lakhs or both.</td>
</tr>
<tr>
<td>66F</td>
<td>Cyber Terrorism.</td>
<td>Life Imprisonment</td>
</tr>
<tr>
<td>67</td>
<td>Publishing or transmitting obscene material in electronic form.</td>
<td>Up to 10 years imprisonment with fine up to Rs 2 lakhs</td>
</tr>
<tr>
<td>71</td>
<td>Misrepresentation and Suppression of material facts</td>
<td>Up to 2 years imprisonment with fine of Rs. 1 lakh or both.</td>
</tr>
<tr>
<td>74</td>
<td>Publication for fraudulent purpose</td>
<td>Up to 2 years imprisonment with fine of Rs. 1 lakh or both.</td>
</tr>
<tr>
<td>85</td>
<td>Criminal liability of top bank management for various computer related offences</td>
<td>Minimum 3 years imprisonment and maximum life imprisonment</td>
</tr>
</tbody>
</table>
Apart from the above, the following important sections have been substituted and inserted by the IT Amendment Act, 2008:

Section 67C – Preservation and Retention of information by intermediaries -
This is related to matter for storing information in electronic form. Banks as intermediaries are required to store electronic information for some time as prescribed by RBI and report the same in its audit report.

Section 69 and 69A– Powers to issue directions for interception or monitoring or decryption of any information through any computer resource – If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource.

Section 69B – Power to authorize to monitor and collect traffic data or information through any computer resource for cyber security.

The cyber police or investigating authority has been authorized to collect data or information that is necessary to monitor the flow of data within or outside the country. Banks have to provide the same to the authority whenever called for.
Section 72A – Punishment for Disclosure of information in breach of lawful contract- The person disclosing shall be punished with imprisonment for a term which may extend to two years, or with fine upto one lakh rupees, or with both.

Section 79 – Exemption from liability of intermediary in certain cases- No person providing any service as a network service provider shall be liable under this information or data made available by him if he proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention.

Section 84A – Modes or methods for encryption shall be prescribed by the CG.

Section 84B – Punishment for abetment of offences- But no express provision made for the length of punishment for abetment to commit an offence under the law.

Section 84C – Punishment for attempt to commit offences - The section reads ‘Whoever attempts to commit an offence punishable by this Act or causes such an offence to be committed, and in such an attempt does any act towards the commission of the offence, shall, where no express provision is made for the punishment of such attempt, be punished with imprisonment of any description

100A service provider is a company that provides organizations with consulting, legal, real estate, education, communications, storage, processing, and many other services.
provided for the offence, for a term which may extend to one-half of the longest term of imprisonment provided for that offence, or with such fine as is provided for the offence or with both. The length of punishment is not explicit in the provision and is left to the discretion of the court.

5.2.7. Indian Contract Act, 1872

The Indian Contract Act, is two century old law, but complete in all aspects relating to contracts including E-contracts. For a valid contract there are certain requirements to be fulfilled which are, that there should be lawful consideration, the consent should be free, the persons entering into contract must be competent persons (they should not be minor, unsound mind or prohibited under law to enter into contract) and the contract should be made to achieve a lawful object. The Act also deals with the different modes of discharge of contract and also special contracts.

Apart from the above requirement, there should be proposal and an unconditional acceptance of the proposal. What one can infer from the above is that the contract enforceable under the law is a process, which has a vital significance in any transaction whether manufacturing or trading or service. The contract has to be valid contract to be enforceable.

101 Section 10 of the Indian Contract Act, 1872.
102 Section 2 (d) defines consideration thus, ‘When, at the desire of the promisor, the promisee or any other person has clone or abstained from doing, or does or abstains from doing, or promises to do or to abstain from doing, something, such Act or abstinence or promise is called a consideration for the promise.’
103 Consent which is not influenced by undue influence, coercion, fraud, misrepresentation or mistake.
104 Minor means persons below 18 years of age, Mohoribibi v. Dharmadas Ghosh, (1903) 30 Cal 539.
105 Section 2 (a) of the Act defines proposal which states ‘when one person signifies to another his willingness to do or to abstain from doing anything, with a view to obtaining the assent of that other to such act or abstinence, he is said to make a proposal’.
106 Section 2 (b) defines acceptance thus, ‘when the person to whom the proposal is made signifies his assent thereto, the proposal is said to be accepted. A proposal, when accepted, becomes a promise’.
E-contract is any kind of contract formed in the course of e-commerce by the interaction of two or more individuals using electronic means, such as e-mail, the interaction of an individual with an electronic agent, such as a computer program, or the interaction of at least two electronic agents that are programmed to recognize the existence of a contract\textsuperscript{107}.

