CRITICAL ANALYSIS OF LEGAL FRAMEWORK REGULATING INTERNET BANKING IN INDIA

Madhura Pitre, Modern Law College, Pune

ABSTRACT:

Internet banking has become an essential part of modern banking services. Internet banking, also known as online banking or e-banking, has become an increasingly popular way for customers to access banking services and manage their accounts. While it offers convenience and flexibility to customers, it also presents several challenges and risks. The legal framework for internet banking in India includes a range of laws and regulations aimed at ensuring the safety and security of customer data and transactions. Although India has a legal framework to regulate internet banking and protect customers from fraud, still number of frauds are reported every day. This present paper tries to discuss the major issues in internet banking and legal framework which tries to overcome these issues. Further this paper also discusses problems in legal system that have created challenges in regulating internet banking in India and recommend few suggestions to deal with this issue.

Introduction:

Technology has brought about a complete paradigm shift in the functioning of banks and delivery of banking services. Gone are the days when every banking transaction required a visit to the bank branch. Today, most of the transactions can be done from the comforts of one's home and customers need not visit the bank branch for anything. Technology is no longer an enabler, but business driver. The use of information technology in banking is now inherent in banking industry. The growth of the internet, mobiles and communication technology has added a different dimension to banking. The information technology (IT) available today is being leveraged in customer acquisitions, driving automation and process efficiency, delivering ease and efficiency to customers. Automated Teller Machines (ATMs), mobile banking and online bill payments facilities to vendors and utility service providers have almost obviated the need for customers to visit a branch. The change has been very productive.[1]

Defining 'Internet Banking' and its features

The word 'Banking' has been defined in the Banking Regulation Act, 19493 as 'the accepting, for the purpose of lending or investment, of deposits of money from the public, repayable on demand or otherwise, and withdrawal by cheque, draft, order or otherwise'. Thus banking means an industry that deals with cash, credit and other financial instruments. The bank accepts deposits from its account holders and uses those deposits in lending loans for the purpose of investment and earns interest in return.[2]

"Internet banking" refers to systems that enable bank customers to access accounts and general information on bank products and services through a personal computer or other intelligent device. Internet banking products and services can include wholesale products for corporate customers as well as retail and fiduciary products for consumers.[3] Most public sector banks are already offering internet banking services, while others are at various stages of implementation.

Features of internet banking:

1. Internet banking is the predominant mode of e-banking. It has made banking

[1] Dr. B.N. Patel, MCQ ON BANKING LAW | 5. Technology and Banking in India
[2] Rohit Jain, Legal Framework of Internet Banking in India, 4, International Journal of Law Management & Humanities, 699, 699, (2021)
[3] Sangeetha Mugunthan, The Dual Facades of Internet Banking : Perspectives on Banker - Customer Relationship, AIRONLINE, CLC 2008

personalised and customised.

2. It enables providing general purpose information to customers through bank's websites, electronic transfer of information through passwords, and fully electronic transactional systems, which allows bi-directional transactional capabilities and requires high degree of security and control.[4]

3. Traditional geographic restrictions have been eliminated by internet banking because customers can now obtain financial services from any location without physically visiting the bank. However, it is important to highlight that this aspect of online banking has created a legal quandary over the jurisdiction or regulatory framework to which this problem should be treated.

4. Both the bank and the consumer find it to be cost- and time-efficient, and it makes transactions possible 24/7, including on holidays.

Reserve bank of India guidelines on Internet Banking

Reserve Bank of India had set up a Working Group on Internet Banking to examine different aspects of Internet Banking which focused on three major areas such as technology and security issues, legal issues and regulatory and supervisory issues. Reserve Bank of India, after having accepted the recommendations has issued following guidelines on 14th June 2001 for implementation by commercial banks:

a) All banks, who propose to offer transactional services on the Internet should obtain prior approval from Reserve Bank of India.

b) Only such banks which are licenced and supervised in India and have a physical presence in India will be permitted to offer Internet banking products to residents of India. Thus, both banks and virtual banks incorporated outside the country and having no physical presence in India will not, for the present, be permitted to offer Internet Banking services to Indian residents.

