Digital Banking Revolution: Legal Perspectives in the Indian Context

Tousif Khan, Ll.M., National Law University and Judicial Academy, Assam.

Abstract

Technology's introduction into the banking industry has completely changed the way financial services are provided, guaranteeing previously unheard-of accessibility and ease. Technological developments have revolutionized traditional banking, empowering consumers and growing the financial ecosystem through anything from mobile banking applications to AI-powered customer service. Examining how technological advancements such as digital wallets, biometric security measures, and real-time financial transfers have changed consumer interactions, this article explores the complex effects of technology on banking services. It also draws attention to the legal structures that control these developments, guaranteeing consumer protection, security, and openness in the digital era. From the standpoint of the consumer, technology has made financial transactions easier, but it also presents problems, including privacy issues and cybercrime. The 2021 Truecaller Global Scam Report makes a shocking discovery that highlights the negative aspects of technology abuse in financial scams. For stakeholders, this research represents a wake-up call to improve protections and address risks.

Keywords: *Privacy Concerns, Technology, Legal Frameworks, Financial Scams, Innovation.*

INTRODUCTION

The integration of technology with banking services has revolutionized the financial sector, giving rise to internet banking, which offers convenience, efficiency, and real-time access to banking services. In India, the rapid growth of digital platforms and technological advancements has transformed the traditional banking model, enabling customers to perform a wide range of financial transactions from the comfort of their homes. Internet banking, often referred to as online or e-banking, has emerged as a critical component of modern banking systems, reshaping customer experiences and banking operations.

With the growing reliance on internet banking, several legal, regulatory, and security issues have surfaced, necessitating a robust legal framework to address concerns around data protection, fraud prevention, and consumer rights. The regulatory landscape in India is shaped by a variety of laws, including the Information Technology Act, 2000, and guidelines from the Reserve Bank of India (RBI), aimed at promoting secure and efficient online banking transactions.

As the internet banking sector continues to expand, the intersection of technology and law becomes increasingly crucial. This analysis seeks to explore the legal aspects governing internet banking in India, examining the evolution of internet banking, the regulatory framework, and the challenges posed by cybersecurity threats, privacy concerns, and the evolving nature of digital finance. The legal analysis also delves into the adequacy of existing laws in fostering innovation while ensuring consumer protection and financial stability in the digital age.

UNIFIED PAYMENTS INTERFACE

Unified Payments Interface (UPI) integrates multiple bank accounts into a single mobile app, allowing seamless fund transfers, merchant payments, and peer-to-peer transactions. The system was piloted by NPCI with 21 banks on April 11, 2016, under the leadership of RBI

Governor Dr. Raghuram G Rajan. Banks began launching UPI-enabled apps on the Google Play store from August 25, 2016.[1]

Unified Payments Interface With UPI, one could manage as many bank accounts as he wants from a single mobile application, and perform fund transfers, merchant payments, and peer-to-peer transactions quite easily. Each bank provides its own UPI app on Android, Windows, and iOS platforms.[2]

In the case of ***American Express Bank Ltd. v. Girdhari Jewellers (P) Ltd.,***[3] (Absence of issue date on credit cards and its legal validity.) Here, American Express (Amex) and Popular Jewellery House entered into an agreement to accept Amex credit cards when customers purchased items from the shop. In two instances in the year 1997, two customers purchased jewellery and produced forged Amex cards, which the shop verified and even obtained approval for the transactions. Later, Amex refused to make payments since the cards were forged. The shop thus complained to the MRTP Commission, which ordered in favour of the shop as it had followed the procedure laid down. The court found that there was no valid reason for Amex to withhold payment as the shop acted properly and was unaware that the cards were forged. The court even pointed out that investigations into the fraud were going on but did not implicate the shop regarding the forged card issue.

In the case of ***B.V.S.P. Choudary v. Station House Officer,***[4] (Directions for recoveries of credit card dues.) The RBI thus laid down guidelines for credit card recoveries. It proscribed criminal force or harassment for such recoveries. A writ was filed in the instant case because some recovery agents of HDFC Bank allegedly kidnapped a scientist, Prof. C.L.N. Murthy, for dues. The petitioner submitted that the agents, in conspiracy with police officers, got papers signed under threat from Murthy. The police rebutted this and contended that Murthy voluntarily approached for help about harassment by the bank.

