International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Digital Banking Fraud and Regulatory Liability in India: Towards a Unified Consumer-Centric Legal Framework

Sowmya B M

2nd Sem LLM, School of Law, Governance and Public Policy, Chanakya University, Devanahalli, Bangalore Rural

Abstract

Digital banking and financial technology (FinTech) have transformed India's financial ecosystem by widening access, lowering transaction costs, and accelerating financial inclusion. At the same time, they have generated novel vulnerabilities, including phishing, SIM-swap fraud, UPI manipulation, malware-based intrusions, and emerging "digital arrest" scams that strain legacy liability doctrines and regulatory arrangements. This article offers a doctrinal and comparative analysis of digital banking fraud in India, examining statutory provisions, Reserve Bank of India (RBI) guidelines, judicial decisions, and the underdeveloped role of cyber insurance in loss allocation. It argues that India's framework is fragmented, underenforced, and insufficiently consumer-centric compared to regimes in the United Kingdom, the United States, and the European Union, where stricter institutional liability standards and reverse burdens of proof are increasingly used. Building on this analysis, the article proposes a unified legal regime for digital banking fraud that incorporates the statutory codification of RBI norms, reverse or strict liability for unauthorised transactions, integrated data protection and cybersecurity obligations, specialised dispute resolution mechanisms, and the structured use of cyber insurance. The study contributes to the literature on digital financial regulation in the Global South by reframing digital banking fraud as a systemic regulatory problem rather than an individual contractual dispute and by outlining a reform model that seeks to balance innovation, inclusion, and consumer protection.

Keywords: digital banking; cyber fraud; RBI; Consumer protection; FinTech regulation, banking liability, cyber insurance, and India

1. Introduction

The Indian banking sector has undergone a structural transformation with the advent of digital technologies, particularly in the post-2010 era. The advent of innovations such as the Unified Payments Interface (UPI), mobile banking, artificial intelligence-driven financial services, and digital wallets has reconfigured the access and delivery of financial services. These developments have significantly furthered financial inclusion and transactional efficiency but have simultaneously increased the exposure of consumers and financial institutions to cyber risks, such as data breaches and fraud, which can undermine trust in digital financial systems.

Digital banking fraud has emerged as a central challenge in contemporary financial law and regulation. Unlike traditional banking fraud, centred on forged instruments or in-branch misappropriation, digital

fraud is characterised by anonymity, speed, cross-border reach, and technological complexity, which complicates detection, attribution, and remediation. The proliferation of sophisticated scams—including phishing and vishing, SIM-swap attacks, malware-enabled account takeovers, UPI-based manipulation, and coercive "digital arrest" schemes—raises fundamental questions about the adequacy of existing legal frameworks and the allocation of loss between banks, customers, intermediaries, and the state.

This article addresses a core question of banking and financial regulation: who should bear liability for losses arising from digital banking fraud in India—banks and payment service providers, customers, intermediaries such as telecom operators and FinTech platforms, or the state through regulatory design and oversight? Answering this question requires an integrated analysis of general banking statutes, cyber-law provisions, consumer-protection legislation, RBI circulars, and judicial approaches to negligence, consent, and burden of proof.

Indian legal scholarship has often treated digital banking fraud either as an extension of conventional cybercrime or as a narrow issue within private-law doctrines of contract and negligence. This article departs from that approach in three respects. First, it conceptualises digital banking fraud as a systemic, multi-stakeholder regulatory risk rather than merely an individual mistake between the bank and the customer. Secondly, it combines doctrinal analysis of Indian statutes, RBI circulars, and case law with a structured comparison of liability regimes in the United Kingdom, United States, and European Union to identify alternative regulatory models and benchmarks. Thirdly, it foregrounds the underexplored role of cyber insurance within a broader public-law architecture of risk allocation and accountability (Gupta, 2021; Srinivasan, 2019), particularly in how it can mitigate financial losses and enhance accountability in the event of cyber incidents.

Methodologically, the study adopts a doctrinal and comparative approach. It analyses statutory instruments, including the Reserve Bank of India Act 1934, the Banking Regulation Act 1949, the Information Technology Act 2000, the Consumer Protection Act 2019, and the Indian Contract Act 1872 (Government of India, 1872, 1934, 1949, 2000, 2019), alongside RBI guidelines on customer liability, cybersecurity, and digital payments (Reserve Bank of India, 2017, 2021, 2023). It further examines key judicial decisions on banking liability and confidentiality—such as State Bank of India v. Shyama Devi (1978), Canara Bank v. Union of India (2017), and Justice K.S. Puttaswamy v. Union of India (2017)—and draws on comparative materials relating to the Electronic Fund Transfer Act (EFTA) and Regulation E in the United States (Consumer Financial Protection Bureau, 2021), the Payment Services Regulations and voluntary reimbursement schemes in the United Kingdom (Financial Conduct Authority, 2020), and the Second Payment Services Directive (PSD2) and related data-protection norms in the European Union (European Commission, 2018).

