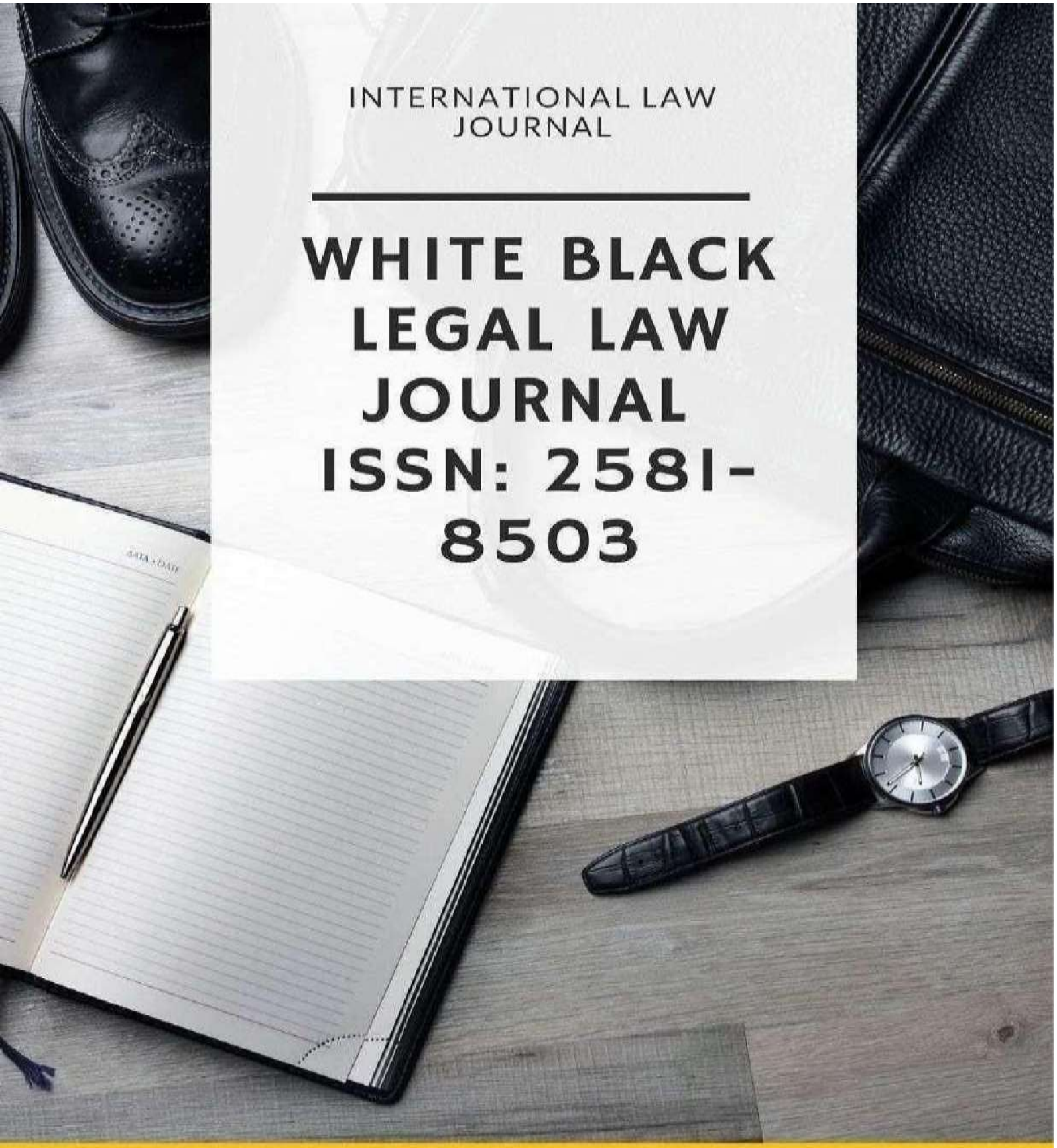

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

DISCLAIMER

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

CYBER FRAUD AND BANKING LIABILITY: A CRITICAL LEGAL STUDY OF THE RESPONSIBILITY OF BANKS IN UNAUTHORISED DIGITAL TRANSACTIONS IN INDIA

