VOLUME 6 | ISSUE 2

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

CONSUMER PROTECTION IN BANKING AND DIGITAL PAYMENTS IN INDIA: ASSESSING THE EFFICACY OF LEGAL AND REGULATORY SAFEGUARDS IN THE DIGITAL AGE

- Shreya Kashid[1]

Abstract

The proliferation of digital banking, Unified Payments Interface (UPI), mobile wallets and online payment services has transformed financial transactions in India. While these innovations offer speed, convenience and wider access, they have also exposed consumers to rising risks: unauthorized transactions, frauds, service failures, cheque dishonour and delays in grievance-redressal. This paper examines whether the existing laws and regulations in India provide adequate protection to consumers in banking and digital-payment services. It focuses on key statutes , the Consumer Protection Act, 2019, the Negotiable Instruments Act, 1881 as well as relevant guidelines issued by the Reserve Bank of India (RBI) and the Insurance Regulatory and Development Authority (IRDA). Drawing upon case law,[2] recent fraud data and regulatory documents, the study classifies prevalent consumer issues, assesses how regulatory bodies respond, and analyses the magnitude of consumer harm. The findings indicate that while the current legal framework offers several protections (such as restrictions on customer liability for some unauthorised digital transactions, and mandated grievance-redress mechanisms), significant gaps remain: unclear liability in third-party frauds, slow resolution of disputes, low consumer awareness of rights and inconsistent practices among banks and payment-aggregators. The paper finds with recommendations for legal amendments and regulatory upgrades including clearer

[1] (LL.M) from Prestige Institute of Management and Research Department of Law, Indore (MP).
[2] study on consumer safety in India's digital-payment ecosystem

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

https://www.ijalr.in/

liability norms, faster complaint-processes, stronger enforcement and better consumer education to strengthen consumer protection in India's evolving digital-finance era.

Introduction

Over the last few years, India has witnessed a dramatic transformation in the way financial transactions are conducted. The advent of digital banking, the widespread adoption of real-time payment systems such as the Unified Payments Interface (UPI), mobile wallets and other online payment services have ushered in an era of convenience, speed and greater financial inclusion. For instance, in 2024 alone India recorded roughly 208.5 billion digital payment transactions, with UPI accounting for about 83 % of that volume. UPI transaction volumes have surged such as processing over 172 billion transactions in 2024, reflecting around 46 % growth over the previous year. This scale of adoption underscores the rapid digitalisation of the payment's ecosystem in India and the central role that banking and digital-payment services now play in everyday life.

At the same time, with this rapid growth, significant risks come for the consumers who use banking and digital payment services. Cases of unauthorised transactions, fraud, service lapses, delays in grievance-redressal, and issues such as cheque-dishonour continue to surface. For example, reports show a 72-year-old resident in Pune lost around ₹3.4 lakh to a "KYC update" fraud involving remote access and unauthorised UPI transactions. These developments raise concerns about whether the legal and regulatory framework is sufficiently robust to protect consumers' rights in this new environment.

Within this context, this research paper undertakes a critical evaluation of the legal and regulatory mechanisms that are in place in India to protect consumers in the realms of banking, digital payments and related services. It focuses on key statutes like the Consumer Protection Act, 2019 and the Negotiable Instruments Act, 1881, as well as relevant guidelines issued by the Reserve Bank of India (RBI) and the Insurance Regulatory and Development Authority of India (IRDA). The assessment employs a doctrinal research method supplemented by case studies and

Growing risks in digital banking,Legal gaps in digital payments

empirical data to classify the common problems faced by consumers, assess how well regulatory bodies respond to them, and analyse the magnitude of consumer harm.

The significance of this study stems from the fact that as digital transactions become the norm rather than the exception, consumers must be protected not only against traditional banking risks (such as cheque-dishonour or bank service deficiency) but also against novel digital risks (such as app-based fraud, phishing, unauthorised UPI mandates and payment-aggregator failures). The paper contends that while the existing framework does provide useful protectionsuch as limitation of liability in certain unauthorised digital transactions and mandated grievance-redress mechanisms, there remain important gaps: ambiguous liability in third-party digital fraud, slow dispute resolution processes, low consumer awareness of rights, and inconsistent practices among banks and other payment service providers.

Legal / Regulatory Framework

Consumer Protection Act, 2019 (CPA, 2019)

- The Act was enacted to replace the earlier Consumer Protection Act, 1986, and came into force across India (with varying commencement dates) to provide better protection of consumer interests. https://ncdrc.nic.in/bare_acts/CPA2019.pdf
- Under the CPA, "consumer" includes a person who buys any goods or hires or avails any service for consideration **including through electronic means or by online transaction**. https://consumeraffairs.gov.in/pages/consumer-protection-acts
- Banking services and digital payment services fall within the definition of "service" under the Act, thereby enabling consumers to approach consumer forums for deficiency of service, unfair trade practice, etc.
- Features of the Act that assist consumer protection in the digital age include establishment of the Central Consumer Protection Authority (CCPA) to regulate and enforce consumer rights, inclusion of e-commerce transactions, class-action suits, mediation, product/service liability, and faster dispute mechanisms. https://doca.gov.in

- Therefore, under CPA, consumers using digital banking/payment platforms have a statutory route for redress this forms a key part of the framework we are assessing.

