ONLINE BANKING FRAUD IN INDIA: LEGAL FRAMEWORK AND CHALLENGES

Priti Somnath Dhere, Shri Navalmal Firodia Law College, Pune

ABSTRACT

As banking becomes digital, fraud has also become a growing concern in the lives of ordinary people. The rapid growth of internet banking, mobile banking, UPI, and digital wallets has made financial transactions easier and faster. However, it has also increased online banking fraud through phishing, fake banking calls, OTP fraud, identity theft, and unauthorized transactions. In India, the Information Technology Act, 2000, banking regulations, and cybersecurity measures provide a legal framework to address online banking fraud. However, victims still face challenges such as lack of awareness, delays in reporting, difficulties in identifying offenders, and recovering lost money. This study examines the legal framework relating to online banking fraud in India and analyses the practical challenges faced by victims. It also aims to suggest measures to improve cybersecurity, public awareness, investigation, and victim protection. Stronger enforcement and faster complaint mechanisms can help reduce online banking fraud and protect banking customers. Greater public awareness, stronger cybersecurity measures, and faster reporting and investigation mechanisms can reduce online banking fraud and improve the protection of banking customers. The main aim of this study is to examine the legal framework relating to online banking fraud in India and identify the practical challenges faced by victims. The objectives are to understand the concept and major forms of online banking fraud, examine the relevant legal and regulatory provisions, analyse the challenges in reporting and investigation, and suggest measures for improving prevention, enforcement, and victim protection. The study suggests stronger implementation of cybersecurity Increase Cybersecurity.

Keywords: Online Banking Fraud, Cybercrime, Digital Banking, Internet Banking, Cybersecurity, Information Technology Act, Financial Fraud, Consumer Protection, Legal Remedies.

1. INTRODUCTION

The digitalisation of banking has brought considerable benefits. Customers can transfer funds through electronic systems, make payments through UPI, use mobile applications and receive instant transaction alerts. Businesses can receive payments electronically, while governments can distribute benefits directly into bank accounts. Digital banking has therefore become an important part of India's economic and financial infrastructure.

However, the same technology that provides convenience can also be misused. Cyber criminals do not necessarily need physical access to a bank branch or ATM to steal money. A fraudster may instead manipulate a customer through a telephone call, fraudulent message, fake website, malicious link or impersonation of a bank official. In many cases, the victim is persuaded to reveal an OTP, password, PIN, card information or other authentication credential. In other cases, malware or unauthorised access may allow the offender to interfere with the victim's device or banking account.

Online banking fraud is therefore different from traditional forms of theft in an important respect: **the victim may voluntarily perform the transaction because the offender has successfully deceived the victim.** This makes prevention, investigation and determination of liability legally complicated.

The problem also involves more than criminal punishment. Once fraudulent money has been transferred, the victim wants immediate assistance from the bank, freezing of the recipient account and recovery of the money. Consequently, the legal framework must address three connected questions: **Who committed the fraud? Who is responsible for the loss? And what remedy is available to the victim?** The Information Technology Act, 2000 remains a central statute for cyber offences, including identity theft and cheating by personation through computer resources.[1]

2. MEANING AND NATURE OF ONLINE BANKING FRAUD

Online banking fraud may broadly be understood as the use of computers, mobile devices, electronic communication systems, digital payment platforms or other technological means to

[1] Information Technology Act, 2000, 43, 43A, 66, 66C, 66D, India Code.

unlawfully obtain money, banking credentials or financial advantages from another person.

The expression covers a wide range of activities. It is not limited to hacking. A person may commit online banking fraud by pretending to be a bank employee and asking the customer to provide an OTP. Another offender may create a website that looks similar to an authentic banking website and use it to collect usernames and passwords. A fraudster may also convince a victim to install a remote-access application under the false promise of helping with a refund.

One of the important characteristics of online banking fraud is **deception**. The offender often creates a false sense of trust or urgency. For example, the victim may be told that the bank account will be blocked unless KYC is updated immediately, or that a refund can be processed only after clicking a particular link. The victim acts on the false information and unintentionally assists the offender.

A second characteristic is **speed**. Digital transactions can be completed within seconds. Once money is transferred to another account, it may be rapidly moved through multiple accounts or converted into other forms of value. This creates difficulty for investigating authorities because the time available to trace and freeze the funds can be extremely short.