In E-Contracts the offer is not made directly to the customer. The consumer ‘browses’ the available goods and services displayed on the merchant’s website and then choose what he would like to purchase. The offer is not made by website displaying the items for sale at a particular price. This is actually an invitation to offer and hence is revocable at any time up to the time of acceptance. The offer is accepted through e-mails or by just clicking ‘I Agree’.

The significance of the contract assumes importance in cyber world where anonymity and speed of transaction are key elements. Contracts entered through online process are called as electronic contracts. Electronic contracts helps people to avail the transactions and agreements electronically without meeting each other personally. In an electronic contract normally two parties are involved, the originator and the addressee. The originator is one who sends, stores or transmits electronic messages.\textsuperscript{108} The message is transmitted to the ‘addressee’ is one whom the originator intends to receive the electronic record but does not include intermediary.\textsuperscript{109} Intermediary is a person who transmits, stores or receives message on behalf of another or provides any service in

\begin{small}
\textsuperscript{107}Definition as given under U.S ‘The Uniform Computer Information Transactions Act’.
\textsuperscript{108} Section 2 (1) (az) of the IT Act, 2000.
\textsuperscript{109} Section 2(b), Ibid.
\end{small}
respect thereof. If we apply the above theory then in the terms of contract, the result is originator is the promissory; addressee is promise and intermediary is the service of carrier.\textsuperscript{110} Electronic message/data can be transmitted without human intervention. As soon as the message is transmitted to the intermediary and is out of control of the originator, it is regarded as delivered.\textsuperscript{111}

According to section 12 of the IT Act, if the originator has stipulated for acceptance (I agree) and if that for formalities is completed by the addressee, it becomes a binding/valid contract. The legal requirement of signing the electronic document is also fulfilled by attesting digital signature through a private key assigned to the party by the certifying authority. This part concludes two aspects of contract that is proposal and acceptance. The third part is that the consent must be free that is it must not be taken by coercion,\textsuperscript{112} undue influence,\textsuperscript{113} fraud,\textsuperscript{114} misrepresentation,\textsuperscript{115} or by mistake. Among them fraud is both civil wrong as well as criminal wrong. And in commercial


\textsuperscript{111} Section 13 of the IT Act, 2000.

\textsuperscript{112} Section 15 of the \textit{Indian Contract Act} defines Coercion” is the committing, or threatening to commit, any act forbidden by the Indian Penal Code, or the unlawful detaining, or threatening to detain, any property, to the prejudice of any person whatever, with the intention of causing any person to enter into an agreement.

\textsuperscript{113} According to 16 of the \textit{Indian Contract Act}, ‘a contract is said to be induced by” undue influence where the relations subsisting between the parties are such that one of the parties is in a position to dominate the will of the other and uses that position to obtain an unfair advantage over the other’.

\textsuperscript{114} Section 17 of the \textit{IC Act} defines fraud as “fraud” means and includes any of the following acts committed by a party to a contract, or with his connivance, or by his agent, with intent to deceive another party thereto of his agent, or to induce him to enter into the contract, the suggestion, as a fact, of that which is not true, by one who does not believe it to be true, the active concealment of a fact by one having knowledge or belief of the fact, a promise made without any intention of performing it, any other act fitted to deceive and any such act or omission as the law specially declares to be fraudulent.