The article proceeds in ten parts. Section 2 briefly traces the evolution of banking regulation in India to show how regulatory responses have historically lagged structural change. Section 3 maps the nature and typology of digital banking frauds, emphasising their systemic features and implications for liability design. Section 4 analyses the existing Indian legal framework governing digital banking fraud, highlighting statutory and regulatory fragmentation. Section 5 examines judicial approaches to banking liability in fraud cases and identifies emerging trends in digital contexts. Section 6 outlines doctrinal and regulatory challenges posed by digital fraud to conventional concepts of consent, negligence, and burden of proof. Section 7 considers the role and limitations of cyber insurance as a risk-sharing mechanism. Section 8 presents a comparative analysis of liability regimes in the UK, US, and EU. Section 9 presents

reform proposals for a unified, consumer-centric regime to address digital banking fraud in India, while Section 10 provides the conclusion.

2. Evolution of Banking Regulation in India

2.1 Pre-nationalisation

The evolution of Indian banking regulation reflects the broader trajectory of the country's economic and institutional development. Before nationalisation, the banking system was characterised by minimal regulatory intervention and dominated by private banks, many of which were closely linked to industries and business groups (Tannan, 2017). The absence of robust prudential standards and supervisory mechanisms produced frequent bank failures, poor governance, and low depositor confidence.

The establishment of the Reserve Bank of India in 1934 marked an important step towards centralised monetary regulation, but its early role remained largely confined to monetary policy rather than comprehensive supervision (Government of India, 1934). The enactment of the Banking Regulation Act 1949 significantly strengthened oversight by introducing licensing, capital requirements, and supervisory powers over management and operations (Government of India, 1949). Nevertheless, banking services remained heavily urbanised, with the rural and agricultural sectors largely excluded, and the nexus between banks and industrial houses contributed to imprudent lending in the absence of effective depositor protection schemes, which ultimately led to financial instability and limited credit access for underserved populations.

2.2 Nationalisation and "social banking"

The nationalisation of major commercial banks in 1969, followed by a second phase in 1980, marked a decisive turn toward state-led banking policies (Tannan, 2017). Nationalisation aims to align banking operations with distributive objectives, such as financial inclusion, poverty alleviation, and sectoral credit targeting. It facilitated a major expansion of branch networks into rural and semi-urban areas, improving access to banking services for previously underserved populations.

During this period, "social banking" became central, and the RBI's regulatory role expanded to encompass directed credit, interest-rate regulation, and priority-sector lending. However, heightened political interference, reduced managerial autonomy, and weak risk management practices fuel rising non-performing assets and declining profitability, revealing the limitations of a heavily state-dominated model, which ultimately undermines the effectiveness of social banking initiatives and the overall stability of the financial system.

2.3 Liberalisation and prudential regulation

Economic liberalisation in the early 1990s was another turning point. In response to a balance-of-payments crisis, the government adopted reforms aimed at enhancing efficiency, competition, and financial stability. The Narasimham Committee Reports recommended a transition from direct controls to prudential regulation and risk-based supervision, including capital-adequacy norms, income-recognition and asset-classification standards, and reduced statutory pre-emptions (Narasimham Committee, 1991, 1998). These reforms, combined with the adoption of Basel standards and later the Insolvency and Bankruptcy Code 2016 (Government of India, 2016), reoriented the framework towards market-based discipline and institutional resilience. The entry of new private and foreign banks increased competition and innovation, though asset-quality issues and corporate defaults continued to pose systemic risks (Singh, 2018).

2.4 Digital transformation and regulatory lag

Rapid technological change and the emergence of digital financial services, including mobile banking,

UPI (Unified Payments Interface), digital wallets, and AI-based solutions, define the contemporary phase. Government initiatives such as Digital India and the Pradhan Mantri Jan Dhan Yojana have accelerated the uptake of digital payment systems and expanded access to formal finance (Reserve Bank of India, 2023). At the same time, cyber fraud, data breaches, and unauthorised electronic transactions have exposed significant vulnerabilities in the digital banking ecosystem, leading to concerns about consumer trust and a need for stronger security measures to protect users.

Existing regulatory frameworks, designed primarily for analogue operations, struggle to address the complexities of digital transactions, especially liability allocation, data protection, and the regulation of non-bank FinTech entities (Gupta, 2021). The main trend is that regulations have been slow to catch up with changes in the sector's technology and risk profile, leading to significant gaps in addressing emerging issues such as cybersecurity threats and consumer protection in digital transactions. This trajectory is central to understanding why digital banking fraud currently sits within a fragmented and conceptually outdated legal framework, which fails to adequately address the complexities and rapid evolution of digital financial services and the associated risks.

3. Nature and Typology of Digital Banking Frauds

In India, digital banking fraud operates within a technologically complex and often borderless environment, exploiting infrastructure and behavioural vulnerabilities. It is a systematic risk capable of eroding consumer confidence and destabilising trust in digital financial systems. Recent data indicate a notable rise in unauthorised electronic transactions and cyber-enabled financial frauds, especially in UPI-based payments and identity theft cases (Reserve Bank of India, 2023).

