# MECHANISM OF ELECTRONIC FUND TRANSFERS: AN ANALYSIS OF LEGAL FRAMEWORK & CHALLENGES

***Mohan Kumar N***

***Christ Academy Institute of Law, Bangalore***

**ABSTRACT**

The purpose of this project is to conduct a thorough examination of electronic fund transfers in India and their significance in the country's banking industry. This paper will chart the emergence of electronic fund transfers, provide a brief historical context, and discuss the various kinds of electronic banking and electronic payment systems available in India. The focus of this project will be on India's legal framework for electronic funds transfers (EFTs) and the difficulties surrounding them. Finally, this paper will shed light on the future road map for EFTs' touchstone, as well as offer improvements that may be made, particularly in terms of the security and privacy of EFT systems.

**INTRODUCTION**

The Indian banking system has seen significant transformations as a result of technological adoption, particularly in the post-reform period.[1] By overcoming geographical obstacles of branch banking and alleviating time, resource, and volume constraints, technology has aided banking organisations in reaching clients' doorsteps. In the 1980s, the expansion and development of information technology, as well as advancements in computer networking, aided banks in automating transactions.[2] As a result of the advent of the internet and the following introduction of e-commerce, m-commerce, and Automated Teller Machines, the sector has undergone structural and functional changes (ATMs).



In addition to scaling boundaries, technology has aided banks in modifying strategic behaviour, increasing efficiency, and lowering transaction costs. In Indian banking, technology began as an enabler, but it has now developed into a business driver and is soon becoming an inseparable part of the process. Banks should embrace progressive

[1]Economic Reforms which took place in 1991, i.e. Liberalization, Privatization and Globalisation (LPG), also known as the New Economic Policy.

[2]R. K. Mittal and Sanjay Dhingra, "Technology in Banking Sector: Issues and Challenges" Vinimaya, Vol. 27,14 (2006-07).

computerization and correspondence advancements to give a very much planned, vigorous, and straightforward monetary foundation moored by proficient instalment and repayment frameworks.

**HISTORY AND BACKGROUND**

In the mid-1960s, the first automated teller machine (ATM) was installed, giving rise to the electronic fund transfer (EFT) system. The ATM had the option to perform account moves, get stores, and circulate cash utilizing a standard attractive stripe card and an individual's 4 digit code/PIN.[3] The RBI pushed for electronic banking in India, based on various recommendations from various committees established from time to time to enhance information technology infrastructure. In 1984, banks began implementing sophisticated technology in their internal systems to boost branch office collaboration and communication.[4]

The key proposals were using Magnetic Ink Character Recognition (MICR) technology in four major cities, establishing universal clearing house procedures, and introducing credit cards and ATMs. The major goal of the Rangarajan Committee Reports on Bank Computerization in 1994 was to provide recommendations on technical concerns related to payment systems. The Committee offered several suggestions, including the implementation of an EFT system, the implementation of MICR clearing in over 100 banks, and the promotion of a card culture. Legislation on EFT and other electronic payment mechanisms was suggested the same year. The RBI proposed a set of EFT Regulations under the RBI, 1934, and a change to the Bankers' Books Evidence Act, 1891.

Furthermore, the Narsimha Committee Report (1998) addressed issues such as financial system strengthening, technical advancement, and human resource development. The Committee emphasised the need of addressing a number of EFT authentication problems. Another committee, led by Dr. A. Vasudevan, advocated that the banking industry's technology be improved, including the legal framework for electronic banking, bank technology planning, technology outsourcing, and government computerization.



[3]Stan Sienkiewicz, "The Evolution of EFT Networks from ATMs to New On-Line Debit Payment Products" Discussion Paper, Federal Reserve Bank of Philla Payment Cards Center (April 2002).

[4] "India and the World: The Changing Paradigms in the Banking Sector due to Technological Advancements" Prajnan, Vol. 39, 130(2010-11).