Reserve Bank of India (RBI) Guidelines & Regulatory Measures

- Beyond general consumer law, the RBI issues a range of guidelines, master directions and circulars that specifically govern digital payments, banking services, payment aggregators, security controls, etc. For example, the Master Direction on Cyber Resilience & Digital Payment Security Controls for non-bank PSOs (issued 30 July 2024) addresses security, data integrity and fraud risk. KPMG Assets
- Key mandates include two-factor authentication for digital payment transactions, secure APIs and data confidentiality, risk monitoring by banks and payment system operators, obligations for payment aggregators/gateways to follow RBI/DPSS directions. https://www.corbado.com/blog/reserve-bank-india-compliance
- RBI also **released a Customer Charter of Right** for bank customers, outlining broad rights such as fair treatment, transparency, suitability, privacy, grievance redress & compensation. https://www.rbi.org.in/commonman/english/scripts/PressReleases.aspx
- Recent draft Digital Banking guidelines direct that banks must not force customers into digital channels (i.e., no mandatory bundling) and must provide choice, simplified terms, local language disclosures.https://bfsi.economictimes.indiatimes.com/articles/rbi-to-banks-ask-first-dont-push-digital-services-on-customers/122818191
- For payment aggregators and gateways, the RBI's guidelines (e.g., on PA/PG regulation) impose obligations for safety, transparency and consumer protection.

4.3 Negotiable Instruments Act, 1881

- Although primarily concerned with negotiable instruments like cheques and promissory notes, the NI Act has relevance in the banking services part of our scope, especially for cheque dishonour cases, s. 138 (penalty for dishonour of cheque) etc.

- Consumers of banking services may face issues when cheques are dishonoured, leading to liability, charges and service deficiency claims. The NI Act helps provide the legal mechanism for such redress under banking/cheque context.
- The interface of traditional banking services (cheques, bank accounts) with digital banking means that this statute still holds relevance in the regulatory framework for consumer protection.

4.4 Role of Insurance Regulatory & Development Authority (IRDA) & Other Regulatory Bodies

While the focus is banking & digital payments, the involvement of insurance services (digital insurance, bancassurance, app-based insurance products) means that the Insurance Regulatory and Development Authority of India (IRDAI) also plays a role in consumer protection in financial services.IRDAI issues guidelines for digital/online insurance services, ensuring disclosure of terms, grievance redressal and customer rights.Coupled with financial sector consumer protection, these bodies collectively form a regulatory ecosystem that seeks to safeguard consumers in banking, digital payment and financial services.

5 Classification of Issues / Problems

Consumers of banking and digital payment services in India face a variety of problems. In this part of the discussion classifies the principal issues under broad headings, each of which will then be examined in later sections.

5.1 Unauthorized Transactions & Digital Payment Frauds

A major category of consumer problems relates to unauthorized transactions, digital payment frauds and misuse of banking/digital payment channels. For example:

1. Data from the Reserve Bank of India (RBI) show that in FY 2023 nearly 6,659 fraud cases (about 49% of all frauds) were in the digital payment — card/internet category. https://indianexpress.com/article/business/banking-and-finance/digital-payment-frauds-in-fy23-rbi-report-8637607/

2. Between April–January 2024-25, about 2.4 million incidents of digital financial fraud were reported, amounting to ≈ ₹4,245 crore. https://www.business-standard.com/finance/news/digital-financial-frauds-touch-rs-4-245-crore-in-the-apr-jan-period-of-fy25-125032001214_1.html
3. These frauds often involve phishing, OTP interception, account takeover, malicious apps, manipulated QR codes, etc. https://www.policycircle.org/policy/why-are-digital-frauds-rising/

These issues raise questions of consumer liability, bank/payment-service provider responsibility, speed and success of refunds, and clarity of the rules for remediating frauds.

5.2 Service Deficiencies / System Failures / Delays in Grievance Redress

Another set of problems are deficiencies in service or system failures in the banking/digital-payment ecosystem. Examples include:

1. Delays in refunding unauthorized transactions, or banks/payment aggregators placing the burden of proof on the customer.
2. Payment aggregator / merchant failures (e.g., a QR payment accepted but funds not credited, or the aggregator disabling the merchant's account without sufficient process).
3. Issues in grievance-redress: consumers may not get timely acknowledgement, tracking, visible process, or compensation.
4. Traditional banking services like cheques and negotiable instruments still face issues of dishonour or delay, causing consumer harm.

5.3 Cheque Dishonour& Issues under the Negotiable Instruments Act

While digital payments dominate current trends, many consumers still deal with traditional instruments such as cheques. Issues here include:

- Dishonour of cheques (for insufficiency of funds, account closure, etc.) leads to liability for payee or drawer under the Negotiable Instruments Act, 1881 (NI Act).