[4] Bimal N. Patel, Banking Law and Negotiable Instruments Act | 6. Technology and Banking: Prateek Kumar & Roopali Gupta

c) Overseas branches of Indian banks will be permitted to offer Internet Banking services to their oversea customers subject to their satisfying, in addition to the host supervisor, the home supervisor.[5]

This notification of 14th June 2001 was amended by RBI notification dated 20.07.2005, where the need for the approval of RBI was scrapped off, the following were the minimum benchmarks of security set up by the RBI:

a) Highly encoded 128 Bit Security Socket Layer based digital signatures for authentication purposes. Every bank should have Security Officer solely dealing with information technology and shall work towards the execution of the rules made under the IT Act, among other things, the Board of Directors shall approve the security policy that is adopted by the bank.

b) At that time login id, password, biometric verification were new notions, hence the banks were asked to adapt to such new concepts wherein the bank must make sure that Internet and Digital Banking System respects the security and privacy by maintaining a line of proxy server-based firewall. All the security structures were to be tested before any kind of Internet Banking facility was available, whereas the upgradation, bug removal and other security software were deemed necessary to be installed.

c) Any security fissure which might open up during the E-banking must be reported and taken care of at the earliest possible opportunity and future policies should be framed while keeping in mind security fissures that are incurred from time to time. Meanwhile, the burden lies upon the bank to keep both encoded and decoded records of all the transactions and messages received during e-transactions.[6]

Legal framework of Internet Banking in India[7]

Banking in India is majorly regulated by the Banking Regulation Act, 1949, and the Reserve Bank of India Act, 1934, and the electronic records & systems are governed by the provisions contained in the Information and Technology Act, 2000 as amended in 2008. Internet Banking

[5] R. N. Chaudhary, Banking Laws, 409 (Central Law Publication 2022)
[6]https://blog.ipleaders.in/the-legal-structure-of-e-banking-in-india/#The_legal_structure_of_e-banking_in_India (last visited on 09/09/2023)
[7] Rohit Jain, Legal Framework of Internet Banking in India, 4, International Journal of Law Management & Humanities, 699, 699, (2021)

is not a separate business, it is just the banking being used through electronic channels, and it is just an additional facility being provided by the banks. There are several enactments controlling internet banking in India. A few of those legislations are: The Information Technology Act, 200, The Banking Regulation Act, 1949, Indian Contract Act, 1872, etc. Let us look at the provisions of all these major banking enactments.

1) **Information Technology Act, 2000**

The Information Technology Act, 2000 is a primary law dealing with cyber-crimes and Electronic Commerce in India. This act have a direct bearing on the working of the internet banking in India and thus it can be said that Internet banking cannot be operated without being in conformity with the IT Act 2000.

Following are the points which highlight the importance of Information Technology Act, 2000 in regards to internet banking:

a) Scrutinization of Documents: Any banking transaction requires scrutinization and retention of various documents and in internet banking these documents are retained and scrutinized in electronic form. The legal recognition to these electronic documents is given by the IT Act only.

b) Electronic Transaction: Every transaction entered electronically is recognized by the provision of the IT Act. Section 10-A of the Act gives validity and enforceability to an electronic transaction, and thus without the provisions of IT Act no internet banking transaction can be challenged in the court of law.

c) Authentication: Authentication of these electronic records for the purpose of electronic banking should be in accordance with the provision of this act.

d) Digital Signature: If the documents are signed electronically of digitally it is governed according to the provisions of this act only. Thus, this act would satisfy the signing of a document for the purposes of Internet Banking.

e) Privacy: Privacy is very important in internet banking because if privacy and security wouldn't had been there, Internet banking may not have survived.