The Integrated Payment and Settlement System's (IPSS) communication backbone is the Indian Financial Network (INFINET), which was developed in 1999. To examine various aspects of the technology, the RBI organised an Internet Banking 'Working Group.' The focal point of the gathering was on three significant parts of banking: innovation and security, lawful troubles, and administrative and administrative issues.[5]

The GOI (Government of India) adopted the IT Act, 2000 to offer legal recognition to electronic transactions, taking into account and acknowledging the relevance of the aforesaid challenges. The RBI Act was also amended, giving the Reserve Bank the authority to oversee electronic cash transfers between banks and financial institutions. Further legal difficulties and advancements relating to EFTs will be discussed in the third and fourth chapters, but before that, this paper has to be brightened up, therefore it is necessary to examine the various forms of electronic banking and payment systems in India.

## FORMS OF ELECTRONIC BANKING AND ELECTRONIC PAYMENT SYSTEMS IN INDIA

- **Forms of Electronic Banking:-**

1. *Internet Banking:*

Customers must physically visit the bank branch to conduct activities such as cash deposits or withdrawals, fund transfers, or account statements in conventional banking, however with internet banking, similar transactions may be accomplished using computers without having to visit the bank office. Both the consumer and the bank benefit from this arrangement.

The consumer is free of the negative effects of travel, and the time saved may be put to better use in other ways. The most significant benefit of internet banking is that it allows customers to do basic financial activities from anywhere in the globe using a PC or laptop. Customers use the internet to visit the bank's website to check and view their account information as well as complete basic banking operations.

2. *Mobile Banking:*

[5]Working Group on Internet Banking, 2001 under the Chairmanship of S.R.Mittal.

You can bank from anyplace from anywhere, at any time, and regardless of the weather with mobile banking. The requirement of a computer or laptop with an internet connection is the most important disadvantage of internet banking. In the United States and Europe, this is certifiably not a significant hindrance, however in China and India, it is. Portable financial addresses this basic imperative of online banking by diminishing the client's need to just a wireless. Smartphone banking is a sort of banking and financial service that allows customers to access their accounts from their smartphones in real time. The use of a mobile phone for financial transactions is known as mobile banking. Mobile banking is a supplement to internet banking.

3. *Telephone Banking:*

Telephone banking entails dialling a phone number and listening to a recorded message before hitting the phone's corresponding buttons to access an account, transfer cash, seek statements, or request a cheque book.[6] It allows consumers to check their accounts at their leisure and do simple tasks without having to visit the bank. An automated voice response system is used in the telephone banking service. Its goal is to provide all consumers with a 24-hour service that is quick, convenient, and secure.

Accordingly, phone banking can be characterized as a protected, fast, and advantageous method for acquiring an assortment of administrations via telephone as opposed to visiting a branch, for example, account data, exchange execution, announcing a lost ATM card, requesting a really take a look at book, etc. Banking is feasible even while a person is on the go.

4. *Automated Teller Machine (ATM):*

Clients/Customers can set aside instalments, withdrawals, and other monetary exercises utilizing an ATM, which is a self-administration electronic machine. It's a positive step toward better customer service. At any time of day or night, customers can use the ATM. ATMs have given banks and other financial institutions a competitive advantage in conducting business. An ATM card, a plastic card with a magnetic strip that holds the client's



[6] Seema Kapoor and Deepak Dhingra, "Application of Information Technology in Banking" published in *E-banking in India- Challenges and Opportunities,* 106 (New Century Publications, New Delhi, 1st edition, 2007).

name, card number, bank information, validity period, and signature panel, is issued to the consumer.

Each card bearer is granted a private personal identification number (PIN). When a consumer wishes to use the card, he must insert it into the slot on the machine. The consumer enters his PIN once the card has been recognised. After confirming the clients' authentication, he must input the amount to be withdrawn. The output slot of the ATM spits out the amount of cash input for withdrawal by the customer after processing the transaction.

- **Forms of Electronic Payment System:-**

  Using an electronic payment system is a convenient way to make a purchase or pay for a service without having to carry cash or go through the process of writing out a check. The E-Banking service relies heavily on the electronic payment mechanism. Electronic payments claim to be the most advantageous method of completing cash-based transactions since they are the most convenient.