AUTHORED BY - DR. MADHU SOODAN RAJPUROHIT*
& MR. HIMANSHU SOLANKI*

ABSTRACT

The rapid expansion of digital banking in India has significantly transformed the nature of financial transactions. Internet banking, mobile banking, debit and credit cards, UPI, digital wallets and other electronic payment mechanisms have provided speed, accessibility and convenience to consumers. However, this technological advancement has also resulted in a sharp rise in cyber fraud, including phishing, OTP fraud, SIM-swap fraud, identity theft, unauthorised fund transfers, fake customer-care fraud and fraudulent digital payment transactions. In such cases, the central legal issue is whether the loss should be borne by the customer or by the bank. This paper critically examines the responsibility of banks in cases of unauthorised digital transactions in India. It analyses the Reserve Bank of India's framework on limiting customer liability, the burden of proof placed upon banks, the duty of banks to maintain secure electronic banking systems, and the remedies available under cyber law, consumer protection law and the RBI Ombudsman mechanism. The paper argues that banks cannot avoid liability merely by stating that a transaction was completed through OTP, PIN or valid credentials. Unless customer negligence is clearly proved by the bank, liability should not be shifted to the customer. The paper concludes that stronger statutory recognition, strict regulatory enforcement and faster compensation mechanisms are necessary to protect digital banking consumers in India.

Keywords: Cyber Fraud; Banking Liability; Unauthorised Digital Transactions; RBI Guidelines; Digital Banking; Consumer Protection.

1. INTRODUCTION

The banking sector in India has undergone a remarkable transformation in the last two decades.

* Professor of Law, Government P.G. Law Collage, Pali, Rajasthan.
* Research Scholar, Faculty of Law, Jai Narain Vyas, University Jodhpur, Rajasthan.

Traditional banking, which was once dependent upon physical branches, cheque books and manual verification, has now shifted towards a technology-driven system. Customers today can transfer funds, pay bills, invest, withdraw money, apply for loans and manage accounts through internet banking, mobile banking, debit cards, credit cards, ATM services, UPI platforms and other digital payment applications.[1]

This digital transformation has undoubtedly made banking services faster, more efficient and more accessible. However, the same transformation has also exposed banking customers to a wide range of cyber risks. Cyber criminals increasingly use technological as well as psychological methods to deceive customers and unlawfully transfer money from their accounts. These frauds include phishing links, fake banking websites, OTP fraud, SIM-swap fraud, card cloning, remote-access application fraud, fake customer-care numbers, malware attacks and identity theft.[2]

In most cases of unauthorised digital transactions, the customer claims that the transaction was not authorised, while the bank denies liability on the ground that the transaction was completed through valid credentials, OTP, PIN, password or registered mobile number. This creates a serious legal controversy: **should the mere technical completion of a digital transaction be treated as proof of customer authorisation, or should the bank be required to prove actual customer negligence?**

The issue is important because banks are not ordinary service providers. Banks are custodians of public money and operate under strict regulatory supervision. When banks provide digital banking facilities, they also undertake a duty to maintain secure systems, protect customer data, detect suspicious transactions, issue timely alerts and provide effective grievance redressal.[3] Therefore, the responsibility of banks in cyber fraud cases cannot be examined only through the lens of contract law. It must also be analysed under banking regulation, cyber law, consumer protection law and principles of financial justice.

The Reserve Bank of India has issued important directions to protect customers in unauthorised electronic banking transactions. The RBI circular dated 6 July 2017 specifically recognises the principle of zero liability and limited liability of customers and places the burden of proving customer liability upon the bank.[4]

[1]Reserve Bank of India, *Digital Payment Security Controls Directions, 2021*, RBI/2020-21/74, DoS.CO.CSITE.SEC. No.1852/31.01.015/2020-21, dated 18 February 2021

2 Information Technology Act, 2000, ss. 43, 66, 66C and 66D

3 Reserve Bank of India, Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions, RBI/2017-18/15, DBR.No.Leg.BC.78/09.07.005/2017-18, dated 6 July 2017

4 Ibid

2. STATEMENT OF THE PROBLEM

Cyber fraud in digital banking presents a complex legal problem. On one hand, banks argue that they cannot be held responsible for every fraud committed by third-party criminals. On the other hand, customers argue that they should not be made to suffer financial loss when the banking system fails to prevent, detect or reverse unauthorised transactions.