- Consumers may be unaware of their rights when a bank dishonours a cheque or fails to communicate.
- The interface between digital banking (account closures, online-only banking) and cheque usage can cause additional friction.

5.4 Ambiguity of Liability, Third-Party Frauds & Payment Aggregator Risks

A further category involves more complex issues where liability is unclear or where multiple parties are involved (bank + payment service provider + merchant + aggregator). These include:

- Frauds where the customer's credentials are compromised via an external app or aggregator, raising issues of how far the bank or payment service provider is responsible.
- Situations involving **mule accounts** or laundering of funds through multiple accounts, which complicate tracking and consumer redress.
- Payment aggregators / gateways sometimes operate with less direct consumer-facing regulation, leading to inconsistent practices.
- **Third-party merchant risks:** consumers pay via a merchant QR or aggregator, but dispute resolution may become complex when service lapses involve the merchant rather than the bank.

5.5 Consumer Awareness, Digital Literacy & Accessibility Issues

Finally, many of the problems stem not only from system faults, but from consumer-side issues:

- Lack of awareness among consumers about their rights under law, limitations of liability, complaint-process steps.
- Digital literacy gaps especially among elderly or rural users who may not recognize phishing or bogus apps.

- Accessibility issues: terms and conditions may be in English, notifications may not be clear, banking apps may have complex user-interfaces, and consumers may find complaint-tracking difficult.

6 Case Law & Precedents

In this part of the discussion reviews landmark and illustrative judicial decisions that shed light on how Indian courts have treated consumer protection issues in banking and digital payment services. These cases help demonstrate both the strengths and weaknesses of the legal/regulatory framework.

6.1 KC Varghese v. SBI Cards & Payment Services Ltd. (DCDRC, Dec 18 2023)

In this case, the complainant, K.C. Varghese, brought a complaint under the Consumer Protection Act, 2019 alleging unauthorised transactions of ₹49,000 using his credit-card issued by SBI Cards & Payment Services Ltd. (SBI Cards). https://www.casemine.com/judgement/in/667151fb61b4c06996440eb4

Key points:

- The complainant alleged that his card credentials, CVV and OTP were compromised even though he had not authorised the transactions.
- SBI Cards contended that the complainant was negligent in sharing credentials and the bank's systems were secure.
- The forum framed the issues: (i) whether there was a deficiency in service by the bank, and (ii) if so, what reliefs should follow.
  This situation illustrates how consumer courts are willing to engage with digital banking frauds under the Consumer Protection Act, but also highlight that liability often hinges on proving bank negligence vs customer negligence.

6.2 State Bank of India v. Madan Lal Gupta (DCDRC, Dec 05 2024)

In this case, the complainant found that an amount of ₹49,367.50 was debited from his account without his authorization. The bank responded that the complainant had willingly

shared credentials and used a third-party app. https://www.consumercourt.in/judgment/state-bank-of-india_vs_madan-lal-gupta

The consumer forum dealt with whether the bank had a service-deficiency, or whether the complainant's own actions (clicking unknown link, sharing OTP) precluded bank liability. This ruling highlights a recurring theme: courts often examine customer conduct closely (downloading unknown apps, sharing credentials) before holding the bank liable. The case underscores the interplay of user negligence and bank responsibility.

6.3 State Bank of India v. M.S. Bakankar (Aug 04 2023)

Here, bank was found to be deficient in service because it failed to send mandatory SMS alerts for card transactions, a requirement under the Reserve Bank of India (RBI) guidelines. The bank paid ₹1,00,000 compensation. https://www.consumercourt.in/judgment/state-bank-of-india_vs_m.s.-bakankar

This situation is significant because it emphasizes the bank's duty to comply with regulatory instructions e.g., SMS alerts and shows that failure triggers liability even where the customer may also have some role. It demonstrates that regulatory adherence is key in dispute resolution.

6.4 Suresh Chandra Singh Negi & Another v. Bank of Baroda & Others (Allahabad High Court, July 17, 2025)

The court dealt with unauthorized electronic transactions of approximately ₹38.78 lakh in accounts of accountholders, and the petitioners sought refund claiming cyber fraud. https://www.mondaq.com/india/financial-services/1688906/allahabad-high-court-clarifies-bank-liability-in-cases-of-alleged-unauthorized-electronic-transactions-a-case-defining-customer-responsibility

Key takeaways:

- The High Court held there was no unauthorized transaction since the evidence showed use of credentials/OTP by the accountholder or with their knowledge; thus, the bank was not liable.
- The judgement emphasized that the RBI circular on "Limiting Liability of Customers in Unauthorized Electronic Banking Transactions" is designed to protect genuine victims but cannot be abused to cover negligence.
  This situation is important for showing the boundary of customer protection: when the customer's own action (or negligence) is involved, courts may relieve banks of liability.