[1] Unified Payments Interface (UPI) <https://www.npci.org.in/what-we-do/upi/product-overview >: last accessed 13-10-2025
[2] CASHLESS INDIA - Unified Payments Interface, <http://cashlessindia.gov.in/upi.html >: last accessed 13-10-2025
[3] American Express Bank Ltd. v. Girdhari Jewellers (P) Ltd.,W.P. (C) 9559/2004, decided on 13-9-2006 (Del)
[4] B.V.S.P. Choudary v. Station House Officer, AIR 2008 AP 147

The court insisted that every bank should adhere to the fair debt collection practices and a cardholder can approach the law if he is being subjected to intimidation or harassment.

INDIAN LEGAL REGIME IN GOVERNING OF BANKING SYSTEM

a) Internet Banking In Relation To Bharatiya Nyaya Sanhita, 2023

BNS punishes the offenders for an act done with a guilty mind, which is to say, "no act is an offence without a guilty mind." Though fraud as such is not considered a different offense in itself, fraud acts, and internet banking is one included in that category, are punishable under the BNS. The relevant sections of the BNS can indeed be applied to internet banking offenses despite the sophistication of online fraud, specially under Chapter XVII, which deals with crimes relating to money.

Thus, the following sections are applicable in such a situation:

1. ***Theft***[5]: Theft is the dishonest taking of another's movable property out of possession without his consent. Once property attached to the earth is detached, it becomes subject to theft. Moving can be by removing obstacles or sending an animal in motion. Consent may be explicitly or implicitly given by the owner or a person authorized to give it.

2. ***Extortion***[6]: Extortion sees a person putting someone in fear of injury with the view to getting property or other valuables dishonestly. Punishments vary depending on the degree of threats and run from seven to up to ten years imprisonment, with or without fines. The threat of death, grievous harm, or severe criminal accusations attract higher sentences. It is also punishable to attempt making a person experience such type of fear.

[5] Sec. 303
[6] Sec. 308

3. ***Dishonest misappropriation of property***[7]***:*** This section defines the offense of dishonest misappropriation of movable property, which is punished with imprisonment from six months to two years and a fine. It states that even temporary misappropriation amounts to the offense. If a person finds unclaimed property and takes it with an intention of restoring it to the owner, he does not commit the offense of dishonesty. However, if he appropriates the property for his own use, having known or having reasons to believe, the rightful owner can be found by reasonable means and without genuinely attempting to find him, he commits the offense. As to what are "reasonable means" or "reasonable time" to find the owner is a question of fact. It is sufficient that the finder does not believe the property to belong to him or cannot in good faith believe the real owner cannot be found.
4. ***Criminal breach of trust***[8]***:*** Criminal breach of trust is dishonest misappropriation or conversion by a person entrusted with property or of legal directions or contracts express or implied regarding the trust. Employers who deduct employee contributions for Provident or Pension Funds, or for Employees' State Insurance, without depositing them in the respective funds are said to have dishonestly utilized such contributions in contravention of law.
5. ***Cheating*****:** Fraudulently or dishonestly inducing a person to deliver property etc.[9] This can be done by the use of electronic means as well hence, it is applicable along with the relevant sections of the IT Act.
6. The term *"forgery"* has been defined in relevance to the electronic record as well, *i.e.* the offence of forgery is said to be committed when anyone makes not only a false document but also a false electronic record.[10] The term *"making of false document"* also includes affixing electronic signature on any electronic record.[11]
7. Use of forged documents or electronic record and use of such forged document as genuine. [12]The IT Act, 2000 has amended the original sections to add "electronic documents" in the definition of forged documents.