3.1 Phishing and vishing

Phishing and vishing remain among the most prevalent forms of digital banking fraud. They rely on deceptive communications—via email, SMS, or voice calls—designed to induce users to disclose passwords, PINs, and one-time passwords. These attacks typically impersonate banks or government authorities and deploy social-engineering techniques that exploit trust, urgency, and fear.

Legally, phishing and vishing raise difficult questions about consent and negligence. Banks often argue that customers voluntarily disclosed credentials and therefore bear responsibility, while customers contend that their apparent consent was vitiated by misrepresentation or coercion. This ambiguity complicates the application of doctrines under the Indian Contract Act 1872 and related negligence principles (Government of India, 1872).

3.2 SIM-swap fraud

SIM-swap fraud involves fraudsters gaining control of a victim’s mobile number, often by obtaining a duplicate SIM through forged documents or collusion. Once in control, they intercept OTPs (one-time passwords) and authentication messages, gaining access to accounts and digital wallets. This form of fraud illustrates the interdependence between banking institutions and telecom service providers, yet current law provides no clear standards for telecom operator liability, producing regulatory gaps and disputes over responsibility.

3.3 Malware and device-based attacks

Malware-based attacks deploy malicious software embedded in applications, links, or compromised websites to infiltrate user devices and harvest financial data or manipulate transactions in real time. The increasing reliance on smartphones, combined with uneven cyber hygiene, heightens risk, particularly as users often neglect to update their software or use strong passwords, making their devices more vulnerable

to malware attacks. From a liability standpoint, these attacks complicate the assignment of fault: banks might contend that customers neglected to secure their devices, whereas customers might assert that banks have a responsibility to establish monitoring systems capable of identifying unusual activity. This tension reveals the limits of bilateral negligence frameworks.

3.4 UPI and real-time payment fraud

UPI has revolutionised retail payments by enabling instant, low-cost transfers, but its speed and irreversibility have also made it fertile ground for fraud, such as fraudulent collect requests, QR code manipulations, and social engineering schemes that induce users to authorise transfers. Once executed, UPI payments are often practically irreversible, limiting prospects for recovery even when fraud is swiftly reported (Reserve Bank of India, 2017).

The legal challenge is to reconcile the efficiency and finality of real-time systems with robust consumer protection and ex post remedies. The existing law lacks clear statutory rules for default liability for unauthorised UPI transactions, leaving RBI circulars and contractual terms carrying much of the burden.

3.5 Digital "arrest" scams and hybrid fraud

Digital "arrest" scams involve fraudsters impersonating law-enforcement or regulatory officials to coerce victims into transferring funds under threat of prosecution or detention. Fraudsters often execute these schemes through video calls or spoofed communication channels, combining elements of cybercrime, impersonation, and psychological coercion. Such frauds make it hard to tell the difference between legitimate and illegitimate transactions, as victims often approve payments due to fear and false information, which complicates liability rules that depend on clear consent.

3.6 Systemic features and implications

Across these modalities, three systemic features are salient for liability design: pronounced information asymmetry between users and system operators, dense interdependencies among banks, payment service providers, fintech platforms, and telecom operators, and social engineering techniques that blur the line between authorised and unauthorised transactions. Micro-level fault and individual negligence doctrines structurally misalign with the way harm occurs in digital ecosystems. A framework that continues to treat the bank-customer relationship as a two-party contractual arrangement risks misallocating losses and underincentivising systemic risk mitigation, particularly because it overlooks the interconnected nature of digital ecosystems, where multiple parties contribute to and share in the risk of harm.

4. Legal Framework Governing Digital Banking Fraud in India

India's legal framework is multi-layered and fragmented, spanning banking legislation, cyber-law provisions, consumer-protection statutes, contractual doctrines, and RBI guidelines. Taken together, these instruments provide a patchwork of protections, but they do not establish a coherent regime that directly articulates liability rules for unauthorised digital transactions (Gupta, 2021; Singh, 2018), leaving consumers vulnerable to fraud and disputes regarding accountability in such transactions.

4.1 Statutory framework

Key statutes include the Reserve Bank of India Act 1934, the Banking Regulation Act 1949, the Information Technology Act 2000, the Consumer Protection Act 2019, and the Indian Contract Act 1872 (Government of India, 1872, 1934, 1949, 2000, 2019). The RBI Act and the Banking Regulation Act focus more on institutional authorisation, prudential standards, and supervisory powers than on detailed consumer-side liability rules for electronic fraud (Tannan, 2017). The IT Act provides penal provisions concerning unauthorised access, data theft, and computer-related offences (sections 43 and 66), but it is

predominantly criminal in orientation and does not specify civil liability standards or compensation mechanisms tailored to digital banking fraud.

The Consumer Protection Act 2019 extends consumer-protection principles to electronic commerce and service delivery, but its application to digital banking disputes has been ad hoc. The Indian Contract Act continues to govern bank–customer relationships as debtor–creditor arrangements, with doctrines of free consent, misrepresentation, and negligence providing the basic toolkit. These doctrines presuppose relatively direct and transparent interactions and struggle with technologically mediated, multi-intermediary frauds, such as those involving online banking scams or phishing attacks that complicate the traditional understanding of consent and misrepresentation.