6.5 Summary of Patterns from Case Law

From these decisions, several patterns emerge:

1. Courts consistently treat the bank's failure to follow regulatory guidelines (e.g., sending alerts, secure systems) as **deficiency in service**.
2. The customer's role (sharing credentials, installing unknown apps, failing to notify bank immediately) is heavily scrutinized; contributory negligence often reduces or eliminates liability of service provider.
3. Refunds and compensation are ordered when banks/payment service providers fail to meet regulatory/contractual obligations, especially with minimal or no customer fault.
4. Cases involving digital payment fraud add new complexity: multiple parties (bank, payment aggregator, merchant, third-party app) may be involved; proof of who caused the loss becomes critical.
5. The jurisprudence still lacks consistency in deciding what "reasonable steps" banks/PSPs must take based on evolving digital risks.

7 Role of Regulatory Bodies

Court interpretations of consumer rights

7.1 Reserve Bank of India (RBI)

- The RBI is the key regulator for banking and digital payment systems in India. Its role in consumer protection includes:
- Issuing guidelines and circulars to banks and non-bank payment service providers (PSPs) on digital banking, UPI, fraud control, customer liability, and grievance-redress mechanisms.
- Releasing a "Customer Charter of Rights" for bank customers, covering areas like transparency, privacy, grievance redressal and fair treatment.
- Monitoring the payments ecosystem (including payment aggregators, mobile wallets, UPI) via its Department of Payment & Settlement Systems (DPSS) and Cyber Security & IT operations.
- Imposing obligations on banks/PSPs to adopt two-factor authentication, secure APIs, fraud reporting and early blocking of suspicious transactions.
- Investigating large scale digital frauds, issuing data on digital payment fraud incidence, and directing banks to compensate/resolve cases in prescribed timeframes.

7.2 Insurance Regulatory and Development Authority of India (IRDAI)

While the primary focus is banking and digital payments, IRDAI plays a role in digital insurance and bancassurance services. In the context of consumer protection:

- IRDAI issues regulations for online insurance platforms, disclosure norms, grievance redressal, and mobile-/app-based insurance services.
- It ensures that insurers/insurance intermediaries offer adequate consumer disclosures, simplify contracting online, and provide accessible complaint mechanisms.
- In the broader financial-services consumer protection ecosystem, IRDAI complements RBI by regulating those digital finance products that cross into insurance territory (for example, insurance top-ups via mobile wallets, digital insurance apps).

The inclusion of IRDAI in the regulatory architecture ensures that "digital financial services" are not limited to banking but cover adjacent areas.

7.3 Consumer Protection Mechanisms & Other Bodies

- The Central Consumer Protection Authority (CCPA) under the Consumer Protection Act, 2019 also holds a role: investigating unfair trade practices, deficiency of service, mis-selling in digital financial services, and class-action suits.
- The Banking Ombudsman scheme (by RBI) provides a lower-cost recourse for grievances against banks/PSPs.
- Consumer courts/disputes redressal commissions at state/district levels adjudicate deficiency of service claims under CPA.
- Cyber-crime cells, law-enforcement agencies and Payment System Operators (like the National Payments Corporation of India-NPCI) also play supporting roles in fraud detection and response.

7.4 Higher Court Ruling & Its Implications

One important higher court decision is from the Allahabad High Court in *Suresh Chandra Singh Negi & Anr. v. Bank of Baroda & Ors.* (July 2025). The court held that the bank bears **the burden of proving** the customer's liability in cases of unauthorised electronic banking transactions pursuant to the RBI's 2017 Circular. Significantly, the court emphasised that the RBI Circular is meant to shield genuine victims of cyber fraud and not to provide a blanket escape to customers who may have been negligent. Although not a Supreme Court ruling, this precedent is highly relevant because it clarifies the interaction between regulatory policies (RBI's circulars), bank obligations and consumer rights in digital banking.https://www.verdictum.in/court-updates/high-courts/allahabad-high-court/suresh-chandra-singh-negi-v-bank-of-baroda-2025ahc115460-db-1585294

7.5 Assessment of Regulatory Effectiveness

In assessing how well these bodies perform, the following observations emerge:

- **Strengths**: The RBI and IRDAI have proactively issued guidelines recognizing digital-age risks (UPI frauds, Payment Aggregators, two-factor authentication). The CPA (2019) and CCPA provide a statutory overlay for consumer rights. The existence of Banking Ombudsman and consumer fora provide multiple redress routes.
- **Weaknesses / Gaps**:
  - Enforcement: While guidelines exist, consistent enforcement (across banks, PSOs, aggregators) appears patchy.
  - Clarity of Liability: Regulatory documents sometimes leave ambiguity around third-party/aggregator liability, which courts highlight.
  - Speed of Redress: Consumers still face delays in complaint resolution, which undermines protection.
  - Consumer Awareness: Regulatory bodies issue documents but consumer awareness remains low; many losses are attributed to user-negligence rather than system failure.
  - Oversight of non-bank PSPs/Aggregators: While payments have digitised rapidly, regulatory oversight of newer intermediaries (aggregators, fintech apps) is still developing.