[7] Sec. 314
[8] Sec. 316
[9] Sec. 318 (1) & 318(4)
[10] Sec. 336
[11] Sec. 335(*iii*)
[12] Sec. 340

*b) **Prevention of Money Laundering Act, 2002***

Money laundering is a large-scale problem in India, generally related to politicians, corporations, and the stock market. Investigations are done by the Enforcement Directorate and Income Tax Department. Out of the total tax dues of Rs 2.48 lakh crores, Rs 1.30 lakh crores pertain to money laundering and securities scams. To tackle this, India passed the Prevention of Money Laundering Act, 2002. The Act applies to all financial institutions, banks, mutual funds, insurance companies, and their intermediaries. Even the RBI, SEBI, and IRDA come within its ambit[13]

The offence of money laundering.— Anyone who directly or indirectly tries to participate in, assists, or is involved in any process related to the proceeds of a crime—such as hiding, possessing, acquiring, using, or presenting it as clean property—will be guilty of *"money laundering".* A person will be guilty of money laundering if they are involved in any of the following actions related to criminal proceeds:

- Hiding,
- Possessing,
- Acquiring,
- Using,
- Presenting as clean property,
- Claiming it as clean property.

The act of money laundering continues as long as the person is benefiting from the criminal proceeds in any of these ways.[14]

[13] The Act is passed as a consequence of the Political Declaration adopted by the Special Session of the UN General Assembly 1999 which called upon the Member States to adopt an anti-money laundering law and connected programmes. Accordingly, the Standing Committee on Finance presented its recommendations to the Lok Sabha on 4-3-1999.

[14] Sec. 3 as amended in 2012

In the case of ***SEBI v. Sahara India Real Estate Corpn. Ltd.,***[15] It involves a suspected fake deposit scheme by Sahara India Real Estate Corporation, and the Supreme Court ordered Sahara to refund money it had collected from the public, with an annual 15% interest. A sum like this should be deposited with interest in the entire remaining amount into the SEBI Sahara Refund Account before entertaining any claim for redemption or refund of any nature. At that time, if Sahara proves that it has already returned certain funds, it will become entitled to a refund of such amount. The court also said it could sell Sahara's properties to recover the needed amount, but it has so far refrained from doing so because the company repeatedly said it will generate the needed cash.

The conviction for money laundering shall be sentenced with an imprisonment term of not less than three years, extendable to seven years, and may be liable to pay a fine. Provided that if the predicate offence is under Part A, paragraph 2 of the Schedule, then the maximum imprisonment term shall be ten years instead of seven years.[16]

c) Internet banking and the Payment and Settlement Systems Act, 2007

The RBI is empowered to take action under the law for various offences, including operating a payment system without authorization, failing to comply with authorization terms, not submitting required statements or documents, providing false information, disclosing prohibited data, and failing to follow RBI directions.

These offences can be summarised as below:

1. **Dishonour of electronic funds transfer for insufficiency, etc. of funds in the account.—** A person who attempts to transfer funds electronically from their bank account and the transaction fails due to insufficient funds or exceeds the arranged limit is liable to imprisonment of up to two years, a fine twice the amount transferred, or both. However, this shall only apply if:

- The transfer was for paying off a debt or liability;

[15] SEBI v. Sahara India Real Estate Corpn. Ltd., (2016) 1 SCC 48.
[16] Sec. 4

- The transfer followed the system provider's guidelines;
- The beneficiary demands payment within 30 days of being notified of the failed transfer;
- The transferor does not pay the amount due within 15 days of issue of notice;

It is assumed that the transfer was for paying off a debt unless proved otherwise. The defence that the person didn't know their account balance was insufficient won't be accepted. It will be assumed by the court that the transfer had failed if the bank confirms so, unless proved otherwise. The provisions of the Negotiable Instruments Act, 1881 also come into play where relevant in case of dishonoured electronic funds transfers.[17]

2. **Violation of Section 4.** [18]— If a person violates Section 4 or the terms under **Section 7**[19], they commit an offence that can lead to at least one month of imprisonment, which may go up to 10 years, or a fine up to ₹1 crore, or both. Additionally, a fine of ₹1 lakh per day will be charged for each day the violation continues.[20]

3. False statement.— Anyone who knowingly makes a false statement or omits important information in an application for authorization, return, or any document required under this Act, shall be punishable with imprisonment of up to three years and a fine between ₹10 lakh and ₹50 lakh. [21]