The difficulty becomes greater because customers usually do not have access to technical evidence. The bank possesses server logs, IP address details, device records, authentication records, beneficiary details, transaction monitoring data and fraud alerts. The customer only sees the final result: money has been debited from the account without genuine consent.

Banks often reject customer claims by stating that the transaction was completed through OTP, PIN, password or registered mobile number. However, cyber frauds today are sophisticated. Fraudsters may obtain OTPs through deception, fake links, SIM swapping, malware, screen-sharing applications or social engineering. Therefore, the use of OTP or digital credentials should not automatically prove negligence on the part of the customer.[5]

The core legal problem is that customers are frequently denied refund without a proper investigation and without the bank discharging its burden of proof. This results in denial of consumer justice and weakens public trust in digital banking.

3. OBJECTIVES OF THE STUDY

The present paper has the following objectives:

3.1 To examine the nature and forms of cyber fraud in digital banking transactions.

3.2 To analyse the legal responsibility of banks in cases of unauthorised digital transactions.

3.3 To study the RBI framework relating to zero liability and limited liability of customers.

3.4 To examine the burden of proof in cases of unauthorised electronic banking transactions.

3.5 To analyse whether OTP, PIN or password-based authentication is sufficient to deny customer claims.

3.6 To study the relevance of the Information Technology Act, 2000, Consumer Protection Act, 2019, Payment and Settlement Systems Act, 2007 and RBI Ombudsman mechanism.

3.7 To suggest reforms for strengthening customer protection and banking accountability in cyber fraud cases.

5 Ibid.; see also Information Technology Act, 2000, ss. 66C and 66D

4. RESEARCH METHODOLOGY

The present study adopts a **Doctrinal Legal Research Methodology**. It is based on the analysis of statutory provisions, RBI circulars, regulatory directions, judicial decisions, consumer forum decisions, legal principles and secondary materials. The paper is analytical and critical in nature. It focuses on Indian law and regulatory practice relating to cyber fraud, unauthorised digital transactions and banking liability.

The study relies upon the following legal materials: the Reserve Bank of India circular on customer protection in unauthorised electronic banking transactions, the Information Technology Act, 2000, the Payment and Settlement Systems Act, 2007, the Consumer Protection Act, 2019, the Digital Personal Data Protection Act, 2023, the Bharatiya Nyaya Sanhita, 2023 and the RBI Integrated Ombudsman Scheme, 2021.[6]

5. MEANING AND NATURE OF CYBER FRAUD IN DIGITAL BANKING

Cyber fraud in digital banking refers to fraudulent activity carried out through electronic means with the intention of unlawfully accessing, transferring or misappropriating money from a bank account. It involves the misuse of digital technology, computer resources, electronic communication, banking credentials or payment systems.

Cyber fraud differs from traditional fraud because the offender may not physically interact with the victim or the bank. The entire fraud may be committed through a mobile phone, computer, fake link, remote access application, cloned SIM card or digital payment platform. This makes investigation difficult and also raises complex questions regarding jurisdiction, evidence and liability.

In digital banking fraud, the transaction may appear to be valid from the bank's technical point of view because it may have passed through OTP, PIN or password verification. However, from the customer's perspective, the transaction may be completely unauthorised because the customer never intended to transfer the money. Therefore, the legal system must distinguish between **technical authentication** and **genuine authorisation**.

6 Information Technology Act, 2000; Consumer Protection Act, 2019; Payment and Settlement Systems Act, 2007; Digital Personal Data Protection Act, 2023; Bharatiya Nyaya Sanhita, 2023; Reserve Bank of India, Integrated Ombudsman Scheme, 2021.

6. COMMON FORMS OF BANKING CYBER FRAUD

6.1 PHISHING FRAUD

Phishing is one of the most common forms of cyber fraud. Fraudsters send fake emails, SMS messages or links that appear to be from banks, government agencies, courier companies or payment platforms. When the customer clicks the link and enters banking details, the fraudster obtains access to the customer's credentials.[7]

6.2 VISHING OR VOICE PHISHING

In vishing, the fraudster calls the customer pretending to be a bank official, RBI officer, customer-care executive or payment service representative. The customer is induced to share OTP, card number, CVV, PIN or account details.