7.6 The Way Forward for Regulators

Based on the above, it is the following:

A review of regulatory authorities overseeing India's digital-financial ecosystem
Key weaknesses in oversight

- RBI/IRDAI should issue clearer, binding rules (not just guidelines) on liability, timeframe for refunds, reporting obligations for banks/PSPs and inaugurate strong audit/penalty mechanism.
- CCPA and consumer fora must be empowered to handle class-action suits against banks/PSPs for widespread digital-fraud.
- Regulators should push for regular consumer-education campaigns, especially for digital payment literacy (UPI safety, OTP sharing risks).
- Coordination between regulators (RBI, IRDAI, CCPA), law-enforcement, and payment infrastructure bodies (NPCI) needs strengthening to address cross-platform frauds and aggregator liability.
- Real-time monitoring of digital payment channels and mandatory incident-reporting by banks/PSPs to RBI for systemic tracking of fraud patterns.

8 Statistical / Empirical Evidence

In this part of the discussion presents recent data and trends that help quantify the scale of digital-banking and payment-service use in India, and the associated consumer-risk issues. It provides empirical grounding for the legal/regulatory assessment in later sections.

8.1 Growth of Digital Payments

- According to the Reserve Bank of India (RBI), digital payment transactions in India reached **18,120.82 crore** in volume (and value of ₹2,330.72 lakh crore) up to January 2025. https://www.pib.gov.in/indexd.aspx
- The RBI's Digital Payments Index (DPI) registered a year-on-year growth of 10.7 % as of March 2025, rising to 493.22 from 445.5 a year earlier.https://ai.economictimes.com/news/economy/finance/digital-payments-rise-10-7-pc-at-end-march-2025-rbi-data/articleshow/122956186.cms
- The share of the digital payments (card/internet channels) among all banking fraud cases remained high: in FY25, the card/internet category accounted for 56.5 % of fraud

incidents in banks. https://government.economictimes.indiatimes.com/news/rbi-reports-over-50-drop-in-digital-banking-frauds-in-fy25/121791537

8.2 Fraud Incidence & Value

- In FY25, banks reported **13,516 fraud cases** in the "card/internet" category amounting to around **₹520 crore**.
- For FY24, the number of such frauds was 29,082 with value ~₹1,457 crore — showing a drop in number and value in FY25.
- The total number of digital payment-fraud incidents (across categories) over the past decade was reported at 63,315 cases involving losses of ~₹733.26 crore for amounts ≥ ₹1 lakh. https://government.economictimes.indiatimes.com/news/rbi-reports-over-50-drop-in-digital-banking-frauds-in-fy25/121791537

8.3 Risk Exposure, Awareness and Consumer Behaviour

- A survey ("The State of Digital Payments in India", Aug 2024) found that both consumers and merchants perceive **online financial fraud** as a major challenge in the digital payments ecosystem. chase-advisors.com
- Fraud types data: According to a report, phishing caused about **38 %** of fintech frauds in India in 2025. jisasoftech.com

8.4 Interpretation & Trends

The growth in transaction volume shows deep penetration of digital payments: interacting with this trend, consumer protection must scale in parallel. The reduction in number and value of card/internet frauds in FY25 compared to FY24 suggests some positive impact of regulatory/technological measures (e.g., stronger authentication) but the still large numbers underscore persistent risk. The high share of frauds in digital channels (56.5 % in FY25) shows that as usage grows, the risk-surface grows too — especially in newer forms of payments (UPI/wallets) that may challenge legacy redress mechanisms.The gap between reported frauds and actual consumer losses may be significant: many incidents

go unreported or are resolved outside formal systems, thereby underestimating true scale. The data on consumer/merchant perception of fraud suggest that issues of awareness, digit-literate behaviour, informed consent are meaningful parts of the problem—not just technological vulnerability.

8.5 Relevance to This Study

- These statistics help frame the urgency and magnitude of the issue: consumer protection in digital banking/payments isn't a hypothetical concern but involves real volume and value of transactions and fraud loss.
- Empirical evidence supports the need for examining how well laws/regulations respond to these risks: e.g., if frauds form ~56% of incidents, yet resolution/compensation remain slow, then there is a gap.
- The data permit analysis of how regulatory bodies (banks, RBI, payment service providers) perform vis-à-vis actual outcomes (fraud counts, losses, redress).
- By comparing trends (growth of digital payments vs fraud incidence) we can assess whether protections are keeping pace with adoption.

Fiscal Year	Metric	Value	Source
FY 2024-25	Total digital payment transactions in India	~ 221.9 billion	https://www.financialexpress.com/business/banking-finance-upi-share-in-digital-payments-rises-to-83-7-in-fy25-3861812
FY 2024-25	Share of Unified Payments	~ 83.4-83.7%	https://www.business-standard.com/finance/news/upi-s-contribution-to-payments-ecosystem-

Statistical indicators highlighting the scale and risks within India's digital-payment ecosystem.