  The following are some of the payment mechanisms used in the electronic payment environment:

1. *Digital Cheque:*

   Digital cheques are electronic payment devices that leverage networking services to allow e-customers to issue digital cheques to e-merchant establishments to cover transactions conducted over the internet. Paper checks issued in a physical banking setting are analogous to digital cheques. The digital cheque system is run through the internet and has enough security built in.

2. *Electronic Cash:*

   Electronic cash, commonly referred to as digital money, is a type of payment method that is utilised in online banking and financial services. It's a secure and private online payment system that combines technological convenience with privacy and security. Electronic currency is a convenient way to pay for online purchases that combines the advantages of credit and debit cards and is only used by the account holder.

The owner or user must be identified and verified before electronic cash may be accepted. E-mint is the electronic cash issuing bank that is allowed to sign the electronic cash. E-cash security is ensured using security measures such as digital signature algorithms.

3. *Electronic Purse (E-purse):*

The "electronic purse" is a wallet-sized smart card with a programmable chip that saves e-money to be used in a virtual trading environment for making payments. In a virtual setting, the e-mint or a banker electronically loads money into an e-purse. It is utilised to complete any e-transaction payment. The user's authenticity is validated using a card vending machine located in the merchant's e-mall. It is a handy way of payment that allows you to pay your expenses for each transaction. When the value of an e-purse is exhausted, it is charged.

4. *Electronic Cards:*

The term 'electronic card' refers to an electronic card with a PIN that is used for online commerce transactions. The customer who e-shops, the e-merchant, the merchant's E-Banking institution, and the card issuing bank are the four entities that make up the electronic credit system. The merchant server, merchant bank, and card issuing bank are all involved in credit card transactions.

**LEGAL FRAMEWORK**

1. **Information Technology Act, 2000:**

The IT Act of 2000 is India's foremost regulation overseeing cybercrime and electronic business. This rule straightforwardly affects the activity of web based banking in India, and consequently it very well might be expressed that web banking can't be directed except if it is as per the IT Act 2000.



The following considerations highlight the importance of the IT Act of 2000 in the context of online banking:

- *Scrutinization of Documents:*

Any financial transaction needs the evaluation and storage of several papers, which are now saved and evaluated in an electronic format with online banking. The IT Act is the only piece of legislation that recognises these electronic documents.[7]

[7] Chapter III of The IT Act, 2000, No.21, Act of Parliament, 2000 (India).

- *Electronic Transaction:*

  The clause of the IT Act recognises every electronic transaction. Section 10-Aof the Act provides for the legitimacy and enforceability of an online transaction; subsequently, without the arrangements of the IT Act, no online transaction might be tried in a court.

- *Authentication:*

  The verification of this electronic information with the end goal of electronic banking ought to follow the provisions of this act.

- *Digital Signature:*

  In the event that the papers are marked electronically or carefully, they are controlled simply by the prerequisites of this demonstration. Subsequently, this act would address the issue of marking a record for Internet Banking.[8]

- *Privacy:*

  Internet banking would not have lasted if privacy and security had not been included.[9]

- *Data theft:*

  IT Act in Section 66 condemns an assortment and variety activities connecting with information stealing or hacking. A couple of instances of information theft incorporate hacking and inserting virus in to online system framework.

  The motivation behind the IT Act is to empower online business and e-administration, which are basic for the activity of online banking in India.

Following are some of the key provisions of the IT Act: -

1. Section 3(2): This section acknowledges just one kind of technology for authenticating electronic records (crypto function and hash function). In some countries, this strategy has been kept technology-neutral.
2. Section 4: This section gives legitimate acknowledgment to every electronic agreement and arrangements.
3. Section 72: It establishes a punishment in the event of a breach of privacy.



[8] Electronic Document.
[9] Penalized under Section 72 of The IT Act, 2000, No.21, Act of Parliament, 2000 (India).

4. Section 79: It safeguards communication network operators and shields them from liability in the case of unlawful behaviour on their connection.