6.3 SIM-SWAP FRAUD

In SIM-swap fraud, the fraudster obtains a duplicate SIM card or fraudulently transfers the customer's mobile number to another SIM. Once the fraudster controls the mobile number, OTPs and banking alerts may be intercepted. This type of fraud is particularly serious because the customer may not even receive transaction alerts in time.[8]

6.4 UPI FRAUD

UPI fraud may occur through fake collect requests, QR code manipulation, fake payment screenshots, fraudulent links, screen-sharing apps or deception regarding UPI PIN. Many customers are misled into believing that they must enter UPI PIN to receive money, whereas entering PIN generally authorises payment.

6.5 REMOTE ACCESS APPLICATION FRAUD

Fraudsters often persuade victims to install remote access or screen-sharing applications. Once installed, the fraudster may view OTPs, banking details and transaction activity. Such frauds are common in fake customer-care complaints, online marketplace transactions and refund scams.

6.6 CARD CLONING AND ATM FRAUD

Card cloning involves copying card data through skimming devices. Fraudsters may use cloned cards to withdraw money from ATMs or conduct fraudulent transactions.

6.7 IDENTITY THEFT

Identity theft occurs when personal information such as Aadhaar details, PAN details, mobile number, banking credentials or KYC documents are misused to conduct

7 Information Technology Act, 2000, s. 66D

8 Reserve Bank of India, Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions, supra note 3

fraudulent transactions. Under Indian cyber law, dishonest use of another person's password, digital signature or unique identification feature may attract liability under Section 66C of the Information Technology Act, 2000.[9]

7. BANK-CUSTOMER RELATIONSHIP IN THE DIGITAL ERA

Traditionally, the relationship between a banker and a customer has been described as a debtor-creditor relationship. When a customer deposits money, the bank becomes debtor and the customer becomes creditor. However, the modern bank-customer relationship is no longer limited to deposit and withdrawal. Banks now provide technological platforms, payment gateways, authentication systems, mobile applications, internet banking portals and digital transaction infrastructure.

This expansion of banking services has expanded the legal duty of banks. A bank that provides digital banking facilities must ensure that such facilities are reasonably safe, secure and reliable. The customer relies upon the bank's technical expertise and regulatory compliance. Therefore, banks owe a duty of care in maintaining secure systems and preventing unauthorised transactions.

The duty of care of banks includes ensuring secure digital banking architecture, maintaining fraud detection and prevention systems, sending real-time alerts, providing easy reporting channels, blocking accounts or cards upon complaint, investigating unauthorised transactions fairly, reversing unauthorised debits in appropriate cases, complying with RBI timelines, protecting customer data and educating customers about cyber risks.[10]

The Reserve Bank of India's Digital Payment Security Controls Directions, 2021 require regulated entities to implement security controls for digital payment channels and conduct fraud analysis to identify causes of fraud and prevent recurrence.[11]

8. RBI FRAMEWORK ON CUSTOMER PROTECTION IN UNAUTHORISED DIGITAL TRANSACTIONS

The most important regulatory framework on this issue is the RBI circular dated **6 July 2017**, titled **"Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions."** The circular applies to scheduled commercial banks, small finance

9 Information Technology Act, 2000, s. 66C

10 Reserve Bank of India, Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions, supra note 3.

11 Reserve Bank of India, Digital Payment Security Controls Directions, 2021, supra note 1.

banks and payments banks.[12]

The circular is based on the principle that customers should not suffer loss where they are not responsible for the unauthorised transaction. It recognises that banks must have appropriate systems and procedures to ensure safety and security of electronic banking transactions, robust fraud detection and prevention mechanisms, risk assessment mechanisms, customer awareness measures and effective grievance redressal mechanisms.[13]

The circular is extremely important because it recognises that digital banking security is not merely the responsibility of the customer. Banks must maintain systems that protect customers from fraud.