Fiscal Year	Metric	Value	Source
	Interface (UPI) in total transaction volume		volume-grows-to-83-4-in-fy25-125052900871_1.html
FY 2024-25	Value of UPI transactions	~ ₹ 261 lakh crore	https://www.financialexpress.com/business/banking-finance-upi-share-in-digital-payments-rises-to-83-7-in-fy25-3861812/
FY 2023-24	Fraud cases (card/internet category)	29,082 cases	https://www.ndtvprofit.com/business/card-internet-transactions-accounted-for-806-frauds-in-fiscal-2024-fy24-rbi-annual-report
FY 2023-24	Value of card/internet frauds	≈ ₹ 1,457 crore	https://www.ndtvprofit.com/business/card-internet-transactions-accounted-for-806-frauds-in-fiscal-2024-fy24-rbi-annual-report
FY 2024-25	Number of fraud cases (card/internet)	~ 13,516 cases	https://government.economictimes.indiatimes.com/news/digital-payments/upi-dominates-digital-payments-in-india-with-837-market-share-in-fy25/121528453
FY 2024-25	Digital Payments Index	493.22 (10.7%	https://economictimes.indiatimes.com/news/economy/finance/digital-payments-rise-10-7-pc-at-end-march-2025-rbi-

Fiscal Year	Metric	Value	Source
	(March 2025)	YoY rise)	data/articleshow/122956186.cms

9 Assessment: How Well Are Consumers Protected?

In this part of the discussion critically evaluates the effectiveness of the legal, regulatory and practical safeguards for consumers in banking and digital payments in India , identifying both strengths and significant gaps.

9.1 Strengths of the Current Framework

- The enactment of the Consumer Protection Act, 2019 has broadened the scope of consumer protection to include services "availed through electronic means or by online transaction". This enables customers using digital banking/payment services to seek redress under consumer law.
- The Reserve Bank of India (RBI) has issued specific guidelines and directions for banks and payment service providers (PSPs) covering digital security, customer grievance-redressal, customer liability in unauthorized transactions, etc.
- Judicial precedents show that consumer forums and courts are willing to find banks/PSPs liable for "deficiency of service" when regulatory obligations are not met (for example, failure to send transaction alerts, or poor system controls).
- Empirical data reflects the scale of digital payments and suggests that regulatory awareness is increasing for example, fraud incidence data and reporting are becoming visible, which supports transparency and accountability.

9.2 Gaps and Weaknesses

- **Ambiguity of liability**, especially in complex digital frauds involving third parties (aggregators, merchants, payment gateways) or where the customer's negligence is alleged: Courts often scrutinize user behavior intensely, which may place a higher burden on the consumer.
- **Slow resolution of disputes**: Even when protections exist in law or regulation, consumer redress mechanisms (ombudsman, consumer courts) may be slow, and consumers may face delays or uncertainties.
- **Enforcement challenges**: Regulatory guidelines exist but consistent enforcement across banks, PSPs, fintech's remains uneven; non-bank payment service intermediaries may operate in regulatory grey zones.
- **Infrastructure and system risk**: Some banks still rely on legacy systems or inadequate technology platforms, which may undermine consumer safeguards (e.g., system outages, capacity issues). https://cio.economictimes.indiatimes.com/news/strategy-and-management/consumer-centric-evolution-banks-must-modernize-upi-switches-before-its-too-late/114226298
- **Digital literacy, awareness and inclusion issues**: A significant number of consumers (especially in rural/semi-urban areas) may not be aware of their rights, safe digital-practices or complaint pathways. Low digital/financial literacy increases vulnerability. https://www.merchantpaymentsalliance.in/wp-content/uploads/2025/02/Digital_Digitalisation-and-Financial-Inclusion-for-the-Next-100-Million_compressed.pdf
- **Statutory/regulatory gaps**: While there are statutes and guidelines, the regime lacks a dedicated banking/digital payment consumer-protection statute; cybersecurity, data-privacy and cross-border transaction issues still lack fully matured legal architecture. https://lawfullegal.in/digital-banking-and-cybersecurity-laws-in-india-emerging-legal-challenges/

9.3 Overall Evaluation

On balance, the consumer-protection regime in India for banking and digital payments has made **meaningful progress** there is a robust overlay of consumer-law (CPA), regulatory supervision (RBI, IRDAI), and active case-law. It offers consumers a **greater degree of protection** than was available a decade ago.

At the same time, the pace of digital transformation of banking and payments has arguably outstripped the evolution of enforcement, infrastructure, consumer awareness and tailored regulation. Therefore, the protections are uneven in practice while many consumers may be well-protected, a sizeable portion remains at risk due to system, infrastructure, literacy or regulatory-enforcement gaps.