\textsuperscript{115} Misrepresentation” means and includes, the positive assertion, in a manner not warranted by the information of the person making it, of that which is not true, though he believes it to be true, any breach, of duty which, without an intent to deceive, gains an advantage to the person committing it, or any one claiming under him, by misleading another to his prejudice or to the prejudice of any one claiming under him and causing, however innocently, a party to an agreement to make a mistake as to the substance of the thing which is the subject of the agreement.
transaction, fraud affects the most. In case of banker and customer relationship is a contractual relationship and hence after the advent of E-Banking fraud has played a pivotal role. Though Indian Contract has defined fraud, but the wrong is civil in nature. The person who has suffered injury or damage can claim only compensation. Fraud committed on banks or by banks is criminal in nature because it involves a deceptive act perpetrated on a victim which is done for personal or financial gain. Hence, the definition of fraud as stated in contract law can be used only to know the meaning and claiming compensation. E-Banking is ultimately an E-Contract and all the provisions of Indian Contract Act applies to it muttas mundadis.

5.2.8. Indian Penal Code, 1860

Crime is both a social and economic phenomenon. It is as old as human society. In developing economies, cyber crime has increased at rapid strides, due to the rapid diffusion of the Internet and the digitization of economic activities. The improvement of online banking system and its increased use by consumers worldwide has made this service a privileged target for cyber criminals.

Sweeping amendments were made to certain provisions of Indian Penal Code (herein referred as IPC).\textsuperscript{116} Section 172 relating to documents to be produced before a Court of Justice includes electronic records, section 192 on

\textsuperscript{116} For example, section 29A, under which the word ‘electronic record’ was given meaning as, as in IT Act.
makes false entry in books of records, and section 463, the amendment is inserting false electronic record with the intent to cause damage or injury.

The significant amendment was to section 464 of the Act which is as follows- A person is said to make a false document or false electronic record, if, first, who dishonestly or fraudulently makes, signs, seals or executes a document or part of a document, or makes or transmits any electronic record or part any electronic record, or affixes any digital signature on any electronic record, or makes any mark denoting the execution of a document or the authenticity of the digital signature, with the intention of causing it to be believed that such document or part of a document was made, signed, sealed or executed by or by the authority of a person by whom or by whose authority he knows that it was not made, signed, sealed or executed, or at a time at which he knows that it was not made, signed, sealed or executed; or affixed with, or Secondly.- Who, without lawful authority, dishonestly or fraudulently, by cancellation or otherwise, alters a document or an electronic record in any material part thereof, after it has been made or executed or affixed with digital signature either by himself or by any other person, whether such person be living or dead at the time of such alteration; or Thirdly.- Who dishonestly or fraudulently causes any person to sign, seal, execute or alter a document or an electronic record or to affix his digital signature on any electronic record knowing that such person by reason of unsoundness of mind or intoxication

117 Stated thus ‘ for the words ‘makes any false entry in any book or record, or makes any document containing a false statement, the words ‘makes any false entry in any book or record, or electronic record or makes any document or electronic record containing a false statement’ was substituted.
118 The words in italics are added newly to the section.
cannot, or that by reason of deception practiced upon him, he does not know the contents of the document or electronic record or the nature of the alteration. Then section 469, for the words "intending that the document forged" the words "intending that the document or electronic record forged" was substituted. Section 474, for the portion beginning with the words "Whoever has in his possession any document" and ending with the words "if the document is one of the description mentioned in section 466 of this Code", the following words were substituted, "Whoever has in this possession any document or electronic record, knowing the same to be forged and intending that the same shall fraudulently or dishonestly be used as a genuine, shall, if the document or electronic record is one of the description mentioned in section 466 of this Code.". IPC is a legislation which is probably the most widely used law in criminal jurisprudence, serving as the main criminal code of India. Offences or crimes have been elaborately dealt under this legislation listing punishment for each offence. IT Act 2000 has amended the sections dealing with records and documents in the IPC by inserting the word ‘electronic’ thereby treating the electronic records and documents on par with physical records and documents. The sections dealing with false entry in a record or false document are (ex. 192, 204, 378, 383, 463, 464, 468, 469, 470, 471, 474, 476, 499, etc) have since been amended as electronic record

119 Theft.- of Hard ware.
120 Extortion- Web-Jacking.
121 Forgery – of signatures and digital signatures.
122 Making a False document- like e-mails, pan card.
123 Forgery for the purpose of cheating.
124 Forgery for purpose of harming reputation.
125 Defamation.
and electronic document thereby bringing within the ambit of IPC, all crimes to an electronic record and electronic documents just like physical acts of forgery or falsification of physical records. Internet frauds in India are recent phenomena but over the years, it has emerged like an organized crime. Hackers may be anywhere in the world and employ any technique to commit the fraud. Even mobile transactions are hit by the frauds. There are three crucial elements which are considered responsible for the commission of frauds in banks:

a. Involvement of bank's employee or in connivance with outsiders;
b. Failure of the bank staff to follow the instructions and guidelines; and
c. External elements or collusion between various parties or by a hacker.