## 2. Indian Penal Code, 1860:

The Indian Penal Code punishes a number of Internet banking-related offences. The IPC has several sections that safeguard Internet Banking-related frauds, thefts, and other crimes. Unsurprisingly, the Indian Penal Code has a number of sections that overlap with the IT Act of 2000. The following are a few of the provisions:

1. *Data Theft:*

Data theft, whether on web or not (online or offline), is included in the definition of theft under Section 378 of the IPC. Hacking, spreading malware, damaging information servers, and denying access to someone who has been authorised access are all methods for stealing data related with online banking. As a result, data security becomes critical. And the IPC prohibits such conduct in order to protect the interests of online banking customers. In India, data theft is also prohibited under Section 424 of the Indian Penal Code, which punishes anybody who aids or hides the data.

2. *Acquisition of a fraudulent transaction:*

In the event that an individual acquires the returns of taken merchandise through a web based financial exchange, he will be arraigned under Section 411 of the IPC and face a maximum sentence of 90 days in prison, a fine, or both. This IPC arrangement is equivalent to Section 66-B of the IT Act, which makes it illicit to get taken PC assets or correspondence hardware[10].

3. *Personation Fraud:*

Personation fraud is punishable under Section 411 of the IPC. The same is chargeable under Section 66-C of the IT Act[11]. Personation fraud refers to any individual who commits the offence of cheating using a computer.

4. *Mischief:*

[10] Information Technology Act, 2000: S.66-B.
[11] Information Technology Act,2000: S.66-C.

That anybody who injects/brings a virus into a system with malicious intent, damages the system, or restricts access to the person authorised to use the system is guilty of offence, which is punished by up to three months in jail, a penalty, or both u/s 425 IPC.

5. *Forgery:*

Forgery in Online transfers is possible by providing fraudulent electronic papers or other records.

Other illegal behaviours that are not punished under the IPC but are punishable under the IT Act are listed below. A few examples are:

The IPC doesn't punish an individual who charges the administrations/services he gives to the record of someone else by obstructing or controlling any system or network. Area 43(h) of the IT Act makes such a Punishable

- Attempting to tamper with a computer source document charged u/s 65 of the IT Act.[12]
- Banking puts a premium on protection while marking in, contributing passwords, and executing. Section 66E of the IT, Act[13] punishes Infringement of safety or security while managing on the online transfers.

**3. Additional Legislations:**

U/s 40A (3) of **Income Tax Act, 1961**: This section is accessible to the record client assuming the cash are sent through online transfers. This segment attempts to battle tax avoidance by oppressing any exchanges costing more than 20,000 to bank investigation.[14]

U/s 6 of **Negotiable Instrument Act, 1881**: The thoughts of Truncated Cheque and e-cheque were added. These checks are electronic negotiable instruments utilized in internet banking. These gadgets are expected to satisfy least security principles while utilizing advanced marks (which might be connected with biometric).[15]



U/s 11 of **Prevention of Money Laundering Act, 2002**: Each banking organisation and mediator must preserve a record of all transactions. This is true for all banks, regardless of

[12] Information Technology Act, 2000: S.17.
[13] Information Technology Act,2000: S.66E.
[14] Income Tax Act,1961: S.40A(3).
[15] Negotiable Instrument Act,1881: S.6.

whether they offer physical or online services. This regulation helps to prevent money laundering using the internet banking system.[16]

**Consumer Protection Act, 1986:** The objective of this Legislation is to safeguard the consumer rights. It is additionally relevant to banking administrations. This regulation shields issues, for example, protection, the mystery of buyer accounts, and the limitations of clients and banks with regards to internet banking.[17]

**Payment and Settlement Systems Act, 2007:**

The PSS Act of 2007 lays out the RBI as the administrative and administrative expert for instalment frameworks in India, as well as other related subjects. The RBI has given two guidelines under the PSS Act: The Board for Regulation and Supervision of Payment and Settlement Systems Regulation, 2008, and the Payment and Settlement Systems Regulations, 2008.