9.4 Key Areas for Improvement[8]

- The regulatory regime needs **clearer liability rules**, especially for newer players (aggregators, fintech's) and for third-party frauds.
- Mechanisms for **faster resolution** of consumer complaints, including digital-first redress pathways (online tracking, time-limits) should be strengthened.
- Enforcement agencies (RBI/IRDAI/CCPA) should ensure **uniform compliance** across banks and PSPs, including non-bank intermediaries.
- Consumer literacy programmed must be scaled – particularly in rural and semi-urban regions – to raise awareness of rights, safe practices and complaint processes.
- Technology/infrastructure upgrades are needed (banks upgrading UPI-switches, legacy systems) so that service reliability and security keep pace with transaction growth.
- Legal / statutory gaps (cybersecurity in banking, data-protection for financial transactions, cross-border digital fraud) should be addressed via amendments or new laws.

10 Recommendations / Reforms

[8] Evaluating consumer protection effectiveness

Based on the assessment of the legal, regulatory and practical environment for consumer protection in banking and digital payments, the following reform recommendations are put forward:

10.1 Clearer & Stronger Liability Norms

- Amend relevant statutes (such as the Consumer Protection Act, 2019 and the Negotiable Instruments Act, 1881) or introduce a dedicated consumer-protection statute for digital financial services to clearly allocate liability among banks, payment service providers (PSPs), payment aggregators and merchants.
- Regulatory guidelines by the Reserve Bank of India (RBI) should be turned into binding rules (rather than only guidelines) with specific timeframes for liability and clear conditions for "unauthorized transactions" refunds.
- Define in regulation the minimum standard of "due diligence" by banks/PSPs (e.g., two-factor authentication, beneficiary verification, anomaly detection) that must be met to shift liability away from consumer.

10.2 Faster & More Accessible Redress Mechanisms

- Mandate that banks/PSPs complete investigation and communicate outcome of unauthorized transaction complaints within a specified short timeframe (e.g., 10–14 working days), failing which automatic provisional refund should be credited to consumer pending final resolution.
- Strengthening online portals (such as e-filing of consumer complaints) and promote digital dispute resolution mechanisms—allow mediation, e-conciliation, online hearings so that geographic/physical barriers do not delay resolution.
- Expand the jurisdiction and capacity of consumer fora and ombudsman schemes to deal with "digital payment" specific complaints and ensure that remedies (refunds, compensation) are actually awarded and executed promptly.

10.3 Enhanced Enforcement & Oversight of Payment Ecosystem

- RBI (and where applicable, the Insurance Regulatory and Development Authority of India (IRDAI)) should set up a **Digital Payments Intelligence Platform** (as has been proposed) to monitor fraud trends, aggregator behavior, complaint patterns, and trigger early warnings. https://economictimes.indiatimes.com/industry/banking/finance/banking/rbis-proposed-digital-payments-intelligence-platform-will-mitigate-frauds-say-experts/articleshow/110801767.cms
- Introduce mandatory reporting obligations for banks/PSPs/aggregators: number of frauds, average refund time, unresolved complaint volume should be published annually for transparency and benchmarking.
- Regulators should carry out periodic audits of payment aggregator / PSP systems, and impose penalties for non-compliance (e.g., failure to send alerts, weak authentication, inadequate grievance-redress infrastructure).

10.4 Strengthening Consumer Awareness & Digital Literacy

- Launch national campaigns (in multiple languages) to educate consumers about safe digital-payment practices (e.g., not sharing OTP, verifying beneficiary name, suspicious links), their rights under the law, and how to report complaints.
- Integrate digital-financial literacy modules into school and college curricula, especially covering UPI, mobile wallets, bank apps, basic "**what to do if you suffer a fraud**".
- Focus special efforts on vulnerable segments—elderly, rural/semi-urban users, women—both in awareness and in ensuring accessibility (including non-smartphone options). For example, only ~38 % of rural/semi-urban users currently prefer UPI. https://www.ey.com/en_in/newsroom/2024/12/upi-most-preferred-payment-mode-for-38-percent-indians-in-rural-and-semi-urban-areas-96-percent-demonstrate-strong-inclination-to-save-and-invest-ey-and-cii-report

Proposed reforms targeting liability, enforcement, and grievance mechanisms

10.5 Technological & Infrastructure Enhancements

- Banks and PSPs must upgrade legacy systems and adopt advanced authentication, device-fingerprinting, fraud-analytics and biometric or token-based verification so that system vulnerabilities do not become consumer risk points.
- Promote interoperability and low-cost acceptance infrastructure (especially in rural/semi-urban areas) so that consumers are not forced into unsafe alternatives for convenience. https://community.nasscom.in/communities/policy-advocacy/policy-brief-highlights-of-the-high-level-committee-report-on-deepening-digital-payments.html
- Regulators should encourage innovation via "regulatory sandbox" for fintech/PSPs but ensure that sandboxed entities have consumer-protection safeguards before scaling.