f) Data theft: Section 66 of the IT Act penalizes a number of acts relating to theft of done on computer system, few ways in which data theft can be done are: hacking, introducing and spreading viruses through computer networks, etc.

g) The object of the IT Act is to facilitate e-commerce and e-governance which are important for the functioning of Internet banking in India. By looking at the above points it can be said that the Information Technology Act, 2000 has laid down the basic legal framework conducive to the Internet banking in India. And thus accordingly a comprehensive way needs to be adopted so as to bring uniformity and harmony between the provisions of the IT act and the guidelines issued by the Reserve Bank of India.

Few of the important provisions of the IT Act are as follow: -

i. Section 3(2): This section recognizes only one particular technology (crypto function and hash function) as a means of authenticating electronic records. This approach has been kept technology neutral in various nations.

ii. Section 4: This provision gives legal recognition to all the contracts and agreements made in electronic form.

iii. Section 72: It provides for the penalty in case of privacy breach

iv. Section 79: It provides immunity to the network service providers and excludes them from liability in case of any illegal activity committed through their network.

In January 2011, RBI constituted G Gopalakrishna Working Group to review the security of Electronic Banking in India. The committee on April 2011 notified few changes which constitute the current regulatory guidelines.

2) Indian Penal Code, 1860

Many of the Internet Banking related crimes are penalized by the Indian Penal Code. There are various provisions of IPC which protects Internet Banking related frauds, theft, etc. There are several provisions in the Indian Penal Code that overlaps the IT Act, 2000. Few of those provisions are discussed below:

a) Data Theft: As defined under Section 378 of IPC, theft also includes theft of data online

or otherwise. There are a number of ways in which the data relating to internet banking can be stolen like for example: hacking, spreading viruses, destroying computer systems, denying access to a person authorized. And thus protection of data becomes crucial. And IPC bars such activities protects the interest of internet banking users. Section 424 of IPC also bars data theft in India by punishing the person who assists or conceals the data.

b) Receipt of a stolen property: If any person receives the furtherance of any property stolen from an internet banking transaction, he shall be held liable u/s 411 of IPC and shall be punished with imprisonment up-to 3 months or with fine or with both. This provision of IPC is similar to Section 66-B of the IT Act, which provides punishment for dishonestly receiving stolen computer resource or communication device.

c) Cheating by Personation: Section 411 (Dishonestly receiving stolen property) of IPC provides punishment for or any act committed through cheating by personation. Section 66-C of IT Act also punishes the same. Any person who commits the offence of cheating by means of computer is said to do Cheating by Personation.

d) Mischief: It is needless to say that any person who, with a wrongful intention, introduces viruses into computer system, damages the computer system or denies the access to the person authorized to use that system, shall be liable for mischief, which is punishable under Section 425 of IPC with imprisonment up-to 3 months or with fine or with both.

e) Forgery: In Internet Banking Transactions forgery can be done by giving false electronic documents or other records.

There are a number of other criminal activities which the IPC doesn't punish, but are punishable under the IT Act. Few of them are:

i. IPC doesn't punish a person who charges the services availed by him to the account of some other person by tampering or manipulating any computer system, or computer network. Such an act is punished u/s 43(h) of the IT Act.

ii. Tampering with computer source document. To a certain extent it is punished u/s 409 of IPC but it is not extensively been described there. And thus section 65 of the IT Act

deals with it.

iii. Violation of Security/Privacy while transacting online: Punishable u/s 66E of IT Act. Privacy while logging, entering password, transacting, is very important in Internet Banking.

iv. Preservation of Intermediaries (Banks in our case): Section 67 requires an 'intermediary' to preserve and retain all such information that the central government prescribes. This provision was challenged before the court in the case of Shreya Singhal vs. Union Of India, wherein the court affirmed the validity of this section.