4.2 RBI regulations and customer liability guidelines

As the primary banking regulator and payments overseer, the RBI has issued several circulars and guidelines on cybersecurity, digital payments, and customer liability. A key instrument is the framework that categorises customer liability into "zero", "limited", and "full" based on reporting timelines, system deficiencies, and customer negligence (Reserve Bank of India, 2017). This reflects a move toward a more consumer-protective approach, which recognises that customers should not bear losses from systemic failures or third-party breaches beyond their control.

However, RBI guidelines lack the formal status of primary legislation and are difficult to enforce directly in judicial proceedings. Their normative authority is strong in regulatory practice but weaker in private litigation, leaving scope for banks to interpret or limit their application in individual cases, which can lead to inconsistencies in how regulations are applied across different banks and situations.

4.3 Cybersecurity and payment-system regulations

The RBI has also provided guidelines on cybersecurity, IT management, and security measures for digital payments for the organisations it regulates, which include rules for using multi-factor authentication, encryption, monitoring risks, and reporting incidents (Reserve Bank of India, 2021). These measures are essential for ex ante risk reduction but focus largely on institutional processes rather than ex post liability allocation and consumer compensation. They adopt an institution-centric perspective, prescribing internal controls without fully addressing how failures should translate into concrete liability for users.

4.4 Judicial approaches to banking liability

Indian courts have long recognised a duty of care owed by banks to their customers, grounded in contracts and negligence. In State Bank of India v. Shyama Devi (1978), the Supreme Court held banks liable for unauthorised withdrawals resulting from their own negligence, underscoring their obligation to verify transactions and protect accounts. In Canara Bank v. Union of India (2017), the Court emphasised confidentiality and data protection in banking operations, reinforcing the fiduciary dimension of the bank–customer relationship.

However, these precedents emerged in conventional banking contexts and do not directly address the complexities introduced by multi-factor authentication, algorithmic decision-making, third-party platforms, and real-time payments, which are critical factors in understanding the evolving landscape of digital fraud and consumer protection. Recent High Court decisions in digital fraud cases indicate growing sympathy for consumers, but doctrine remains unsettled and heavily fact-specific.

4.5 Intermediary liability and regulatory gaps

Digital transactions involve multiple intermediaries, including payment gateways, FinTech platforms, card networks, and telecom operators. Indian law lacks a clear, horizontally applicable framework assigning responsibilities and liabilities across these actors. In SIM-swap fraud, telecom operators play a critical

role, yet their obligations and potential liability are not clearly defined in telecom regulation or general financial law. Regulatory fragmentation produces overlapping jurisdictions and enforcement gaps across bodies such as RBI, the Ministry of Electronics and Information Technology, and the Telecom Regulatory Authority of India, often leaving consumers facing conflicting narratives of responsibility.

4.6 Data protection and privacy

Data protection is central because unauthorised access to personal and financial data often constitutes the first step in fraud. While the IT Act and associated rules impose certain obligations concerning data security and “reasonable security practices," India has yet to fully operationalise a comprehensive data protection statute comparable to the GDPR (Government of India, 2000; European Commission, 2018). Justice K.S. Puttaswamy v. Union of India (2017) recognises privacy as a fundamental right, underscoring the constitutional importance of data protection, but the statutory translation into specific duties and remedies for digital banking remains incomplete.

4.7 Fragmentation and absence of a unified regime

Taken together, these statutory, regulatory, and judicial elements form a patchwork rather than a coherent regime. No single instrument explicitly establishes a default liability standard for unauthorised electronic banking transactions or a unified framework for allocating losses among banks, customers, and intermediaries. Instead, RBI circulars and case-by-case judicial reasoning fill the gap, undermining predictability and contrasting sharply with dedicated statutory arrangements such as the EFTA/Regulation E in the US or PSD2 in the EU (Consumer Financial Protection Bureau, 2021; European Commission, 2018), which provide clear guidelines and protections for consumers in electronic banking transactions.

5. Judicial Approach to Banking Liability in Digital Fraud Cases

The judiciary occupies a central position in shaping banking liability, particularly where legislative and regulatory frameworks are incomplete. Traditionally, courts have approached banking liability through doctrines of contract, negligence, and duty of care, developed in paper-based and branch-based banking contexts (Singh, 2018).

5.1 Traditional approach and its limits

Historically, the bank-customer relationship has been characterised as one between a debtor and a creditor, underpinned by a contract and accompanied by a duty of reasonable care in executing customer mandates. Banks are expected to check for unusual signatures, verify instruments, and protect accounts from obvious fraud. If they don't, they could be found negligent (State Bank of India v. Shyama Devi, 1978; Tannan, 2017). These principles work tolerably well for forged cheques or manual withdrawals but are harder to apply in digital environments, where the rapid evolution of technology and sophisticated cyber fraud techniques can complicate detection and verification processes, leading to increased risks for banks and their customers if adequate measures are not implemented.

Multi-factor authentication, algorithmic decision-making, and automated real-time payments complicate the question of what constitutes reasonable care and make it unclear at which point in a distributed system negligence, if any, should be located.