4. Failure to produce documents.— Where any person fails to produce any statement, information, returns or other documents or to furnish documents as required under **Section 12**[22] or **Section 13**[23] while an inspection is made under **Section 14**[24], then such failure shall be punished with fine up to Rs 10 lakhs in respect of each offence and if persistence continues then the fine may extend to Rs 25,000 for every day until such refusal, etc. continues.[25]

[17] Sec. 25
[18] Payment system not to operate without authorisation.
[19] Issue or refusal of authorisation.
[20] Sec. 26(1)
[21] Sec. 26(2)
[22] Power to call for returns, documents or other information.
[23] Access to information.
[24] Power to enter and inspect
[25] Sec. 26(3)

5. Disclosure.— If someone discloses information in violation of **Section 22**[26], they can be punished with imprisonment for up to six months, a fine of up to ₹5 lakhs or twice the amount of damages caused by the disclosure (whichever is higher), or both. [27]

6. Non-compliance with the directions.— On failure to comply with a direction given by the RBI, or to pay the penalty within 30 days, a person is liable to imprisonment for at least one month, extending up to 10 years, and a fine all the way up to ₹1 crore, or both. In case the contravention is continuing, there would, in addition, be a further fine of up to ₹1 lakh for every day for which the failure continues. [28]

7. Contravention of the Act.— If any contravention is committed or if any default is made in respect of any order, regulation made under the Act of 2007, then the defaulter shall be punished with fine which may extend to Rs 10 lakhs and where such contravention or default is continuing then with an additional fine extending up to Rs 25,000 for every day after the first during which the contravention or default continues. [29]

d) ***Information Technology Act, 2000***

The Information Technology Act, 2000 (IT Act) plays a crucial role in regulating internet banking in India. It provides a legal framework for electronic transactions and online activities, including those related to banking services.

Legal Recognition of Electronic Transactions:[30] Electronic records are legally recognized, allowing banks to offer online services such as e-statements, online transactions, and account management through digital means.

Electronic communication.—If an acknowledgement is sent by an "originator" to the "addressee" by e-mail, without any intermediary, it amounts to electronic communication by e-mail which is an alternative to the paper based method of communication. This mode of transaction is legally recognized under Section 4 of the Information Technology Act, 2000.[31]

[26] Duty to keep documents in the payment system confidential.
[27] Sec. 26(4)
[28] Sec. 26(5)
[29] Sec. 26(6)
[30] Sec. 4
[31] Sudarshan Cargo Pvt. Ltd. v. Techvac Engineering (P) Ltd., 2013 SCC OnLine Kar 5063.

Legal recognition of electronic signatures:[32] The IT Act grants legal recognition to digital signatures, ensuring their use in authenticating digital documents and transactions in banking, such as agreements, contracts, and loan applications.

Filing of nomination papers.—Directions issued by the High Court to State Election Commission to accept nomination papers in electronic form by applying Information Technology Act, are not permissible. Section 6 of Information Technology Act, not applicable to State Election Commission. Legislature alone is competent to provide for filing of nomination papers in electronic form.[33]

Retention of Electronic Records:[34] Banks are required to retain electronic records in the same way as physical records, allowing for audits and legal verification of transactions.

Security of electronic records — Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 providing for security of biometric information deemed to be "electronic record" and "sensitive personal data or information" under Information Technology Act, 2000. Directions issued to Government to address issue regarding apprehension of leak of biometric information collected under Aadhaar Scheme. According to the Objects of the Aadhaar Act, the information in the Aadhaar database was to be secured and protected.[35]

Penalties for Unauthorized Access:[36] This section imposes penalties for unauthorized access, hacking, or damage to bank systems or data. It includes provisions against cybercrime that directly impact banking.

[32] Sec. 5
[33] W.B. State Election Commission v. Communist Party of India (Marxist), (2018) 18 SCC 141.
[34] Sec. 7
[35] Binoy Viswam v. Union of India, (2017) 7 SCC 59.
[36] Sec. 43

Hacking and Cybercrime:[37] This section prescribes punishment for hacking into banking systems and unauthorized access to sensitive information, with imprisonment and fines for offenders.