9. ZERO LIABILITY OF CUSTOMERS

The RBI circular recognises the concept of **Zero Liability**. A customer may have zero liability in two important situations.

First, where the unauthorised transaction occurs due to contributory fraud, negligence or deficiency on the part of the bank, the customer is entitled to zero liability. This applies irrespective of whether the transaction is reported by the customer or not.[14]

Secondly, where the unauthorised transaction occurs due to a third-party breach and neither the bank nor the customer is at fault, the customer may still have zero liability if the customer reports the unauthorised transaction within the prescribed time.[15]

This principle is highly significant because cyber fraud is often committed by third parties. If the customer has not contributed to the fraud and reports the transaction promptly, the loss should not be imposed upon the customer.

10.LIMITED LIABILITY OF CUSTOMERS

The RBI framework also recognises situations where the customer may bear limited liability. This generally depends upon the delay in reporting the unauthorised transaction and the nature of the transaction. The underlying principle is that customers must report unauthorised transactions promptly so that the bank can stop further loss.[16]

However, limited liability does not mean that the bank can arbitrarily impose liability on the

12 Reserve Bank of India, Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions, supra note 3
13 Ibid
14 Ibid.
15 Ibid
16 Ibid

customer. Even in cases of delayed reporting, the bank must act according to RBI norms and must determine liability in a fair, transparent and reasoned manner.

11.BURDEN OF PROOF ON BANKS

One of the most important aspects of the RBI framework is that the **Burden of Proving Customer Liability Lies on The Bank**.[17]

This rule is legally sound because banks control the technical infrastructure and possess the relevant evidence. A customer cannot be expected to produce server logs, IP records, authentication trails, device fingerprints or internal fraud alerts. Therefore, when a bank alleges customer negligence, it must prove such negligence through reliable evidence.

The bank should be required to produce login records, device details, IP address records, beneficiary addition details, transaction authentication records, SMS and email alert records, call records or complaint records, evidence of customer consent, evidence of customer negligence and internal fraud-risk assessment.

A mere statement that OTP or PIN was used should not be sufficient to discharge the bank's burden.

12.OTP, PIN AND PASSWORD: TECHNICAL AUTHENTICATION VERSUS LEGAL AUTHORISATION

A recurring issue in banking cyber fraud cases is whether use of OTP, PIN or password proves that the customer authorised the transaction. Banks generally argue that once OTP or PIN is used, the transaction must be treated as valid.

This argument is legally weak if applied mechanically. Technical authentication only proves that the banking system processed the transaction through certain credentials. It does not conclusively prove that the customer voluntarily, knowingly and consciously authorised the transaction.

Modern fraudsters can obtain OTPs or credentials through phishing links, fake customer-care calls, SIM-swap fraud, malware, remote access applications, screen-sharing fraud, fake KYC update messages, social engineering and data leakage.[18]

Therefore, the correct legal test should be whether the bank can prove that the customer

17 Ibid. RBI states that the burden of proving customer liability in unauthorised electronic banking transactions lies on the bank

18 Information Technology Act, 2000, ss. 66C and 66D

knowingly, voluntarily or negligently disclosed confidential credentials, and whether such disclosure directly caused the loss.

Unless this is proved, customer liability should not be presumed.

13.SHADOW REVERSAL AND TIME-BOUND REDRESSAL

The RBI framework also requires banks to provide timely relief to customers. In unauthorised electronic banking transactions, banks are required to credit the amount involved in the unauthorised transaction to the customer's account within the prescribed period, without waiting for settlement of insurance claims or recovery from fraudsters.[19]

The purpose of this requirement is to ensure that customers are not forced to suffer financial hardship for long periods. Cyber fraud victims often lose life savings, business funds or essential household money. Delay in refund can cause serious financial and mental distress.

The complaint must also be resolved within the RBI-prescribed period. Failure to follow the RBI timeline may amount to deficiency in banking service and may justify compensation before the Consumer Commission or relief before the RBI Ombudsman.