5.2 Application to digital transactions

In digital fraud cases, courts increasingly encounter three competing narratives. Banks typically argue that robust authentication mechanisms were in place and that any breach resulted from the customer’s disclosure of credentials or failure to maintain device security. Customers contend that they were deceived through sophisticated social engineering or technical attacks and did not understand or control the systems

executing transactions. Intermediaries often claim they merely provide technical infrastructure without direct control over user conduct, yet this raises questions about their responsibility in ensuring the security and transparency of the systems they support.

Judgements in such cases are highly fact-specific, with courts scrutinising the sequence of events to determine whether customer conduct was negligent and bank systems were reasonably secure. The notion of reasonable care thus becomes the focal point for liability allocation, yet its interpretation remains fluid and technologically under-specified, particularly as new banking technologies and security measures continue to evolve and challenge existing legal frameworks.

5.3 Burden of proof and evidentiary asymmetries

One of the most difficult issues in digital banking litigation is the allocation of the burden of proof. Traditionally, customers must prove a transaction was unauthorised and that they acted responsibly. In digital contexts, this requirement clashes with significant informational asymmetries: relevant logs, configurations, and forensic data lie almost entirely with banks and service providers, while customers lack both access and expertise.

Courts that adhere strictly to traditional burden rules risk placing an unrealistic evidentiary burden on consumers, effectively precluding relief. Some High Court decisions suggest a willingness to soften or shift the burden where the bank controls the evidence needed to explain how a disputed transaction occurred, but a clear and uniform doctrinal approach has yet to emerge, leaving consumers uncertain about their rights and the standards that will be applied in such cases.

5.4 Role of RBI guidelines

RBI circulars on customer liability and digital-payment security have begun to influence judicial reasoning, even though they lack the status of primary legislation (Reserve Bank of India, 2017, 2021). Courts sometimes use the RBI classification of zero, limited, and full customer liability as a normative benchmark when assessing whether a bank should reimburse a victim. At the same time, the non-statutory nature of these guidelines leaves their application open to judicial discretion. Banks may invoke RBI frameworks to limit exposure by emphasising customer negligence or delayed reporting, while customers cite them as arguments for zero liability in cases involving systemic flaws or third-party breaches.

5.5 Emerging trends and doctrinal gaps

Recent trends indicate a gradual but uneven shift toward a more consumer-centric approach, particularly where customers appear to have been victims of sophisticated fraud rather than gross negligence. Courts have stressed the duty of banks to implement robust security systems and respond promptly to fraud reports, and some have indicated that mere interaction with a fraudster—such as sharing an OTP under deception—should not automatically bar relief. Yet doctrinal gaps remain substantial: there is no authoritative Supreme Court judgement directly addressing contemporary digital banking fraud, nor is there a settled standard for shifting or reversing the burden of proof. Jurisprudence remains in a transitional phase.

6. Doctrinal and Regulatory Challenges

Digital banking fraud exposes core tensions between traditional legal doctrines and technologically mediated financial systems. These tensions manifest in questions of consent and voluntariness, negligence and reasonable care, attribution of fault in multi-party systems, and the interface between private law and public regulation (Gupta, 2021).

6.1 Inadequacy of traditional consent and negligence

Classical contract law assumes parties possess sufficient information and autonomy to provide free and informed consent and that negligence can be evaluated against a stable notion of reasonable care. In digital fraud scenarios, these assumptions often break down. Customers may authorise transactions or share credentials under false pretences, coercion, or severe informational asymmetry, such as in phishing or digital arrest scams. Treating such consent as legally unimpeachable ignores the manipulative conditions under which it was obtained.

Negligence standards premised on a generic reasonable person may also be ill-suited where technical complexity is high and digital literacy uneven. Expecting ordinary users to understand evolving fraud vectors and maintain perfectly secure practices risks normalising a level of care more appropriate to professional system operators than lay consumers, which could lead to increased vulnerability and potential harm for those who lack the necessary technical knowledge.

6.2 Ambiguity in multi-stakeholder ecosystems

Digital banking ecosystems involve banks, payment service providers, FinTech platforms, telecom operators, card networks, and outsourced IT firms. Fraud may arise from vulnerabilities at any point or from interactions among them, such as when a payment service provider's system is compromised, affecting the security of transactions processed by banks and FinTech platforms. Indian law offers no general framework for allocating liability across these stakeholders. In the absence of such a framework, disputes devolve into mutual blame-shifting, with each actor emphasising the responsibility of others and the customer. RBI guidelines partly address banks and regulated payment providers but do not comprehensively cover all intermediaries or resolve deeper questions about primary versus residual liability (Reserve Bank of India, 2017), which can lead to ongoing disputes and confusion regarding accountability in financial transactions.

6.3 Regulatory fragmentation and coordination

Regulatory oversight is split across the RBI, the Ministry of Electronics and Information Technology, the Telecom Regulatory Authority of India, and consumer-protection fora, each operating under distinct mandates. This fragmentation generates overlapping jurisdictions, conflicting priorities, and gaps in enforcement—particularly in cross-sectoral frauds such as SIM swaps or multi-channel scams. Without mechanisms for information-sharing, joint standard-setting, and integrated enforcement, regulators risk working at cross-purposes, which can lead to ineffective responses to fraud and ultimately allow fraudulent activities to proliferate unchecked.