Though there are various kinds of frauds, but purely from reporting standpoint, RBI has classified frauds on the basis of the provisions of the IPC-

a. Misappropriation (Section 403 IPC) and criminal breach of trust (Section 405 IPC);
b. Fraudulent encashment through forged instruments, manipulation of books of account or through fictitious accounts and conversion of property (Sections 477A, 378 and 120 A);
c. Unauthorized credit facilities extended for reward or for illegal gratification;
d. Negligence and cash shortages;
e. Cheating (Section 415 IPC) and forgery (Section 463 IPC);
f. Forgery of electronic records (Section 465 IPC);
g. Bogus websites, cyber frauds, phishing (Section 420 of IPC)

h. Irregularities in foreign exchange transactions; and

i. Any other type of fraud not coming under the specific heads as above.

Though no specific section defines fraud, all the above provisions are related with the offence. The courts in India have dealt with E-Banking frauds combining sections of IPC and IT Act.

Ex. *Syed Asifuddin and Ors. v. The State Of Andhra Pradesh and others*[^126^], where case was registered under Sections 409, 420 and 120B of IPC, 1860 and Section 65 of the IT, 2000, the court stated ‘whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy, or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakhs rupees or both.

Further, while giving explanation to section 65 of the IT Act it stated the word "dishonestly" shall have the meaning assigned to it in section 24[^24^] of the IPC and the word "fraudulently" shall have the meaning assigned to it in section 25[^25^] of the IPC.

[^126^]: 2005 Cri. L.J 4314
[^127^]: Section 24 of IPC defines dishonestly as ‘whoever does anything with the intention of causing wrongful gain to one person or wrongful loss to another person, is said to do that thing” dishonestly”.
[^24^]: Section 25 of IPC defines fraudulently as ‘a person is said to do a thing fraudulently if he does that thing with intent to defraud but not otherwise’.
To mitigate this confusion, a definition of fraud was, however, suggested in the context of electronic banking in the Report of RBI Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds\textsuperscript{129}, which reads as ‘a deliberate act of omission or commission by any person, carried out in the course of a banking transaction or in the books of accounts maintained manually or under computer system in banks, resulting into wrongful gain to any person for a temporary period or otherwise, with or without any monetary loss to the bank’.

\textbf{5.2.9. Indian Evidence Act, 1872}

The enactment and adoption of the \textit{Indian Evidence Act} was a path-breaking judicial measure introduced in India, which changed the entire system of concepts pertaining to admissibility of evidences in the Indian courts of law.

The nature of evidence in the real world and virtual world is different. This disparity is conspicuous in all the stages of evidence detection, gathering, storage and exhibition before the court\textsuperscript{130}. Contrary to the real world crimes, where tangible evidences in the form of finger prints, weapon of crimes, blood stain marks, can be traced, in the virtual world such traces becomes very difficult to find. The process of preservation of cyber crime evidences lies within the understanding of an efficient and knowledgeable computer forensics expert because any carelessness in the process can lead to diminutive value of the evidence.

\textsuperscript{129}G.Gopalakrishna committee established in 2010.

Once the required evidence is identified than the investigator must ensure that the same is collected by adhering to the legal requirements. The legal requirement are, evidence is collected only after the requisite warrant for is issued, if the information appears to be outside the scope of the warrant then additional warrant be issued, completion of the investigation, and other formalities. The evidence collected becomes valid in the court of law only if the evidence is collected by legal means.\footnote{Dr. S.V. Joga Rao, ‘Law of Cyber Crimes & Information Technology Law’, Nagpur, Wadhwa and Co., (2007), p. 197.} The \textit{Indian Evidence Act} was amended according to the requirements of the IT Act.