3) Other Legislations

a) Income Tax Act 1961:

As per Section 40A(3) the benefit of this section is available to the account holder only when the amount is transferred through internet banking or through a cheque. This section is intended to prevent tax evasion and to bring all the transactions above 20,000 under the preview of the bank[8].

b) Negotiable Instrument Act, 1881:

By Section 6 of the Act, the concept of Truncated Cheque and e-cheque was added. These cheques are negotiable instruments in electronic format which are a part of internet banking. All these instruments are required to maintain minimum safety requirements with the use of digital signatures (which may be linked with biometric)[9].

c) Prevention Of Money Laundering Act, 2002:

Section 11 imposes a duty on every financial institution and intermediary to maintain a record of every transaction. This applies to all the banks whether offering physical or internet services. This provision helps the prevention of money laundering from taking place through the internet banking.[10]

[8] Income Tax Act 1961, Section 40A (3), 43 Act of Parliament 1961 (India)
[9] Negotiable Instrument Act, 1881, Section 6, 26 Act of Parliament 1881 (India)
[10] Prevention of Money Laundering Act, 2002, Section 11, Act of Parliament 2002 (India)

d) Consumer Protection Act, 2019:

This act aims to protect the interests of the consumers. It is also applicable to Banking Services as well. The issues such as privacy, the secrecy of consumer's accounts and the rights and liabilities of customers and banks, etc. in respect of internet banking are protected through this act[11].

e) State Bank of India Act, 1955

Section 44 provides for a secrecy clause by virtue of which, the bank as a whole and its directors, local boards, auditors, advisers, officers or other employees of the State Bank are obligated as to fidelity and secrecy, by a declaration in prescribed form. It provides that, the State Bank shall observe, except as otherwise required by law, the practices and usages customary among bankers, and, in particular, it shall not divulge any information relating to or to the affairs of its constituents except in circumstances in which it is, in accordance with the law or practice and usage customary among bankers, necessary or appropriate for the State Bank to divulge such information[12].

Internet banking fraud:

Internet Banking Fraud is a fraud or theft committed using online technology to illegally remove money from a bank account and/or transfer money to an account in a different bank. Internet Banking Fraud is a form of identity theft and is usually made possible through techniques such as phishing.

Legal Remedies for internet banking fraud:

1. Information Technology Act of 2000:

The first step is to notify the bank as soon as possible. The bank must take reasonable steps to guarantee that its customers have access to secure online banking. The bank must install CCTV cameras in its offices and ATMs, warn consumers of any transactions from their accounts via email and SMS alerts, track irregular or unexpected transactions, and so on. A person who is

[11] Consumer Protection Act,2019, No.35 of 2019 (India)
[12] http://elplaw.in/wp-content/uploads/2018/08/Data-Protection-26-Privacy-Issues-in-India.pdf last visited on 09/05/2023

a victim of online banking fraud can file a complaint with the Adjudicating Officer under Section 46 of the Information Technology Act, 2000, alleging that the bank failed to implement appropriate security measures. Banks and other intermediaries that do not adopt acceptable security measures for safe banking are required to provide adequate compensation to customers, according to Section 43A of the Information Technology Act of 2000. The bank must demonstrate that it took adequate steps to prevent any illegal or unauthorized transactions.

2. RBI Ombudsman Scheme:

If the bank fails to take action after submission of the complaint regarding deficiency of service, the consumer can lodge complaint against the bank based on RBI Ombudsman Scheme, whereas before approaching the ombudsman, the consumer must file the complaint with the bank. Only after bank fails to respond within 30 days from the lodgement of the complaint or if the bank rejects the complaint wholly or partially the consumer can approach the Ombudsman. The RBI Ombudsman Complaint can be made through the online portal at www.bankingombudsman.rbi.org.in.