6.4 Weak enforceability of non-statutory norms

RBI circulars and guidelines structure digital-payment security and customer-liability norms, yet their enforceability is limited compared to statutes. While banks must comply as a matter of regulatory obligation, individual consumers may find it difficult to rely on these guidelines as independent causes of action in court. This creates a paradox: some of the most detailed norms governing digital banking fraud exist outside the core corpus of enforceable private-law rights and remedies, leaving significant discretion to courts and tribunals, which may lead to inconsistent rulings and uncertainty for consumers seeking justice.

6.5 Data protection, privacy, and cybersecurity gaps

Digital banking fraud is often precipitated by failures in data protection and cybersecurity, yet Indian law still lacks a fully implemented, comprehensive data-protection regime with clear obligations and sanctions (Government of India, 2000; Justice K.S. Puttaswamy v. Union of India, 2017). Existing IT Act provisions

and rules impose certain security requirements but do not articulate granular duties tailored to financial-sector data flows, which leaves significant vulnerabilities in the protection of sensitive financial information and fails to address the specific risks associated with digital banking fraud. This gap weakens both ex ante incentives for robust data protection in banking and ex post remedies for individuals whose data has been compromised, leading to increased risks of data breaches and insufficient recourse for affected customers.

6.6 Technological asymmetry and consumer vulnerability

A pronounced technological and informational asymmetry exists between financial institutions and ordinary users. Banks and service providers design, deploy, and control digital infrastructures, whereas customers interact only with user-facing interfaces and have limited capacity to detect or mitigate systemic vulnerabilities. A liability framework that treats these parties as equally positioned in knowledge and control risks entrenching unfair burdens on consumers. This asymmetry strongly justifies shifting the primary risk of digital fraud onto system operators and embedding consumer-protection principles within liability rules.

7. Cyber Insurance and Allocation of Digital Banking Risk

Cyber insurance has emerged globally as an instrument for transferring or sharing financial risks associated with cyber incidents, including data breaches and certain types of digital fraud (Srinivasan, 2019). In digital banking, insurance arrangements can affect how losses are ultimately borne among banks, customers, and insurers, particularly by influencing the incentives for risk management practices and the allocation of liability in the event of a cyber incident.

In India, the cyber-insurance market remains nascent, with limited penetration among retail consumers and uneven coverage of digital banking risks. Banks sometimes offer bundled insurance products with digital accounts and payment services, but terms, exclusions, and claim procedures vary widely and may not be well understood by customers, leading to potential gaps in coverage and unexpected financial liabilities in the event of a cyber incident.

From a regulatory perspective, insurance can serve as a complementary mechanism within a broader risk-allocation architecture but cannot substitute for clear primary rules of liability. Poorly designed products may even undermine incentives for robust security if they encourage risk externalisation without adequate constraints. Public-law considerations should guide the integration of cyber insurance into the legal framework for digital banking fraud. Regulators should encourage standardised and transparent policy terms, ensure that coverage does not erode baseline liability obligations for banks and intermediaries, and consider targeted incentives for products that enhance consumer protection (Srinivasan, 2019).

8. Comparative Perspectives: UK, US, and EU

Comparative experience offers insights into alternative models for allocating liabilities to digital payment systems and protecting consumers against unauthorised transactions. While direct transplantation into the Indian context is not feasible, the UK, US, and EU exemplify distinct strategies for consumer protection in digital payment systems, such as the UK's strong regulatory framework, the US's emphasis on consumer education, and the EU's comprehensive legal protections against unauthorised transactions (Consumer Financial Protection Bureau, 2021; the European Commission, 2018; the Financial Conduct Authority, 2020).

8.1 United Kingdom

In the UK, liability for unauthorised electronic payments is governed primarily by the Payment Services Regulations (PSRs), which implement EU directives, supplemented by regulatory guidance and voluntary industry codes. As a general rule, payment service providers must promptly refund unauthorised transactions, subject to limited exceptions for fraud or gross negligence by the user (Financial Conduct Authority, 2020).

Recently, the focus has shifted to authorised push-payment scams, where fraudsters deceive consumers into initiating payments. The Contingent Reimbursement Model (CRM) Code, though voluntary, establishes a framework under which participating firms commit to reimbursing victims who meet specified standards of care. This reflects a shift toward recognising the systemic and psychological dimensions of digital fraud and away from a narrow focus on user faults.

8.2 United States

In the US, the Electronic Fund Transfer Act (EFTA) and its implementing Regulation E provide detailed rules on consumer liability for unauthorised electronic fund transfers (Consumer Financial Protection Bureau, 2021). Liability caps are tied to how quickly consumers report unauthorised activity, with lower caps for prompt reporting and a higher potential liability for delay. Financial institutions must investigate disputes and provisionally credit disputed amounts pending resolution.