A third characteristic is **anonymity and geographical reach**. The victim, bank account, mobile number, digital device and offender may all be located in different places. A fraud may involve several intermediaries and accounts across different jurisdictions.

A fourth characteristic is the use of **stolen or compromised identity information**. Banking credentials, passwords, card information, mobile numbers and other personal information may be obtained through phishing, data breaches or social engineering. The Information Technology Act specifically criminalises fraudulent or dishonest use of another person's electronic signature, password or unique identification feature.[2] Thus, online banking fraud is simultaneously a **technological, financial, criminal and consumer-protection problem**.

3. HISTORICAL DEVELOPMENT OF ONLINE BANKING AND CYBER FRAUD IN INDIA

The development of online banking in India can be understood as part of the broader

[2] Information Technology Act, 2000, Section 66C, Bharatiya Nyaya Sanhita, 2023, 318–19, India Code.

transformation from traditional banking to electronic banking. Initially, banking technology was primarily used for internal operations such as computerised record keeping and interbranch transactions. Gradually, customers received access to ATMs, electronic fund transfers, internet banking and mobile banking.

The emergence of internet-based financial services created a need for legal recognition of electronic records and transactions. The **Information Technology Act, 2000** became an important milestone in this development. It provided legal recognition to electronic records and electronic commerce and introduced a statutory framework for several forms of cyber misconduct.

The growth of electronic banking also changed the nature of financial crime. Traditional bank fraud could often be investigated by examining physical documents, signatures and branch records. The expansion of mobile banking and digital payments further increased the scale of this transformation. UPI and mobile payment applications made small-value transactions extremely convenient. At the same time, fraudsters began using social engineering techniques specifically designed around digital payment behaviour.

The regulatory response consequently evolved over time. The Reserve Bank of India introduced measures concerning customer liability for unauthorised electronic banking transactions and later issued the **Master Direction on Digital Payment Security Controls, 2021**, which establishes common Minimum Security controls for digital payment products and services.[3]

The RBI subsequently issued revised **Master Directions on Fraud Risk Management in 2024**, strengthening governance, early-warning mechanisms and reporting of frauds to lawenforcement agencies.[4]

The historical development therefore demonstrates an important pattern: **technological innovation has repeatedly been followed by legal and regulatory adaptation**. Nevertheless, law generally develops more slowly than technology. New fraud techniques can emerge before a specific legislative response is created, requiring existing legal provisions to be interpreted

[3] Reserve Bank of India, *Master Direction on Digital Payment Security Controls*, RBI/2020-21/74, DoS.CO/CSITE/SEC.No.1852/31.01.015/2020-21 (Feb. 18, 2021).
[4] Reserve Bank of India, *Master Directions on Fraud Risk Management in Commercial Banks and All India Financial Institutions*, RBI/DOS/2024-25/118, DOS.CO.FMG.SEC No.5/23. 04.001/2024-25 (July 15, 2024).

and applied to new factual situations.

4. MAJOR FORMS OF ONLINE BANKING FRAUD IN INDIA

Online banking fraud occurs through several methods. Understanding these methods is important because each form may involve different legal provisions and different preventive measures.

4.1 Phishing

Phishing involves fraudulent electronic communication designed to obtain confidential information. The offender may send an email, SMS or message containing a link to a fake banking website. The website may imitate the appearance of a genuine bank website. When the customer enters login credentials, the information is captured by the fraudster.

4.2 Vishing and Fake Banking Calls

Vishing refers to fraud conducted through voice communication. The offender may introduce himself as a bank employee, RBI official, police officer or customer-care representative. The victim may be asked to provide an OTP, card number, PIN or other information.

4.3 OTP Fraud

OTP-based fraud occurs when an offender obtains a one-time password through deception or by compromising the victim's device. The OTP may then be used to authenticate a transaction.

4.4 Identity Theft

Identity theft occurs when an offender fraudulently uses another person's identifying information, password or electronic authentication credentials. Section 66C of the Information Technology Act directly addresses identity theft.[5]

4.5 Cheating by Personation

A fraudster may pretend to be a bank employee, customer-care executive, government officer or another person. Section 66D of the Information Technology Act deals with cheating by

[5] Information Technology Act, 2000, Section 66C

personation using a computer resource or communication device.[6] The Bharatiya Nyaya Sanhita, 2023 also contains the offence of cheating by personation.

4.6 Malicious Links and Remote-Access Applications

Victims may be persuaded to click links or install applications allegedly required for refunds, KYC verification or technical support. Such applications can potentially expose sensitive information or allow unauthorised access to a device.