The \textit{Indian Evidence Act} gave recognition to all electronic records and documents\footnote{Section 3 of Indian Evidence Act, 1872.}. In the definition part of the Act, the amendment was made to the word documents which are as follows ‘where the word all documents includes electronic records’.

Words like ‘digital signature’, ‘electronic form’, ‘secure electronic record’, ‘information’ as used in the IT Act, were all inserted to make them part of the evidentiary mechanism in the legislation. The under section 17, for the words ‘oral or documentary’ the words ‘oral or documentary or contained in electronic form was substituted.

Then section 35 of the Act was amended for the word ‘record’, in both the places where it occurs, the words ‘record or an electronic record’ was substituted. Section 39 of the original Act deals with evidence to be given when statement forms part of a conversation, document, book or series of
letters or papers.- ‘When any statement of which evidence is given forms part of a longer statement, or of a conversation or part of an isolated document, or is contained in a document which forms part of a book, or of a connected series of letters or papers, evidence shall be given of so much and no more of the statement, conversation, document, book or series of letters or papers as the Court considers necessary in that particular case to the full understanding of the nature and effect of the statement, and of the circumstances under which it was made’.

The substituted wordings of the section, what evidence to be given when statement forms part of a conversation, document, electronic record\textsuperscript{133}, book or series of letters or papers- ‘When any statement of which evidence is given forms part of a longer statement, or of a conversation or part of an isolated document, or is contained in a document which forms part of a book, or is contained in part of electronic record or of a connected series of letters or papers, evidence shall be given of so much and no more of the statement, conversation, document, electronic record, book or series of letters or papers as the Court considers necessary in that particular case to the full understanding of the nature and effect of the statement, and of the circumstances under which it was made’.

Section 47 was amended and section 47A which emphasis on the opinion as to relevancy of digital signature reads thus- ‘when the court has to form an opinion as to the digital signature of any person, the opinion of the certifying

\textsuperscript{133} Substituted words are in italics.
authority which has issued the Digital Signature Certificate is a relevant fact’. Section 59 was also amended where the word ‘contents of documents’, were substituted with words ‘contents of documents or electronic records’. Section 65 was amended and two subsection section 65A and 65B were inserted. 65A deals with special provisions as to evidence relating to electronic record and 65B deals with admissibility of electronic records.

The other amendments were relating to proof as to digital signature,\textsuperscript{134} proof as to verification of digital signature,\textsuperscript{135} presumption as to electronic records and digital signatures,\textsuperscript{136} presumption as to digital signature certificate,\textsuperscript{137} and production of documents or electronic records which another person, having possession, court refuses to produce before courts.\textsuperscript{138}

Amendments brought to \textit{Indian Evidence Act} were questioned in \textit{P. Padmanabh v. Syndicate Bank Limited},\textsuperscript{139} where court held admissibility of electronic records, any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer (hereinafter referred as the computer output) shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, without further proof or production of the

\textsuperscript{134} Section 67A- the fact that digital signature is of the subscriber must be proved.

\textsuperscript{135} Section 73A- Court may direct for controller of certifying authority or any person who applies the public key to verify the digital signature.

\textsuperscript{136} Section 85B of \textit{Indian Evidence Act}.

\textsuperscript{137} Section 85C, \textit{Ibid}.

\textsuperscript{138} Section 131, \textit{Ibid}.

\textsuperscript{139} AIR 2008 Kant 42.
original, as evidence of any contents of the original or of any fact stated therein of which direct evidence would be admissible.

Admissibility of electronic records as evidence as enshrined in section 65B of the *Indian Evidence Act* is wide enough to cover all types of electronic records as evidence which states as under-

‘Any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer shall be treated like a document, without further proof or production of the original, if the conditions like these are satisfied: (a) the computer output containing the information was produced by the computer during the period over which the computer was used regularly.... by lawful persons.. (b) the information ...derived was regularly fed into the computer in the ordinary course of the said activities; (c) throughout the material part of the said period, the computer was operating properly r was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and (d) the information contained in the electronic record reproduces or is derived from such information fed into the computer in the ordinary course of the said activities’

To put it in simple terms, evidences (information) taken from computers or electronic storage devices and produced as print-outs or in electronic media are valid if they are taken from system handled properly with no scope for manipulation of data.