3. Cyber Cell:

For Online transactions frauds, it is important to lodge a complaint in cyber cell in the nearest area, if cyber cell is not available the complainant can lodge a complaint in the nearest Police Station explaining the complete incidence about the unauthorized transaction and loss of money by unknown person. While lodging complaint it is important to collect 6 months bank statement of the concern bank, to make a copy of SMSs received related to the alleged transaction, to take ID proof and address proof as shown in the bank records. Further, complain can be lodged through cybercrime online portal at https://www.cybercrime.gov.in/Default.aspx [13]

Despite having these legal remedies, the value of the average banking fraud involving cards and internet banking was up 8.5 per cent to Rs 34,802 in 2021-22 (FY22), even as the number of such instances declined year-on-year.

[13] Dr. Kumutha Rathna, Online Banking Fraud in India, 4, 295, 297 (2016)

There were 65,045 such instances of fraud in FY22, according to data released in the Lok Sabha (LS) on 13th March 2023.[14]

Issues in Internet banking:

After looking at the distinguishing features of Internet Banking, we can say that Internet banking has increased the ease of doing business in India. However, there are certain issues in internet banking. Those are as follows:

1. Jurisdictional issues:

Internet banking is a cross-border activity that can pose jurisdictional challenges for regulators. It can be challenging to determine which regulator has jurisdiction over internet banking services that are provided by banks located in different states or countries.

2. Data Privacy:

Data privacy is a significant issue in internet banking. Banks collect and store sensitive customer data, including personal and financial information, which can be misused if not adequately protected. Lack of securitized transactions may result in loss of data, theft, tampering with customers or bank's information, etc. which may result in money laundering, and other frauds. There have been many instances wherein security breach has resulted in leakage of important data and thus, we can say that security issues are the major roadblock in a fully-fledged adoption of internet banking in India[15].

3. Security:

Security is at the root of technology centric banking. Internet has made communication more efficient, but not necessarily safe and secure. Today the world is grappling with issues such as computer virus, hacking, etc. It is important that these issues are addressed effectively.[16]

[14] https://www.business-standard.com/article/finance/rise-in-average-value-of-card-internet-banking-frauds-shows-data-123031401044_1.html last visited on 09/05/2023
[15] Rohit Jain, Legal Framework of Internet Banking in India, 4, International Journal of Law Management & Humanities, 699, 699, (2021)
[16] Bimal N. Patel, Banking Law and Negotiable Instruments Act | 6. Technology and Banking: Prateek Kumar & Roopali Gupta

4. Authentication issue:

In order to verify the authenticity of an instrument, security measures such PIN numbers, customer relationship numbers, passwords, one-time passwords, account numbers, etc. are frequently used. Different nations have established several standards to determine whether a transaction is legitimate. According to India's Information Technology Act of 2009, any subscriber may use a digital signature to verify the authenticity of his electronic record. The problem with authentication is that the Act only specifically recognises one technology (the asymmetric cryptosystem) for authenticating electronic documents, which casts ambiguity on whether the legislation recognises other banking authentication systems or not. Other nations' legislatures have kept the verification process tech-neutral.

Legal issues in regulating internet banking in India:

1. The lack of a comprehensive data privacy law in India has created challenges for regulators in protecting customer data and regulating its use by banks. In the case of District Registrar and Collector, Hyderabad v Canara Bank[17], the Hon'ble Supreme Court clearly held and recognized that right to privacy of person extends to documents of the person/customer which are with bank and must remain confidential. Accordingly, the Hon'ble Supreme Court upheld the order of the High Court, which has invalidated Section 43 of the Stamp Act (as amended in Andhra Pradesh), which empowered the Collector to inspect registers, books and records, papers, documents, and proceedings in the custody of any public officer 'to secure any duty or to prove or would lead to the discovery of a fraud or omission'.[18]

2. Compliance issues: Internet banking is subject to several legal and regulatory requirements, including data protection laws, customer privacy policies, and cybersecurity guidelines. Compliance with these requirements can be challenging for banks, particularly those that operate across multiple jurisdictions. The lack of harmonization of regulations across different jurisdictions has created challenges for banks in complying with these requirements.