4.7 Card and Account Takeover Fraud

Fraud may involve stolen card information, compromised credentials or unauthorised access to banking accounts. Once access is obtained, the offender may initiate transfers or make purchases.

The variety of techniques demonstrates why online banking fraud cannot be addressed through one legal provision alone.

5. LEGAL FRAMEWORK UNDER THE INFORMATION TECHNOLOGY ACT, 2000

The Information Technology Act, 2000 is one of the principal statutes dealing with cyberrelated conduct in India. Although it was enacted during an earlier stage of digital development, several provisions remain relevant to online banking fraud.

Section 43 deals with unauthorised acts relating to computer systems and computer resources. It provides a civil liability framework for specified forms of unauthorised access, downloading, introducing contaminants and damage. Where such conduct is carried out dishonestly or fraudulently, the conduct may also attract criminal liability under Section 66.

Section 43A is relevant where a body corporate possessing, dealing with or handling sensitive personal data or information is negligent in implementing reasonable security practices and procedures and such negligence causes wrongful loss or wrongful gain.[7]This provision is important in considering the responsibility of organisations handling sensitive financial information.

[6] Id. Section 66D.
[7] Information Technology Act, 2000, Section 43A.

Section 66 deals with computer-related offences. Sections 66C and 66D are particularly relevant to online banking fraud. Section 66C deals with identity theft, while Section 66D deals with cheating by personation using a computer resource or communication device.[8]

These provisions are significant because many banking frauds involve a combination of identity misuse and deception. For example, if a fraudster impersonates a bank employee and uses a computer or communication device to deceive a customer into transferring money, the facts may potentially attract Section 66D along with applicable offences under general criminal law.

The Act also contains provisions concerning preservation and retention of information by intermediaries and powers relating to interception and monitoring in specified circumstances. These provisions may become relevant during cybercrime investigation.

However, the Information Technology Act should not be viewed as a complete code for banking fraud. A single incident may involve offences under the IT Act as well as offences under the Bharatiya Nyaya Sanhita. Therefore, modern investigation requires an integrated application of cyber law and general criminal law.

6. BHARATIYA NYAYA SANHITA, 2023 AND ONLINE BANKING FRAUD

The criminal-law framework applicable to online banking fraud has also changed with the enactment of the **Bharatiya Nyaya Sanhita, 2023 (BNS)**. The BNS came into force on July 1, 2024, replacing the Indian Penal Code, 1860 for offences covered by the new legislation.

Section 318 of the BNS deals with **cheating**. It covers situations where a person deceives another person and fraudulently or dishonestly induces that person to deliver property or to do or omit something that causes, or is likely to cause, damage or harm.[9]

This provision is highly relevant to banking fraud because many scams operate through deception rather than direct technical hacking. For example, if a fraudster falsely represents himself as a bank official and induces a customer to transfer money, the conduct may constitute cheating depending on the facts.

[8] Information Technology Act, 2000, Section 43, 66, 66C, 66D.
[9] Bharatiya Nyaya Sanhita, 2023, Section 318.

Section 319 deals with **cheating by personation**. It applies where a person cheats by pretending to be another person or representing himself or another person as someone different from their actual identity.[10] This provision may apply where fraudsters impersonate bank officials, customer-care representatives or other persons to obtain money or confidential information.

The BNS therefore complements the Information Technology Act. The IT Act focuses on the technological method used in certain offences, whereas the BNS provides general criminal offences that may arise from the fraudulent conduct itself.

An important advantage of this combined approach is that law enforcement need not treat online fraud merely as a "computer offence." The underlying conduct—cheating, personation, forgery, dishonest inducement or other criminal behaviour—can also be addressed under general criminal law.

The challenge, however, lies in accurately identifying the applicable provisions and establishing the necessary ingredients through digital evidence.

7. ELECTRONIC EVIDENCE AND THE BHARATIYA SAKSHYA ADHINIYAM, 2023

Online banking fraud is fundamentally dependent on electronic evidence. A criminal investigation may involve bank statements, transaction records, SMS messages, emails, screenshots, call records, mobile-device data, digital payment records, CCTV footage and information obtained from service providers.

The **Bharatiya Sakshya Adhiniyam, 2023 (BSA)** is therefore particularly relevant. It modernises the evidentiary framework and expressly recognises electronic and digital records.