And thus ensuring integrity of data produced directly with or without human intervention accompanied by a certificate signed by a responsible person declaring as to the correctness of the records taken from a system a computer with all the precautions as laid down in the section.
5.2.10. Consumer Protection Act, 1986

Consumer protection in India got a boost with the enactment of Consumer Protection Act, 1986. It provided a power in the hands of Indian consumers to get appropriate, timely and effective grievances redressal against companies and individuals who had provided defective good or deficient services. It has been most effective weapon in the hands of consumers for claiming compensation through speedy redressal. Speedy justice which is fundamental right of the citizens of India has been guaranteed is ensured in this Act. It is a board which is constituted and many of the formalities which are required to be followed in the normal courts need not followed. The justice is ensured by a bench headed by a chairman and two social workers who sit and listen to the matter. Both documentary and oral evidence are taken. Material objects are also examined and justice is ensured.

Customer of a bank is also a consumer as he fits into the definition of consumer\(^\text{140}\) under the law. Consumer is a person who buys or hires and goods or services for a consideration, i.e. free services are not covered under the Act.

\(^{140}\) In the wording of section 2(d) of the Consumer Protection Act, consumer means any person who—

(i) buys any goods for a consideration which has been paid or promised or partly paid and partly promised, or under any system of deferred payment and includes any user of such goods other than the person who buys such goods for consideration paid or promised or partly paid or partly promised, or under any system of deferred payment when such use is made with the approval of such person, but does not include a person who obtains such goods for resale or for any commercial purpose; or

(ii) hires or avails of any services for a consideration which has been paid or promised or partly paid and partly promised, or under any system of deferred payment and includes any beneficiary of such services other than the person who hires or avails of the services for consideration paid or promised, or partly paid and partly promised, or under any system of deferred payment, when such services are availed of with the approval of the first mentioned person but does not include a person who avails of such services for any commercial purposes.
It excludes a person who buys or hires for commercial purpose/activity and not for self-consumption.¹⁴¹

The National Consumer Forum has held that once it is found that there is hiring of service for consideration and that loss has been caused to the complainant on account of negligence and deficiency in rendering the service, the aggrieved consumer is entitled to seek remedy under Consumer Protection Act and the aggrieved consumer is also entitled to seek redressal from appropriate forum.¹⁴² Technological failure and providing confidential details have been treated as deficiency of service in banks¹⁴³ provided the customer has not acted negligently. The bank should give instruction to the customer before providing them with E-Banking facility. Internet banking has now started motivating customers to park their funds with the online banks, which has a substantially impact on the deposit base of the brick and mortar banks.¹⁴⁴ And the same should be encouraged with precautions.

5.2.11. The Payment and Settlement Systems Act, 2007

It is internationally acknowledged that payment and settlement systems should function on a well-founded legal basis¹⁴⁵.

---

¹⁴² Ibid.
¹⁴⁵ The Committee on Payment and Settlement Systems (CPSS) contributes to strengthening the financial market infrastructure through promoting sound and efficient payment, clearing and settlement systems. The CPSS is a standard setting body for payment, clearing and securities settlement systems. It also serves as a forum for central banks to monitor and analyse developments in domestic payment, clearing and settlement systems as well as in cross-border and multicurrency settlement schemes.
This entails among other things, proper authorization requirement for setting up and payment systems, legal recognition for netting, settlement finality, providing for regulation and oversight of the payment and settlement systems. In India there is no enactment which dealt with the issue of Electronic Fund Transfer (EFT). *The Payment and Settlement Act* (herein referred as PSS Act) and the directions and guidelines issued there under deal, to a certain extent, with the issue.\(^\text{146}\)

In order to strengthen the institutional framework for the payment and settlement systems in the country, the RBI constituted, in 2005, a Board for Regulation and Supervision of Payment and Settlement Systems as a Committee of its Central Board. The Board which was chaired by the Governor of RBI, while all the four Deputy Governors and two external Directors of the Central Board are its members. Based on the recommendation of the board the present legislation i.e. *The Payment and Settlement Systems Act, 2007* was drafted which gave wide powers to RBI to govern the payment system in the country. Object of this legislation is to establish safe, secure, sound and efficient payment and settlement systems for the country. Whereas safety in payment and settlement systems relates to risk reduction measures, security pertains to confidence in the integrity of the payment systems. All payment systems are envisaged to be on sound footing with adequate legal backing for operational procedures and transparency norms. Efficiency enhancements are envisaged by leveraging the benefits of technology for cost-effective solutions.