[17] District Registrar and Collector, Hyderabad v Canara Bank (2005) 1 SCC 496
[18] http://elplaw.in/wp-content/uploads/2018/08/Data-Protection-26-Privacy-Issues-in-India.pdf last visited on 09/05/2023

3. Legal Framework: The legal framework for regulating internet banking in India is complex and fragmented. There are several laws and regulations that apply to internet banking, including the IT Act, the RBI Act, the Banking Regulation Act, and the Payment and Settlement Systems Act. The lack of a comprehensive and harmonized legal framework has created challenges for regulators in ensuring effective regulation of internet banking.

4. Under the present regime there is an obligation on banks to maintain secrecy and confidentiality of customers accounts and the risk of banks not meeting this obligation is high on the account of several factors.

5. In Internet banking scenario there is very little scope for the banks to act on Stop payment instructions from the customers. Hence, banks should clearly notify the customers the time frame and the circumstances in which any stop payment instructions could be accepted.

Suggestions[19]:

Technology and security standards:

a) Banks should designate a network and database administrator with clearly defined roles.

b) Banks should have a security policy duly approved by the Board of Directors with segregation of duty of Security officer/Group dealing exclusively with information systems security and Information Technology Division which actually implements the computer systems. Further, Information System Auditor should audit the information system.

c) Banks should introduce logical access controls to data, systems, application software, utilities, telecommunication lines, libraries, system software, etc.

d) At the minimum, banks should use the proxy server type of firewall so that there is no direct connection between Internet and bank's system.

[19] R. N. Chaudhary, Banking Laws, 409 (Central Law Publication 2022)

e) Physical access controls should be strictly enforced. Physical security should cover all the information systems and sites where they are housed, both against internal and external threats.

f) Banks should have proper infrastructure and schedules for backing up data. The backed-up data should periodically tested to ensure recovery without lose of transactions in a time frame as given out in bank's security policy.

g) All applications of banks should have proper record keeping facilities for legal purposes. It may be necessary to keep all received and sent messages both in encrypted and decrypted form.

Regulatory and supervisory standards:

a) Banks will report to Reserve Bank of India about failure of security systems and procedure and the latter, at its direction, may decide to commission special audit/inspection of such banks.

b) Banks must make mandatory disclosure of risks, responsibilities and liabilities of the customers in doing business through Internet through a disclosure template.

c) The Internet banking services should only include local currency products.

d) The products should be restricted to account holders only and should not be offered in other jurisdictions.

Conclusion:

Banking System always has an important role to play in the economy of every nation. The banking system as it stands today has become more intricate with different services stemming from reliance on technological changes which has shaped the complete banking system from a manual intensive industry to a highly automated and technologically dependent industry. Now the internet banking enables the business anywhere any at any time. Internet Banking has now become a virtual blessing as it eliminates few of the problems in the Banking sector and had been proved advantageous to both, the banks and its customers.

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. 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. For customers 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. The legal issues of Internet banking in India must be taken more seriously by all stakeholders especially the Indian banks. However, better results cannot be achieved till cyber security requirements made mandatory on the part of Indian banks.

References:

1. R. N. Chaudhary, Banking Laws, 409 (Central Law Publication 2022)

2. Bimal N. Patel, Banking Law and Negotiable Instruments Act | 6. Technology and Banking: Prateek Kumar & Roopali Gupta

3. Rohit Jain, Legal Framework of Internet Banking in India, 4, International Journal of Law Management & Humanities, 699, 699, (2021)

4. Dr. B.N. Patel, MCQ ON BANKING LAW | 5. Technology and Banking in India

5. Sangeetha Mugunthan, The Dual Facades of Internet Banking : Perspectives on Banker - Customer Relationship, AIRONLINE, CLC 2008