Section 61 provides that an electronic or digital record cannot be denied admissibility merely because it is an electronic or digital record and gives such record the same legal effect, subject to the requirements of Section 63, as other documents.[11] Section 62 deals with special provisions relating to electronic records, while Section 63 deals with their admissibility.

[10] Id. Section 319.
[11] Bharatiya Sakshya Adhiniyam, 2023, Section 61–63.

This framework is important in banking fraud cases because the prosecution generally cannot depend only upon oral testimony. The electronic trail may provide the most important evidence regarding the transaction.

8. ROLE OF THE RESERVE BANK OF INDIA

The Reserve Bank of India plays a central regulatory role in protecting banking customers from unauthorised electronic transactions. Its role is important because criminal law generally operates after an offence has occurred, whereas banking regulation can impose preventive responsibilities on regulated entities.

The RBI issued the **Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions** circular in 2017. The circular provides different levels of customer liability depending upon the circumstances of the unauthorised transaction.

Where an unauthorised transaction results from contributory fraud, negligence or deficiency on the part of the bank, the customer may have zero liability. Similarly, where a third-party breach occurs and the customer reports the transaction within the prescribed period, zero liability may arise.[12]

The circular also recognises situations where the customer has been negligent, such as sharing payment credentials. In such circumstances, the customer may bear the loss until reporting the unauthorised transaction to the bank. Once the transaction is reported, subsequent loss is to be borne by the bank under the stated framework.[13]

The RBI framework is significant because it distinguishes **criminal responsibility of the fraudster** from **financial liability for the unauthorised transaction**. A customer may be a victim of fraud even though the bank must examine whether the customer contributed to the loss.

The circular also requires banks to take steps after receiving notification of an unauthorised transaction. The bank is required to credit the amount involved through a shadow reversal

[12] 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 (July 6, 2017).
[13] Id.

within the specified period and resolve liability within the prescribed framework.

Thus, RBI regulation provides an important customer-protection mechanism in addition to criminal law.

9. DIGITAL PAYMENT SECURITY AND FRAUD RISK MANAGEMENT

The prevention of online banking fraud requires more than criminal punishment. Banks and other regulated entities must maintain effective technological and organisational controls.

The RBI's **Master Direction on Digital Payment Security Controls, 2021** establishes minimum security controls for digital payment products and services. It covers areas including governance, security-risk management, authentication, fraud-risk management, reconciliation, customer awareness and grievance redressal. It also addresses internet banking, mobile payment applications and card payments.[14]

The significance of this framework is that cybersecurity is treated as an ongoing institutional responsibility. Banks must not simply respond after fraud has occurred; they must establish systems designed to identify and reduce risks before customers suffer losses.

The RBI also revised its **Fraud Risk Management Directions in 2024**. These directions strengthen the role of the board and senior management in fraud-risk governance and provide for mechanisms such as early-warning signals and red-flagging of accounts. The RBI has stated that the revised directions are intended to strengthen early detection and prevention of fraud and improve timely reporting to law-enforcement agencies and supervisors.[15]

The importance of these regulatory measures has increased because online banking fraud can involve organised networks rather than isolated offenders. A fraudulent account may be used to receive money from several victims. Multiple accounts may then be used to transfer the funds further.

The regulatory approach should consequently combine **prevention, detection, rapid response and accountability**.

[14] Reserve Bank of India, *Master Direction on Digital Payment Security Controls*, supra note 5.
[15] Reserve Bank of India, *Master Directions on Fraud Risk Management in Commercial Banks*, supra note 6.

10. LIABILITY OF BANKS AND CUSTOMERS

The liability for online banking fraud depends on the reason for the unauthorized transaction and how quickly the customer reports it. Under RBI guidelines, if the fraud occurs because of the **bank's negligence or deficiency**, the customer generally has no liability. Similarly, where there is no customer negligence and the unauthorized transaction is reported within **three working days**, the customer has zero liability.

On the other hand, if the customer is negligent, such as by sharing an **OTP, password, PIN, or other banking credentials**, the customer may bear the loss until the fraud is reported to the bank. Therefore, customers also have a responsibility to keep their banking information secure and report suspicious transactions immediately. Once the bank is informed, it must take appropriate action and provide the required relief according to RBI rules.

Thus, the liability of banks and customers is based on **negligence, responsibility, and timely reporting**. Banks must maintain strong security systems, while customers must use banking services carefully and report fraud without delay.

The appropriate legal approach is therefore one of **shared responsibility based upon the circumstances of each case**.