“Payment Instruction” is defined\textsuperscript{147} ‘as any instrument, authorization or order in any form, including by electronic means, to effect a payment by a person to a participant in a payment system or from one participant in such a system to another participant in that system. The payment instruction can be communicated either manually i.e. through an instrument like a cheque, draft, payment order or through electronic means, so that a payment can be made by either a person to the participant in such a system or between two participants’. Payment system” includes the systems enabling credit card operations, debit card operations, smart card operations, money transfer operations or similar operations.\textsuperscript{148} The RBI has consid(ed factors like, the need for the proposed payment system, the technical standards and design of proposed system, the security procedures and terms and conditions of operation of the proposed system, the procedure for netting of payment instructions, risk management processes, financial status of the applicant, experience of management and integrity of applicant, consumer interests, monetary and credit policies and other relevant factors while authorizing any institution who apply for payment through electronic means.\textsuperscript{149}

RBI has laid down conditions\textsuperscript{150} to be fulfilled by the institution to obtain the authorization letter.\textsuperscript{151} The Act lays down an elaborate mechanism for settlement of disputes between system participants in a payment system,

\textsuperscript{147} Section 2(1) (g) of the PSS Act, 2007.
\textsuperscript{148} Section 2(1) (i), Ibid.
\textsuperscript{149} Section 7 of the PSS Act, 2007.
\textsuperscript{150} Conditions such as technical standard and design of the proposed payment system, terms and conditions for operation including security procedure, manner in which transfer of funds may be effected, etc.
\textsuperscript{151} Section 10 of the PSS Act, 2007.
between system participant and system provider and between system providers. The RBI is empowered to call for from the system provider returns, documents and other information relating to the operation of the payment system. The system provider and all system participants are required to provide Reserve Bank access to any information relating to the operation of the payment system.

Under this legislation, dishonour of an electronic fund transfer instruction due to insufficiency of funds in the account is an offence punishable with imprisonment or with fine or both, similar to the dishonour of a cheque under the NI Act, 1881. Subject to complying with the procedures laid down under the Act, criminal prosecution of defaulter can be initiated in such cases. Hence under this legislation the RBI is able to monitor the electronic payment system in India.

5.3. Conclusion

India continues to be a unique market and regulatory environment with intense involvement of the regulator and the government. Hopefully, the rapid outreach will make the model sustainable for all banks and at the same time offer services really needed by the clients. These two ends are, of course, aligned and mutually beneficial.

---

The gradual regulatory evolution to support banks in their outreach efforts continues and the results are beginning to emerge. Increasing competition has become a challenge for Indian banks but it also provides thoughtful opportunities to develop the banking business as per international standards. The technology holds the key to success of Indian banks as India could leapfrog into internet banking.

Customers of Indian banks are still reluctant in adopting electronic banking. Understanding the reasons for this resistance would be useful for bank managers in formulating strategies aimed at increasing online banking use.\(^{155}\) Crime based on electronic offences are bound to increase and the law makers have to go the extra mile compared to the fraudsters, to keep them at bay. Technology is always a double-edged sword and can be used for both the purposes, good or bad.

Preamble of the IT Act 2000 provides that the Act was passed with the objective to give legal recognition for transactions carried out by means of electronic data interchange and other means of e-commerce. Further the Act has also made amendments to the IPC 1860, Indian Evidence Act 1872, The Bankers Books of Evidence Act 1891, and the Reserve Bank of India Act 1934 for facilitating legal recognition and regulation of the commercial activities. Though this objective of the Act is not to suppress the commercial activity, but has defined certain offences and penalties to smother such omissions, which is understood to come within the characterization of cyber crimes.

security is still a big concern for usage of e-banking services which the present legislation is inadequate to deal with. The challenges ahead to the court of law to apply the provisions have been difficult due to lack of clarity.