Electronic Contracts:[38] Recognizes that contracts formed through electronic means, such as loan agreements, mortgages, or credit card applications made online, are legally valid and enforceable.

Intermediaries Liability:[39] Protects banks acting as intermediaries (e.g., facilitating third-party transactions) from liability if they follow due diligence and comply with the IT Act.

These sections provide a comprehensive legal framework for secure, efficient, and regulated online banking operations under the IT Act.

e) Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

The Rules as a corollary to the IT Act, 2000 are mainly concerned with the personal information of the users. Thus, the personal information of the user in the context of Internet banking shall be the password and the electronic mandates disclosed by the account holder to the bank. Thus, the Rules define the relevant terms as follows:

Password means a secret word or phrase or code or passphrase or secret key or encryption or decryption keys that one uses to gain access to information.[40]

The term "personal information" is defined as any information relating to a natural person (human beings) that available with a body corporate is sufficient to identify such person.[41]

[37] Sec. 66
[38] Sec. 10A
[39] Sec. 79
[40] R. 2(h)
[41] R. 2(i)

"Sensitive personal data or information" denotes such personal information which is related to password, financial information such as bank account or credit card or debit card or other payment instrument details, biometric information or other personal details received by a body corporate under a lawful contract.[42] The personal information or the sensitive personal data shall be obtained by the body corporate only with the consent of the information provider and that even for a lawful purpose.[43]

IMPACT OF INTERNET BANKING IN TERMS OF CUSTOMER

India's banking system is well-capitalized, resilient, and highly regulated. It has superior financial conditions compared to other countries. Recent innovations in the country include payments banks and small finance banks, coupled with government schemes like Pradhan Mantri Jan Dhan Yojana, which promoted access to banking. Further reforms in digital payments, neo-banking, growing NBFCs, and fintech have visibly enhanced financial inclusion and credit growth. India's fintech industry is estimated to grow rapidly and reach $150 billion by 2025, emerging as the third-biggest fintech ecosystem in the world.[44]

A 2015 report on cybercrime in India by Deloitte brought some ominous trends into light, beyond core banking. Online banking, e-banking, ATMs, and retail banking were revealed as the main targets of fraud. These channels, so essential for modern banking, became hotspots for financial crime. Another factor that contributed to the increasing number of fraud cases was the deficiency of appropriate risk assessment tools, with vulnerabilities open to attack. This brings to light the dire need for better security within India's banking sector.[45]

In the case of ***Dr Subramanian Swamy v. Central Bureau of Investigation,***[46] Dr. Subramanian Swamy filed a petition in the Supreme Court, demanding a CBI inquiry into the role of RBI officials in banking scams involving Kingfisher and Yes Bank. He said despite approving

[42] R. 3
[43] R. 5
[44] Banking Sector in India,< https://www.ibef.org/industry/banking-india >:last accessed 28-10-2024
[45] Deloitte, "*Cybersecurity in the Indian Banking Industry : Part 1, Will 2020 Redefine the Cybersecurity Ecosystem?*" (November 2020).
[46] Dr Subramanian Swamy v. Central Bureau of Investigation, [WP (C) No. 196/2021]

fraudulent loans, they were not investigated. The court issued notice after hearing his arguments.

In a related plea, victims of cyber fraud asked the Supreme Court to establish a special agency to deal with growing online banking fraud. They cited inadequate laws and demanded national coordination and more stringent verification by banks to safeguard consumers.[47]

According to True caller Global Scam Report 2021,[48] India is the country to receive the fourth-highest number of spam sales and telemarketing calls. This is the 5th edition of the report, and it lists the Top 20 Countries Affected by Spam Calls in 2021. The report stated that: over 202 million spam calls were made by just one spammer in India this year. That's over 664,000 calls every day and 27,000 calls every hour of every day. With the people navigating through the ongoing pandemic and countries going into the second round of lockdown, this year's report has shown that not only has the pandemic affected communication behavior but also spam patterns around the world. Another interesting insight from the report is that one of the most common scams in the country remains the ever-popular KYC (know your customer) scam where fraudsters pretend to be a bank, wallet, or digital payment service, asking for user KYC documents as mandated by the Reserve Bank of India.