This statutory framework offers clear timelines and procedures for error resolution and grants consumers enforceable rights against financial institutions. Although debates persist over adequacy in light of new fraud typologies, the EFTA illustrates the benefits of a dedicated statute explicitly addressing electronic transfer liability, such as providing consumers with protections against unauthorised transactions and ensuring the timely resolution of disputes.

8.3 European Union

In the EU, PSD2 and related instruments establish a harmonised regime for payment services, including strong customer-authentication requirements and detailed rules on unauthorised transactions (European Commission, 2018). Payment service providers must refund unauthorised transactions by default, with limited scope to hold consumers liable in cases of proven fraud or gross negligence. Providers bear the burden of demonstrating that a transaction was authenticated and correctly executed and that no technical failure occurred.

PSD2 is supplemented by robust data-protection obligations under the GDPR, creating an integrated framework in which payment security and data protection are mutually reinforcing. This integration recognises that protecting personal data is central to preventing and mitigating digital financial fraud.

8.4 Comparative observations

A brief comparison highlights key contrasts with India:

Jurisdiction	Default consumer liability	Burden of proof	Key instruments	Distinctive feature
United Kingdom	Immediate reimbursement unless fraud/gross negligence	On banks to show fraud/negligence	PSRs; CRM Code; FCA rules	Explicit treatment of authorised push-payment fraud; strong consumer orientation
United States	Monetary caps tied to reporting timelines	Institution must investigate and substantiate authorisation	EFTA; Regulation E	Dedicated statute with detailed timelines and procedures
European Union	Full reimbursement unless fraud/gross negligence	Provider must show proper authentication and no system failure	PSD2; GDPR; national laws	Integration of payment security and data protection; strong SCA requirements
India	Circular-based categorisation without statutory backing	In practice, often on consumers to disprove negligence	RBI circulars; IT Act; general laws	Fragmented regime; weak enforceability; no dedicated statute

Leading jurisdictions tend to adopt clear statutory frameworks with default assumptions in favour of consumer reimbursement and to reverse or shift proof burdens. India, by contrast, relies largely on non-statutory regulatory guidance and general laws ill-suited to the specifics of digital payments, which can lead to confusion among consumers and hinder the growth of the digital payment ecosystem.

9. Towards a Unified, Consumer-Centric Legal Framework

The foregoing analysis suggests that India requires a more coherent and explicitly consumer-oriented framework for allocating liability in digital banking fraud. The reforms proposed here centre on three planks: dedicated, statutorily grounded liability rules; integrated data protection and cybersecurity obligations aligned with financial regulation; and specialised dispute resolution and risk-sharing mechanisms.

9.1 Dedicated legislation on digital banking fraud

A central reform priority is the enactment of dedicated legislation addressing digital banking and payment fraud, analogous to EFTA in the US or PSD2-derived frameworks in Europe (Consumer Financial Protection Bureau, 2021; European Commission, 2018). Such legislation should clearly define unauthorised electronic transactions, specify default rules for consumer liability, and codify the duties of banks and payment service providers. RBI's existing circulars on customer liability can serve as a starting point but require full statutory backing and refinement through legislative deliberation (Reserve Bank of India, 2017).

9.2 Reverse or strict liability and burden-of-proof rules

Given technological and informational asymmetries, a shift towards reverse or strict liability standards is normatively and practically justified. Banks and payment providers should bear the burden of proving that disputed transactions were duly authenticated, correctly executed, and not the result of systemic or security failure. Legislation should specify that when a customer disputes a transaction and reports it within a

reasonable time, the provider must promptly investigate and, absent proof of fraud or gross negligence by the customer, reimburse the loss. This would align Indian law more closely with UK and EU models.

9.3 Integrating data protection and cybersecurity with financial regulation

The development of a comprehensive data-protection framework must coordinate with reforms in financial regulation. Financial sector statutes and regulations should explicitly cross-reference and incorporate data protection duties, recognising that breaches of personal and financial data are key enablers of digital fraud (European Commission, 2018; Justice K.S. Puttaswamy v. Union of India, 2017). Regulators should align cybersecurity requirements, data-protection obligations, and payment-system rules to create a coherent set of ex ante duties on banks and FinTech providers. Non-compliance should attract regulatory sanctions and weigh heavily in liability determinations in favour of consumers.

9.4 Institutional coordination and unified oversight

To address regulatory fragmentation, India should consider establishing a formal coordination mechanism or lead authority for digital financial services, tasked with harmonising standards and overseeing cross-sectoral fraud risks. This could take the form of a specialised digital finance council or a strengthened inter-regulatory forum with clear mandates and information-sharing protocols. Such a body could develop unified guidelines on liability allocation across banks, telecoms, and other intermediaries and ensure that sector-specific regulations are coherent.

9.5 Specialised dispute-resolution mechanisms

Traditional courts and general consumer fora may lack the technical expertise and agility to handle complex digital-fraud disputes efficiently. India should therefore develop specialised mechanisms for digital financial fraud resolution, such as dedicated tribunals, ombudsman schemes, or online dispute resolution platforms with time-bound procedures. These mechanisms should be empowered to apply statutory liability rules, draw inferences from institutional control over evidence, and order speedy restitution (Gupta, 2021).