10.6Legal / Regulatory Gaps & Amendments

- Amend the Payment & Settlement Systems regime (e.g., the Payment and Settlement Systems Act, 2007) to explicitly include **consumer protection** and **penalty provisions** for digital-payment service failures. https://taxguru.in/rbi/report-of-the-committee-on-digital-payments.html
- Developing a unified legal framework for data privacy and digital-payment services: though the Digital Personal Data Protection Act, 2023 exists, clearer application to digital-payment ecosystem (aggregators, wallets, merchant apps) is required.
- Introduce mandatory minimum standards for Payment Aggregators / Gateways (net-worth, escrow accounts, merchant background checks) to protect end-consumers especially where PSUs and non-banks operate.
- Encourage cross-border cooperation and standard-setting for international digital-transaction fraud, since digital payments are increasingly globalized.

10.7 Summary of Reform Approach

To sum up, to safeguard consumers in India's rapidly evolving digital finance era, the focus must shift from mere rules to effective execution, from volume growth to consumer-trust growth, and from technology roll-out to inclusion + literacy + redress. The reforms recommended here aim to create a functioning ecosystem where consumers are not just covered by law on paper but visibly protected in practice.

Final Thoughts

The shift toward digital systems of banking and payment systems in India has fundamentally reshaped how financial transactions are conducted. Services such as real-time transfers through the Unified Payments Interface (UPI), mobile wallets and internet banking have brought unprecedented convenience, speed and accessibility. At the same time, this transformation has also introduced new risks for consumers—ranging from unauthorized transactions and frauds to service lapses and ambiguities around liability. This paper has examined whether the existing legal and regulatory architecture—primarily the Consumer Protection Act, 2019, the Negotiable Instruments Act, 1881, and key guidelines issued by the Reserve Bank of India (RBI) and the Insurance Regulatory and Development Authority of India (IRDAI)—adequately safeguards consumers in this digital-finance environment.

The review suggests that while significant progress has been made, the protections currently in place do not fully match the scale and complexity of the risks. On the one hand, consumers benefit from statutory coverage under consumer law, regulatory obligations imposed on banks and payment service providers, and evolving jurisprudence that recognises "deficiency of service" in digital contexts. On the other hand, persistent gaps such as unclear apportionment of liability in third-party frauds, delays in complaint resolution, uneven enforcement across intermediaries, and relatively low levels of consumer awareness limit the efficacy of the regime. Moreover, empirical data shows that the pace of digital-payment adoption is rapid, yet the corresponding safeguards and infrastructure upgrades often lag.

Summarizing the path forward for effective consumer protection in India's digital economy.

Considering these developments, a recalibrated approach is necessary—one that not only focuses on adopting new laws and guidelines but also on effective execution, transparent liability rules, consumer education, technological resilience and inclusive redress mechanisms. Only by aligning the pace of regulatory adaptation with technological innovation and user behavior can the digital finance ecosystem truly deliver the twin goals of convenience and consumer trust.

As India's payments landscape continues to evolve and expand—penetrating rural areas, integrating fintech and bridging financial-inclusion gaps—it is imperative that consumer protection remains a central pillar of policy design and corporate practice. For if consumers feel confident and well-protected, the digital-finance revolution will not only deepen inclusion but also sustain long-term stability and growth. The findings and recommendations of this paper aim to contribute to that journey—towards a system in which every user of banking and digital-payment services can transact with safety, transparency and dignity.

Statutes & Regulations

1. The Consumer Protection Act, 2019 (Act 35 of 2019) (India).
2. The Negotiable Instruments Act, 1881 (Act 26 of 1881) (India).
3. Payment and Settlement Systems Act, 2007 (Act 51 of 2007) (India).
4. "Customer Protection – Limiting Liability of Customers in Unauthorized Electronic Banking Transactions," Circular No. RBI/2017-18/15 DBR.No.Leg.BC.78/09.07.005/2017-18 dated 6 July 2017 (Reserve Bank of India).
5. Reserve Bank of India, *Master Direction on Cyber Resilience & Digital Payment Security Controls for non-bank Payment System Operators*, 30 July 2024 (India).

Key Case-Law

1. Suresh Chandra Singh & Anr. v. Bank of Baroda & Ors., Writ C. No. 24192 of 2022, High Court of Judicature at Allahabad, decided 17 July 2025.
2. State Bank of India v. M.S. Bakankar, Consumer Forum Order dated 4 August 2023.

3. State Bank of India v. Madan Lal Gupta, Consumer Forum Order dated 5 December 2024.
4. IDBI Bank Ltd v. Sarabjeet Singh, Consumer Court Order dated 28 February 2022.
5. (Additional illustrative judgments cited in paper: please ensure full party names, court, date, citation number where available.)

Secondary Sources & Reports

1. Allirajan Muthusamy, "Credit-Card Fraud: How to Protect Yourself by Reporting Unauthorised Transactions" *Mint* (15 Jan 2025) (India) — discussing liability timelines and customer protections.
2. "Limiting Liability of Customers in Unauthorised Electronic Banking Transactions" (Indian Overseas Bank policy document) (accessed via IOB website) — overview of bank/PSP policy in line with RBI circular.
3. "Banks – Refund Unauthorised Transactions: Is Bank Liable for Third-Party Fraud?" *IndiaLaw* Blog (2024) — analyzing bank vs. customer liability in Indian context.