Assuming the framework supplier penetrates any areas of the Act or Regulations, neglects to consent to its requests/bearings, or abuses the agreements under which the authorization was given, the Reserve Bank has the position to pull out the authorisation.[18]

In light of a legitimate concern for the smooth activity of the instalment framework, the RBI has the position to coordinate an instalment framework or framework member to stop or halt from participating in any demonstration, exclusion, or course of lead, or to guide it to play out any demonstrations, as well as to give general headings.[19]

**JUDICIAL PRONOUNCEMENTS**

The aggrieved party guaranteed that his record was unlawfully charged inferable from the bank's ineptitude in **Umashankar Sivasubramaniam v. ICICI Bank**, a case heard by the Adjudicating Authority under the IT Act in Chennai. The occurrence, as indicated by ICICI, includes phishing, and the client is liable for documenting a FIR. The bank additionally contended that the case was not covered under the Information Technology Act of 2000. The Adjudicating Authority viewed ICICI bank blameworthy of abusing Section 85 of the IT Act,

[16] Prevention of Money Laundering Act, 2002: S11.
[17] Consumer Protection Act,1986.
[18] Payment and Settlement Systems Act, S. 8.
[19] Payment and Settlement Systems Act, Ss 17 and 18.

2000, as well as relevant provisions of Section 43A, and requested it to pay a fine of Rs. 12,85,000. The Adjudicating Authority viewed ICICI bank entirely liable of abusing Section 85 of the IT Act, 2000, as well as appropriate arrangements of Section 43A, and requested the bank to pay a fine of Rs. 12,85,000. In an allure documented with the Cyber Appellate Authority, ICICI bank was conceded a stay on the decision.

The Delhi High Court in **Avnish Bajaj v. State**[20], which tended to the criminal obligation of an organization specialist co-op, Baazee.com, for outsider information or data made accessible on their site. That's what the court held if Sections 67 and 85 of the IT Act, 2000 are perused together, it very well may be presumed that, under the guideline of considered criminal responsibility, a body of evidence can be made out against any overseer of an organization regardless of whether the organization isn't named as a denounced, gave the segment's fixings are met.

The aggrieved party in **Rishi Gupta v. ICICI Bank**[21], before the Consumer Disputes Redressal Forum in Bangalore, looked for a request guiding the contrary party bank to discount Rs. 230,000/, in addition to premium of 24% per annum, which the complainant had lost because of the contrary party's supposed carelessness, as well as a request guiding the bank to pay Rs. 100,000/ - as harms for carelessness of administration. The District gathering excused the protest, expressing that the complainant had misbehaved in revealing touchy information of his internet banking to an outsider in light of an email purportedly sent by the contrary party bank, without first checking with the contrary party bank.

In **M/s Pachisia Plastics v. ICICI Bank Ltd**.[22] it was brought before the Consumer Disputes Redressal Forum in Bangalore, claiming insufficiency of administration with respect to the ICICI Bank after a measure of Rs. 1,18,000 was unlawfully deducted from the complainant's record through net banking. The objection was dismissed by the Forum in light of the fact that the bank had neglected to offer satisfactory support.



In **K. Thagyarajan v. ICICI Bank**[23], the complainant guaranteed that his web-based ledger was attacked and a measure of Rs. 77,000/ - was unlawfully moved to one more record by

[20] 150(2008) DLT 769.
[21] CC No. 514 of 2010.
[22] CC No. 1059 of 2008.
[23] CC No. 2969 of 2009.

obscure individuals before the Consumer Disputes Redressal Forum in Bangalore. The grievance guaranteed that the contradicting party bank offered unfortunate support and mentioned a discount of the cash in addition to premium, as well as remuneration of Rs. 300,000/ - . The grumbling was excused since the aggrieved party had given the secret phrase and client id for web-based banking to outsiders, showing that there was no shortfall in help on the contradicting party bank.