9.6 Structuring cyber insurance within a public-law framework

Cyber insurance should be integrated as a complementary tool rather than a substitute for regulation. Regulators may encourage standardised insurance products that cover specified categories of digital fraud with clear disclosure obligations and limits on exclusions. At the same time, legislation should ensure that insurance does not dilute the core liability obligations of banks and intermediaries or weaken security incentives. Public-law oversight of cyber-insurance markets can help align private risk-transfer mechanisms with broader regulatory goals (Srinivasan, 2019), such as enhancing the overall security posture of financial institutions and ensuring that they remain accountable for their cybersecurity practices.

9.7 Enhancing consumer awareness and digital literacy

No liability framework can fully compensate for systemic deficits in consumer awareness and digital literacy. Public authorities, banks, and civil society organisations should collaborate on sustained awareness campaigns focusing on prevalent fraud typologies and safe digital practices (Reserve Bank of India, 2023). Such initiatives should be treated as integral components of the regulatory response, complementing legal reforms. Improved digital literacy enhances the effectiveness of protective rules and helps reduce fraud incidence.

10. Conclusion

The digitalisation of India's banking sector has delivered substantial gains in access, efficiency, and inclusion but has also generated complex and rapidly evolving fraud risks that challenge existing legal

frameworks. India's current approach to digital banking fraud is characterised by statutory fragmentation, reliance on non-statutory guidelines, and judicial doctrines that have yet to fully adapt to the technological and systemic features of digital transactions (Gupta, 2021; Singh, 2018).

Traditional concepts of consent, negligence, and burden of proof, developed for analogue environments, struggle to account for social-engineering attacks, multi-intermediary transaction chains, and pervasive information asymmetries. RBI's efforts to protect customers through circulars on liability and cybersecurity are important but constrained by the absence of dedicated statutory backing and integrated data-protection norms (Reserve Bank of India, 2017, 2021), which limits their effectiveness in addressing the complexities of digital fraud and ensuring comprehensive consumer protection. Judicial responses, though increasingly sympathetic to consumers, remain episodic and doctrinally unsettled, and there is as yet no authoritative Supreme Court pronouncement that squarely addresses digital fraud, which leaves consumers vulnerable and uncertain about their legal protections in the digital space.

Comparative experience from the UK, US, and EU demonstrates the advantages of clear statutory regimes that adopt consumer-friendly default rules, reverse or shift burdens of proof, and integrate payment security with data protection obligations (Consumer Financial Protection Bureau, 2021; European Commission, 2018; Financial Conduct Authority, 2020). While Indian reforms must be context-sensitive, these models provide concrete reference points for developing consumer protection laws that enhance financial security and data privacy in India.

This article has argued for a paradigm shift toward a unified, consumer-centric, and technology-sensitive legal regime for digital banking fraud in India. Key elements include dedicated legislation on digital banking fraud, reversible or strict liability standards backed by clear evidentiary rules, integrated data protection and cybersecurity duties, coordinated institutional oversight, specialised dispute resolution mechanisms, and carefully structured cyber insurance markets (Gupta, 2021; Srinivasan, 2019). By redefining digital banking fraud as a systemic regulatory issue rather than an isolated contractual dispute, the proposed reforms seek to realign incentives, reduce consumer vulnerability, and strengthen trust in India's digital financial ecosystem.

Future research could extend this analysis through an empirical study of fraud-dispute patterns in courts and ombudsman schemes and a behavioural assessment of how different liability rules influence user conduct and institutional investment in security.

References

1. Consumer Financial Protection Bureau. (2021). Electronic Fund Transfer Act (Regulation E).
2. European Commission. (2018). Revised Payment Services Directive (PSD2).
3. Financial Conduct Authority. (2020). Payment services and consumer protection guidelines.
4. Government of India. (1872). Indian Contract Act.
5. Government of India. (1934). Reserve Bank of India Act.
6. Government of India. (1949). Banking Regulation Act.
7. Government of India. (2000). Information Technology Act.
8. Government of India. (2016). Insolvency and Bankruptcy Code.
9. Government of India. (2019). Consumer Protection Act.
10. Gupta, R. (2021). FinTech regulation and consumer protection in India. NUJS Law Review, 14(2), 123–145.
11. Narasimham Committee. (1991). Report on financial system.

12. Narasimham Committee. (1998). Banking sector reforms.
13. Reserve Bank of India. (2017). Customer protection – Limiting liability of customers in unauthorised electronic banking transactions.
14. Reserve Bank of India. (2021). Digital payment security controls.
15. Reserve Bank of India. (2023). Annual report.
16. Singh, A. (2018). Banking and negotiable instruments law. Eastern Book Company.
17. Srinivasan, M. (2019). Insurance law. Eastern Law House.
18. Tannan, M. L. (2017). Banking law and practice in India. LexisNexis.
19. State Bank of India v. Shyama Devi. (1978). AIR SC 1263.
20. Canara Bank v. Union of India. (2017). 2 SCC 666.
21. Justice K.S. Puttaswamy v. Union of India. (2017). 10 SCC 1.