11. REPORTING AND INVESTIGATION OF ONLINE BANKING FRAUD

Prompt reporting is one of the most important practical requirements in online banking fraud. Once the victim discovers the fraud, the first priority should be to contact the bank or payment service provider and request immediate action. The victim should also report the incident to the National Cyber Crime Reporting Portal or the designated cybercrime helpline.

The Government's National Cyber Crime Reporting Portal provides a specific mechanism for reporting financial fraud. The national helpline **1930** is available for immediate reporting of cyber financial fraud.[16]

The importance of immediate reporting arises from the movement of fraudulent funds. If the receiving account can be identified quickly, authorities and financial institutions may have an

[16] National Cyber Crime Reporting Portal, Government of India, *Cyber Financial Fraud – 1930 Helpline*.

opportunity to place restrictions on the funds before they are transferred further.

Thus, effective investigation requires **speed, technical expertise, financial tracing and coordination**.

13. MAJOR CHALLENGES IN COMBATING ONLINE BANKING FRAUD

Despite the existence of several laws and regulatory mechanisms, India continues to face significant practical challenges.

13.1 Lack of Awareness

Many customers are unfamiliar with basic cybersecurity practices. They may not know that legitimate banks generally do not require customers to disclose OTPs, PINs or passwords through telephone calls or messages.

13.2 Sophisticated Social Engineering

Fraudsters increasingly exploit human psychology rather than relying only on technical hacking. They create urgency, fear and trust to persuade victims to take actions that benefit the offender.

13.3 Delay in Reporting

Delay is one of the most serious practical problems. The longer fraudulent funds remain outside effective intervention, the greater the possibility that they will be transferred through several accounts.

13.4 Identification of Offenders

Fraudsters may operate using fake identities, mule accounts, temporary phone numbers and accounts belonging to third parties. Identifying the actual organiser can therefore be difficult.

13.5 Jurisdictional Problems

The victim, bank, accused person, mobile number and recipient account may be located in different States or even different countries. Cybercrime therefore challenges traditional territorial approaches to investigation.

13.6 Digital Evidence Problems

Electronic evidence can be technically complex. Investigators require specialised knowledge to collect and interpret transaction logs, device information, digital communications and other records.

13.7 Recovery of Money

Punishing the offender does not automatically guarantee recovery of the victim's money.

Financial recovery requires rapid tracing and freezing of funds.

13.8 Coordination Between Institutions

Effective action requires banks, police, cybercrime units, telecom companies, payment systems and other institutions to work together. Delays or gaps in coordination can reduce the possibility of recovery.

The RBI itself has recognised cybersecurity as a major operational risk and has continued to strengthen fraud-risk and cyber-resilience measures.[17]

13.9 Investigation Process

The investigation of online banking fraud generally involves registration of the complaint, collection of bank and transaction records, tracing the fraudulent account and digital identifiers, freezing the suspected funds, collecting and preserving electronic evidence, identifying and arresting the accused, and filing the charge-sheet before the court.

13.10 Investigation Loopholes

Major loopholes in investigation include delay in investigation, lack of specialised cybercrime skills, difficulty in tracing fake identities and mule accounts, cross-jurisdictional issues, inadequate digital forensic facilities, and poor coordination between banks, police and other agencies. These difficulties may delay identification of offenders and recovery of the victim’s

[17] Reserve Bank of India, *Annual Report 2024–25*, paras. VI.82–VI.83 (discussing cyber-security measures and revised fraud-risk management).

money.

14. DATA PROTECTION AND ONLINE BANKING FRAUD

The **Digital Personal Data Protection Act, 2023 (DPDP Act)** Online banking involves the collection and processing of customers' personal and financial information for purposes such as KYC, authentication, and transactions. The **Digital Personal Data Protection Act, 2023** provides a legal framework for protecting digital personal data and requires data fiduciaries to take reasonable security safeguards against personal data breaches.

A data breach can expose customer information, which may later be misused by fraudsters for phishing, fake calls, identity theft, and other banking scams. Therefore, **data protection and banking cybersecurity are closely connected**. At the same time, banks and law-enforcement agencies must be able to access relevant information for investigating fraud and tracing offenders. The earlier **Information Technology Act, 2000, § 43A** also addressed compensation for failure to protect sensitive personal data in specified circumstances.