**ISSUES AND CHALLENGES IN ELECTRONIC FUND TRANSFER**

1. *Security and Privacy Issues:*

   Security is the main hindrance to online/internet banking it is a major risk aspect for the system and one of the top concerns for regulators. Human or non-human, accidental or unintended security problems can be classified as internal or external.

   The problem of security entails the use of globally recognised technologies, encryptions/decryptions, and the verification of digital signatures, among other things. Internet banking is an obvious target for hackers because of the quick access to financial accounts. One of the most prevalent techniques of stealing and obtaining personal information from clients is 'phishing.'

   In today's world, privacy is essential for humanity and mankind. In addition, a lack of securitized transactions can lead to data loss, theft, tampering with customers' or banks' information, and other crimes, such as money laundering. There have been several occasions when security breaches have resulted in the disclosure of sensitive data, and so we may conclude that security concerns are the primary impediment to India's complete adoption of online banking.

2. *Legal Issues:*

   Because the internet is a public realm with no geographical boundaries, it poses questions about legal jurisdiction, legal standards for electronic trade, commerce and transactions, and so on.

3. *Supervisory and Operational Issues:*

   Operational risk is the danger of direct or indirect loss caused by inadequate or failed inner

cycles, peoples/people/individuals, and systems, as well as outside occurrences.[24] They are also known as Transactional Risks and are the most prevalent risk connected with internet banking. Operational hazards include inaccuracies in transaction processing, contract non-enforceability, illegal access, and penetration into the bank's system, among others.

This type of risk is usually caused by poor banking software design, other technical inefficiencies, human carelessness, employee fraud, and so on[25]. Although there is a fine border between security and operational challenges, they are frequently used interchangeably. To confirm the authenticity of an instrument, security processes such as PIN numbers, Customer Relationship Numbers, Passwords, OTPs, Account Numbers, and so on are used.

Different countries have established different criteria for determining the validity of a transaction. The Information Technology Act of 2000 in India [26]stipulates that any subscriber may use a Digital Signature to validate his electronic record. The problem with authentication is that the Act only acknowledges one type of technology for authenticating electronic documents (the asymmetric cryptosystem), which creates questions about whether the legislation recognises alternative financial authentication methods. Other nations' legislatures have chosen to keep the authentication method technology neutral.

**RECOMMENDATIONS AND SUGGESTIONS**

- Banks must protect the privacy and security of their customers' accounts, as well as adopt appropriate risk management steps to prevent hacking and technological malfunctions.
- Banks should ensure that sufficient security infrastructure is in place, such as using at least 128-bit SSL for browser-to-web-server interactions and encrypting sensitive data in transit inside the organisation, such as passwords.
- Banks should utilise the most recent software versions or upgrade old software to improve security and management and eliminate bugs and weaknesses.
- Banks should focus their efforts on offering greater technical assistance to their consumers.
- To avoid data loss, banks should ensure that a comprehensive data backup mechanism is in place.



[24] Basel Committee on Banking Supervision Consultative Document Operational Risk, Jan.31, 2001.
[25] S.N GUPTA, THE BANKING LAW, 112, (14th Edition, 2015).

[26] IT Act, 2000: Section 3(2).

## CONCLUSION

Each country's financial framework has a crucial capacity to play in its economy. The financial framework as it exists presently has gotten progressively and increasingly complex, with many administrations coming about because of specialized headways that have changed the entire financial framework from a manual-concentrated business to one that is exceptionally robotized and innovatively based. Presently, online banking permits you to carry on with work from anyplace and whenever. Online Banking has now turned into a virtual gift, as it has settled various troubles in the financial business and has demonstrated advantageous to both banks and their customers.

In terms of variety and creativity, the Indian financial sector has seen a significant transition throughout time. The present payment system must be turned into a future-proof infrastructure. This may be accomplished through standardisation, interoperability, consolidation, the construction of a common infrastructure, and sharing, all of which are linked to product and delivery channel improvements. More capacity building in terms of both systems and human resources in the sector and the RBI is required to move this process ahead. In addition to the requirement to avoid and restrict cybercrime and security concerns, special attention is necessary to maintain flawless business continuity strategies.