14.DIGITAL PAYMENT SECURITY CONTROLS DIRECTIONS, 2021

The RBI Digital Payment Security Controls Directions, 2021 strengthen the argument that banks have a proactive duty to secure digital transactions. These directions require regulated entities to implement common minimum-security controls for digital payment channels such as internet banking, mobile banking and card payments.[20]

These directions are important because they show that cyber fraud prevention is not optional. Banks must adopt appropriate security measures, including fraud monitoring, authentication controls, customer protection mechanisms, awareness systems and grievance redressal.

Thus, if a bank fails to maintain adequate digital security or fraud monitoring, it may be considered negligent.

15.INFORMATION TECHNOLOGY ACT, 2000 AND CYBER BANKING FRAUD

The Information Technology Act, 2000 is the principal law dealing with cyber offences and electronic records in India. Several provisions of the Act are relevant in banking cyber fraud

19 Reserve Bank of India, Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions, supra note 3

20 Reserve Bank of India, Digital Payment Security Controls Directions, 2021, supra note 1.

cases.

Section 43 deals with unauthorised access, downloading, copying, extraction of data, introduction of viruses, disruption of computer systems and related acts. It provides for compensation where loss is caused by unauthorised acts relating to computer systems.[21]

Section 43A provides compensation for failure to protect sensitive personal data where a body corporate is negligent in implementing reasonable security practices and procedures. This provision may become relevant where weak data protection or system negligence contributes to cyber fraud.[22]

Section 66 deals with computer-related offences where acts under Section 43 are committed dishonestly or fraudulently. Section 66(C) deals with identity theft, while Section 66(D) deals with cheating by personation using computer resources.[23] These provisions are particularly relevant in phishing, fake customer-care fraud, online impersonation and fraudulent banking communication.

The IT Act provides a criminal and compensatory framework, but it does not fully determine the liability of banks towards customers. Therefore, RBI guidelines and consumer protection principles remain crucial.

16.BHARATIYA NYAYA SANHITA, 2023 AND CRIMINAL LIABILITY

The Bharatiya Nyaya Sanhita, 2023 has replaced the Indian Penal Code as the principal criminal law statute. It is relevant in cyber banking fraud cases because such frauds may involve cheating, dishonest inducement, forgery, use of forged electronic records, criminal breach of trust and conspiracy.[24]

However, criminal prosecution of fraudsters is different from civil or regulatory liability of banks. A bank cannot avoid its responsibility towards the customer merely by saying that a police complaint has been filed or investigation is pending. Criminal proceedings aim to punish offenders, whereas customer protection aims to restore money and compensate the victim.

Therefore, both remedies may operate simultaneously.

17.PAYMENT AND SETTLEMENT SYSTEMS ACT, 2007

The Payment and Settlement Systems Act, 2007 provides the legal foundation for regulation

21 Information Technology Act, 2000, s. 43.
22 Information Technology Act, 2000, s. 43A
23 Information Technology Act, 2000, ss. 66, 66C and 66D
24 Bharatiya Nyaya Sanhita, 2023.

and supervision of payment systems in India. Digital payment mechanisms operate within a regulated payment ecosystem. Therefore, unauthorised digital transactions affect not only individual customers but also public confidence in payment systems.[25]

Banks and payment service providers are expected to maintain trust, integrity and safety in electronic payment mechanisms. When unauthorised transactions occur due to weak systems, poor monitoring or delayed action, the issue becomes one of payment system governance.

18.DIGITAL PERSONAL DATA PROTECTION ACT, 2023 AND BANKING RESPONSIBILITY

Digital banking depends heavily on personal data. Banks collect and process names, mobile numbers, account details, PAN details, Aadhaar details, addresses, transaction history, device information and financial behaviour. If such data is leaked, misused or inadequately protected, customers become vulnerable to cyber fraud.

The Digital Personal Data Protection Act, 2023 is relevant because it imposes obligations on data fiduciaries to process personal data lawfully and protect it through reasonable safeguards.[26]

In the banking context, banks are expected to maintain strong data protection systems because misuse of customer data can directly facilitate cyber fraud.

Thus, data protection and banking cyber security are closely connected.

19.CONSUMER PROTECTION ACT, 2019 AND DEFICIENCY IN BANKING SERVICE

Banking services fall within the scope of consumer protection law. A customer who suffers loss due to unauthorised digital transactions may approach the Consumer Commission if the bank's conduct amounts to deficiency in service.