Thus, effective prevention of online banking fraud requires an integrated approach combining **data protection, cybersecurity, identity protection, banking regulation, fraud monitoring, and criminal investigation**.[18]

15. HYPOTHESIS ANALYSIS

The hypothesis of this research is: **"Greater public awareness, stronger cybersecurity, and faster reporting and investigation can reduce online banking fraud in India."**

After studying the legal framework and practical challenges, the hypothesis can be considered **proved to a large extent**. Online banking fraud often takes place because customers are not fully aware of phishing links, fake calls, OTP scams, and other methods used by fraudsters. Therefore, public awareness can help customers identify suspicious activities and avoid becoming victims. At the same time, strong cybersecurity measures by banks are important to detect and prevent unauthorized transactions. RBI has also introduced security and customerprotection measures for digital banking.

[18] Digital Personal Data Protection Act, 2023, Act No. 22 of 2023, India Code.

Faster reporting is also very important. When a customer reports fraud quickly to the bank or through the national cybercrime helpline **1930**, there is a better opportunity to take action against the fraudulent transaction. Therefore, awareness alone is not enough; it must be supported by effective cybersecurity, quick reporting, and proper investigation.

Thus, on the basis of this study, the hypothesis is **proved**. A combination of **public awareness, stronger cybersecurity, and quick reporting and investigation** can significantly help in reducing the impact of online banking fraud, although it cannot completely eliminate such fraud.

16. CONCLUSION AND SUGGESTIONS

16.1 Conclusion

Online banking has made financial transactions faster and easier, but it has also increased the risk of phishing, OTP fraud, identity theft and unauthorized transactions. India has several legal and regulatory measures to deal with these problems, including the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Sakshya Adhiniyam, 2023 and RBI regulations. However, the main challenge is not only the availability of laws but their **effective implementation**.

The study shows that quick reporting, proper investigation, strong cybersecurity and public awareness are essential for reducing online banking fraud. RBI guidelines also provide protection to customers in certain cases of unauthorized transactions and require banks to take appropriate security measures. Therefore, prevention and immediate response should be given equal importance along with punishment of offenders.

16.2 Suggestions

1. **Increase Public Awareness:** Banks should regularly educate customers about phishing, OTP fraud, fake calls, malicious links and remote-access scams. Awareness programmes should be provided in simple and regional languages.

2. **Strengthen Cybersecurity:** Banks should use stronger fraud-detection systems, transaction monitoring, multi-factor authentication and security alerts to identify suspicious transactions at an early stage.

3. **Quick Reporting of Fraud:** Banks should provide an easy **"Report Fraud"** facility through mobile banking and internet banking so that customers can report unauthorized transactions immediately.

4. **Better Coordination Between Banks and Police:** Banks, cybercrime authorities and police should share information quickly to trace fraudulent transactions, identify offenders and prevent further loss.

5. **Improve Customer Protection and Recovery:** Banks should provide clear information about customer liability and take immediate steps after receiving a fraud complaint, including appropriate action to prevent further unauthorized transactions.

REFERENCES / BIBLIOGRAPHY

A. STATUTES AND REGULATIONS

1. Information Technology Act, 2000.
2. Bharatiya Nyaya Sanhita, 2023.
3. Bharatiya Nagarik Suraksha Sanhita, 2023.
4. Bharatiya Sakshya Adhiniyam, 2023.
5. Digital Personal Data Protection Act, 2023.

B. RBI MATERIALS

1. 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 (July 6, 2017).

2. Reserve Bank of India, *Master Direction on Digital Payment Security Controls*, RBI/2020-21/74, DoS.CO/CSITE/SEC.No.1852/31.01.015/2020-21 (Feb. 18, 2021).

3. Reserve Bank of India, *Master Directions on Fraud Risk Management in Commercial Banks (including Regional Rural Banks) and All India Financial Institutions*, RBI/DOS/2024-25/118, DOS.CO.FMG.SEC.No.5/23.04.001/2024-25 (July 15, 2024).

4. Reserve Bank of India, *Annual Report 2024–25*.

C. IMPORTANT CASE LAW / JUDICIAL MATERIAL

1. *HDFC Bank Ltd. v. Leela Bharati*, (2024).
2. *Pallabh Bhowmick v. The Ombudsman, Reserve Bank of India*, 2022.

D. GOVERNMENT / ONLINE SOURCES

20. National Cyber Crime Reporting Portal, Government of India.
21. Reserve Bank of India, official website and regulatory publications.
22. India Code, Government of India.