In the knowledge society of the 21st century, the internet is spreading at unprecedented speed. PC took 16 years to reach 50 million people. However, the Internet took only 4 years to have 50 million people. Internet and has endless advantages. Today there is hardly any field or area or institution where technology is not used. On the same side, there is a seamy side to the internet and technology.

[47] At Least 18% Indians Victims ' : Plea In Supreme Court Seeks Guidelines To Curb Online Banking Frauds <https://www.livelaw.in/top-stories/plea-in-supreme-court-seeks-guidelinesto-curb-online-banking-fraud-178566?infinitescroll=1 >:last accessed 2-11-2025

[48] India ranking in global scam report goes up to 4th position: Truecaller, < https://www.business-standard.com/article/economy-policy/india-ranking-in-global-scam-report-goes-up-to-4th-position-truecaller-121121700649_1.html >:last accessed 23-10-2025

The main disadvantage of technology is cyber crime and pornography. Internet and technology can be a boon or bane depending upon our attitude and how we use them. The need for the hour is to have strict laws to check the misuse of technology.[49]

In the case of ***N. Raghavender v. State of Andhra Pradesh,***[50] The Supreme Court held that when customers deposit money in a bank, the bank does not hold it as a trustee; instead, it becomes part of the bank's funds, creating a debtor-creditor relationship. The bank must repay the amount on demand with agreed interest but can use the funds meanwhile for its profit. A bench of Chief Justice NV Ramana, Justice Surya Kant, and Justice Hima Kohli delivered this while deciding the appeal of N. Raghavender, a bank manager convicted of criminal breach of trust, cheating, and falsification of accounts under the IPC and Prevention of Corruption Act. The case involved Raghavender allegedly conspiring with others to make unauthorized withdrawals from the account of Nishita Educational Academy and prematurely encashing two fixed deposits belonging to B. Satyajit Reddy. He was convicted by the trial and high courts but appealed to the Supreme Court. The Court explained that for conviction under Section 409 IPC, the prosecution must prove "entrustment" of property and dishonest misuse; mere retention or error without dishonest intent cannot constitute criminal breach of trust. Similarly, under Section 420 IPC, fraudulent intent must exist at the time the money was obtained; a simple breach of contract does not amount to cheating.

Upon reviewing the evidence, the Supreme Court found:
No proof of unlawful issuance of loose cheques or falsification of accounts.
No financial loss to the bank or any customer.
No evidence of conspiracy among accused persons.
B. Satyajit Reddy suffered no loss from premature FDR encashment, and interest was even paid from the appellant's personal account.

[49] Richard L. Doernberg and Luc Hinnekens. "Electronic Commerce and International Taxation," Kluwer Law International, 1999 Ed., in Mittal, D.P. "Law of Information Technology (Cyber Law)", Taxmann Allied Services Pvt. Ltd., New Delhi, Oct. 2000.
[50] CBI Criminal Appeal No. 5 Of 2010, LL 2021 SC 765.

The bench criticized the CBI for a careless and possibly influenced investigation, noting withheld evidence and unfair procedures. Given the lack of conclusive proof, the appellant was acquitted of criminal charges. However, the Court found his actions amounted to gross misconduct as a bank officer, justifying his dismissal from service, and clarified that his acquittal would not entitle him to reinstatement.

CONCLUSION

The interface of technology with internet banking has thus changed the scenario of traditional banking in India: in terms of convenience, efficiency, and accessibility to more people. As technology evolves, so does internet banking in terms of friendliness, security, and inclusivity, offering services which were once confined to the physical walls of a branch. With the introduction of mobile banking, digital payments, and innovative fintech solutions, India is well on its course toward a cashless economy, ensuring greater financial inclusion and thereby empowering the rural and urban masses.

This rapid growth is also associated with challenges related to cybersecurity threats, data privacy, and the digital divide, which must be addressed through appropriate regulatory frameworks and technology development. Government, regulators, and financial institutions should work in tandem for a secure, transparent, and inclusive digital banking ecosystem.

In other words, the integration of technology and internet banking holds great promise for transforming the financial scenario in India, but it should also be supported by efforts toward security, inclusivity, and ethical use of technology for sustaining this growth.