Deficiency in banking service may include failure to provide secure digital banking systems, failure to send timely alerts, failure to block account/card after complaint, failure to investigate properly, wrongful rejection of refund claim, failure to follow RBI guidelines, delay in complaint resolution, failure to provide transaction records, failure to prove customer negligence and unfair shifting of liability upon the customer.[27]

25 Payment and Settlement Systems Act, 2007.
26 Digital Personal Data Protection Act, 2023.
27 Consumer Protection Act, 2019, ss. 2(7), 2(11) and 2(42)

Consumer Commissions have increasingly recognised that banks must prove customer negligence before denying refund in unauthorised transaction cases.

20.RBI INTEGRATED OMBUDSMAN SCHEME, 2021

The RBI Integrated Ombudsman Scheme, 2021 provides a cost-free grievance redressal mechanism for complaints involving deficiency in services by RBI-regulated entities. It applies where a regulated entity does not resolve the complaint satisfactorily or does not reply within 30 days.[28]

The scheme is important because it provides a simpler and less expensive remedy than civil litigation. Customers can approach the Ombudsman in cases involving wrongful denial of refund, non-compliance with RBI guidelines, delay in complaint handling or deficiency in banking services.

The RBI has also stated that the scheme defines deficiency in service as the ground for complaint and removes rigid jurisdictional limitations of earlier schemes.[29]

21.JUDICIAL AND QUASI-JUDICIAL TRENDS

Recent judicial and consumer forum trends indicate that courts and commissions are increasingly applying RBI's customer-protection framework in favour of victims of unauthorised transactions.

For example, a reported Chandigarh Consumer Commission decision directed Indian Bank to refund money lost in unauthorised ATM transactions. The Commission relied upon RBI's July 2017 circular and noted that the bank failed to prove customer liability and failed to resolve the complaint within the RBI framework.[30]

Similarly, a reported Bombay High Court decision dated 6 April 2026 directed HDFC Bank to reimburse ₹38 lakh lost in a SIM-swap cyber fraud case. The Court reportedly relied upon RBI's 2017 circular and found that the bank failed to prove negligence on the part of the customer.[31]

These decisions show that the legal approach is moving towards greater accountability of

28 Reserve Bank of India, Integrated Ombudsman Scheme, 2021.

29 Reserve Bank of India, Press Release, Prime Minister Launches the Reserve Bank – Integrated Ombudsman Scheme, 2021, dated 12 November 2021

30 Namrata Naman Jha v. Indian Bank, District Consumer Disputes Redressal Commission, Chandigarh, as reported in The Times of India, "Panel orders bank to refund 1L lost in fraudulent transactions."

31 Subodh Korde v. HDFC Bank, Bombay High Court, order dated 6 April 2026, as reported in The Times of India, "User not negligent, give Rs 38 lakh lost in cyber fraud, Bombay High Court tells HDFC Bank."

banks, especially where customers report fraud promptly and banks fail to establish negligence.

22. CRITICAL ANALYSIS OF BANKING LIABILITY

The liability of banks in unauthorised digital transactions should be analysed on the basis of four principles.

22.1 PRINCIPLE OF CUSTODIAL RESPONSIBILITY

Banks hold customer money in trust-like confidence. Though technically the relationship may be debtor-creditor, in practical terms customers rely upon banks to safeguard their money. Therefore, banks must bear a high degree of responsibility.

22.2 PRINCIPLE OF TECHNOLOGICAL CONTROL

Banks control the digital infrastructure. They design or adopt the banking application, authentication process, transaction monitoring system and fraud detection mechanism. Therefore, where failure occurs within the digital ecosystem, the bank cannot simply shift responsibility to the customer.

22.3 PRINCIPLE OF SUPERIOR EVIDENCE

Banks possess technical evidence. Customers generally do not have access to logs, IP addresses, internal alerts or fraud detection data. Therefore, the burden of proof must remain on the bank.[32]

22.4 PRINCIPLE OF CONSUMER PROTECTION

Bank customers are consumers of financial services. The law must protect them against unfair denial of claims, delayed grievance redressal and arbitrary allegations of negligence.

23. CHALLENGES IN THE EXISTING LEGAL FRAMEWORK

Despite RBI guidelines, several practical challenges remain.

First, many banks reject claims by merely stating that OTP, PIN or password was used. Such rejection ignores the reality of modern cyber fraud.

Secondly, customers often face long delays even after promptly reporting fraud. This defeats the purpose of RBI's customer-protection framework.

Thirdly, banks often do not provide full transaction details, technical logs or reasons for rejection. This makes it difficult for customers to challenge the bank's decision.

32 Reserve Bank of India, *Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions*, supra note 3

Fourthly, many customers are unaware of phishing, SIM swap, remote access apps and UPI fraud. Banks must take greater responsibility for customer education.

Fifthly, cyber fraud cases often involve banks, police, payment intermediaries, telecom companies and beneficiary banks. Poor coordination delays recovery and investigation.

Lastly, RBI circulars provide strong protection, but a clear statutory framework on bank liability in unauthorised digital transactions would improve enforcement.

24.SUGGESTIONS AND REFORMS

The following reforms are suggested:

i. The principles of zero liability, limited liability and bank burden of proof should be incorporated into statutory law.
ii. Banks should be required to provide provisional credit within a strict time limit where the customer reports unauthorised transactions promptly.
iii. Banks should not be allowed to deny refund without producing technical evidence showing customer negligence.
iv. Disputed transactions should be reviewed by independent cyber experts or neutral technical auditors.
v. Banks should strengthen artificial intelligence-based fraud monitoring systems to detect unusual transaction behaviour.
vi. Beneficiary accounts and mule accounts should be frozen immediately upon receipt of fraud complaint.
vii. Banks should conduct regular awareness campaigns in simple language regarding OTP fraud, UPI fraud, SIM swap, phishing and remote-access application fraud.
viii. RBI should impose penalties on banks that fail to follow customer-protection timelines or mechanically reject claims.
ix. Banks should create dedicated cyber fraud response teams to coordinate with police, cybercrime portals and payment intermediaries.
x. A sector-wide compensation mechanism may be considered for victims of cyber fraud, funded by banks and payment institutions.

25.CONCLUSION

Cyber fraud in digital banking is one of the most serious legal and regulatory challenges in India's financial system. While digital banking has created speed, convenience and financial

inclusion, it has also exposed customers to new forms of technological and psychological fraud. In such cases, the responsibility of banks must be examined in light of their regulatory obligations, technological control, custodial role and duty of care.

The RBI framework has correctly recognised that customers should not be made liable where they are not at fault. The principles of zero liability and limited liability are essential for protecting digital banking consumers. Most importantly, the burden of proving customer liability lies upon the bank. Therefore, banks cannot deny refund merely by stating that OTP, PIN or password was used. They must prove actual negligence by the customer.[33]

The use of digital credentials may show technical authentication, but it does not always prove genuine legal authorisation. Cyber fraudsters may obtain credentials through phishing, SIM swap, malware, fake customer-care calls or remote access apps. Therefore, a customer-friendly and evidence-based approach is necessary.

The existing legal framework, including RBI circulars, the Information Technology Act, Consumer Protection Act, Payment and Settlement Systems Act, Digital Personal Data Protection Act and RBI Ombudsman Scheme, provides important remedies. However, the practical implementation remains inconsistent. Customers continue to suffer due to delayed refunds, mechanical rejection of complaints and lack of transparency in bank investigations.

In the digital economy, public confidence in banking depends upon strong customer protection. Banks are not merely passive processors of digital transactions. They are custodians of financial trust. Therefore, in cases of unauthorised digital transactions, banking liability must be interpreted in a manner that promotes consumer justice, technological accountability and financial security.

IMPORTANT SOURCES VERIFIED

The RBI's 2017 circular expressly covers unauthorised electronic banking transactions and places the burden of proving customer liability on the bank. (Reserve Bank of India).

The RBI Integrated Ombudsman Scheme provides cost-free redress for deficiency in service where a regulated entity does not resolve or reply within 30 days. (Reserve Bank of India).

Recent reported cases also show courts and consumer fora applying the RBI circular against banks where customer negligence was not proved. (timesofindia.indiatimes.com).

[33] Ibid.