CREDIT CARDS AND ELECTRONIC PAYMENT SYSTEMS IN INDIA: A CRITICAL LEGAL, REGULATORY AND CONSUMER PROTECTION ANALYSIS

Aarushi Rajpurohit, NIMS School of Law, NIMS University, Jaipur

ABSTRACT

The migration of India's payments architecture from cash and cheque-based settlement to card-based and application-driven electronic transfer is among the more consequential legal developments of the last two decades, yet the statutory response to it remains scattered across instruments that were not written with this migration in mind. This article undertakes a comprehensive doctrinal examination of the legal, regulatory and consumer-protection dimensions of credit card and electronic payment systems in India. It situates credit card transactions within contract law, tracing the tripartite (and increasingly multi-party) relationship among issuing banks, acquiring banks, payment networks, merchants and cardholders, and shows how doctrines of unconscionability, fiduciary duty and standard-form contracting continue to structure liability even as the mode of transacting has changed beyond recognition. It then maps the layered regulatory architecture built around the Payment and Settlement Systems Act, 2007, the Information Technology Act, 2000, and the extensive circular-based rule-making of the Reserve Bank of India, arguing that this architecture, while functionally adequate for day-to-day supervision, lacks the codified clarity that a mature payments economy requires. The article devotes particular attention to consumer protection, examining the zero- and limited-liability framework for unauthorised transactions, the expanding judicial reading of "service" under the Consumer Protection Act, 2019, and the practical shortcomings of grievance redressal in a system where disputes are technologically opaque to the very consumers it protects. A dedicated discussion of data protection, privacy and cybersecurity follows the recognition of informational privacy as a facet of Article 21 in Justice K.S. Puttaswamy v. Union of India, and considers what that recognition demands of a payments ecosystem still without a fully operative, sector-specific data protection regime. A comparative section draws lessons from the codified consumer-finance statutes of the United States and the open-banking, GDPR-integrated model of the United Kingdom, before the article closes with a set of specific, implementable recommendations directed at legislative consolidation, strengthened enforcement, standardised disclosure and cybersecurity

baselining. The central argument is that Indian law has kept pace with the payments revolution operationally but not architecturally, and that the next phase of reform must be aimed at coherence rather than mere expansion.

Keywords: Credit Cards; Electronic Payment Systems; Reserve Bank of India; Consumer Protection Act, 2019; Data Privacy; Cybersecurity; Payment and Settlement Systems Act, 2007; FinTech Regulation.

I. INTRODUCTION

Money has always taken the shape of the technology available to move it, but rarely has that shape changed as quickly as it has over the last fifteen years in India. A generation that once queued at bank counters with cheque books now settles a grocery bill by scanning a code with a mobile phone, and a credit card that used to be a marker of urban affluence is now one instrument among several UPI, wallets, NEFT, RTGS, IMPS, through which value moves in fractions of a second. This is not simply a technological story. Every one of those instruments sits inside a legal relationship: a contract between a cardholder and an issuing bank, a statutory authorisation for a payment system operator, a regulatory direction on authentication, a constitutional guarantee of privacy that attaches to the data the transaction leaves behind. The law has had to keep pace with a payments ecosystem that redesigns itself faster than legislatures ordinarily move, and it has done so largely through the delegated, circular-based rule-making of the Reserve Bank of India (RBI) rather than through comprehensive primary legislation.

This article is concerned with three intertwined questions that arise from that state of affairs. First, what is the legal character of a credit card or electronic payment transaction, and how does the multi-party structure of such transactions cardholder, issuing bank, acquiring bank, merchant, payment network, and increasingly a chain of technology intermediaries sit within the inherited doctrines of Indian contract law? Second, what does the regulatory architecture built around the Payment and Settlement Systems Act, 2007[1] and the Information Technology Act, 2000 actually deliver in terms of certainty, accountability and consumer safety, and where does it fall short of a codified regime? Third, how adequately does Indian law protect the consumer who is, in almost every one of these transactions, the least informed and least powerful party particularly where the harm in question is an unauthorised transaction, a data breach, or a cybersecurity failure that the consumer had no realistic means of preventing?

The significance of these questions is not merely academic. Credit card transactions are, at

[1]The Payment and Settlement Systems Act, 2007, No. 51, Acts of Parliament, 2007 (India).

bottom, an extension of credit governed by principles that long predate the technology: offer, acceptance, consideration, and the general contractual apparatus found in the Indian Contract Act, 1872[2]. But the terms on which that credit is extended are almost invariably drafted unilaterally by the issuing bank and presented to the cardholder on a take-it-or-leave-it basis. Standard form contracting of this kind is not unique to credit cards, but the consequences of an unfavourable term are amplified when the underlying subject matter is a consumer's access to credit and, increasingly, their financial identity. The Supreme Court's recognition in Central Inland Water Transport Corporation v. Brojo Nath Ganguly[3] that unconscionable terms in a standard form contract may be struck down as opposed to public policy remains, decades later, one of the more useful doctrinal tools available to a court examining a credit card agreement, precisely because it does not depend on the existence of a specific consumer-finance statute.

Layered on top of this contractual foundation is a regulatory structure that has grown almost entirely through subordinate legislation. The Payment and Settlement Systems Act, 2007 supplies the statutory basis for the RBI's authority to license and supervise payment systems, but the substantive content of consumer safeguards authentication requirements, tokenisation mandates, the zero- and limited-liability framework for unauthorised transactions is found not in the Act itself but in RBI master directions and circulars. This is administratively efficient: circulars can be updated far more quickly than an Act of Parliament, which matters in a sector where the underlying technology changes annually. It is also, from a rule-of-law perspective, imperfect: a consumer's substantive rights against a bank rest on instruments that are more difficult to locate, interpret and enforce than a codified statute, and that can in principle be varied by the regulator without the deliberative process that attends legislative amendment.

The judiciary has, in the absence of comprehensive legislation, done a considerable amount of the work of adapting general legal principles to the digital context. The evidentiary framework for electronic records, established in Anvar P.V. v. P.K. Basheer[4] and refined in Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal[5], now determines whether a bank's transaction logs or a consumer's screenshot of an SMS alert can even be placed before a court. The extension of "service" under consumer protection law to banking and professional services, achieved in Lucknow Development Authority v. M.K. Gupta[6] and Indian Medical Association

[2]The Indian Contract Act, 1872, No. 9, Acts of Parliament, 1872 (India).
[3]Central Inland Water Transport Corp. Ltd. v. Brojo Nath Ganguly, (1986) 3 SCC 156 (India).
[4]Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473 (India).
[5]Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1 (India).
[6]Lucknow Dev. Auth. v. M.K. Gupta, (1994) 1 SCC 243 (India).

v. V.P. Shantha[7], is what allows a cardholder aggrieved by an unauthorised transaction to approach a consumer forum at all. The recognition of a constitutional right to privacy in Justice K.S. Puttaswamy v. Union of India[8] supplies the doctrinal basis on which any future data protection claim in the payments space will ultimately rest. None of these decisions were written with credit cards or UPI in mind, yet each has become structurally important to how the sector is regulated in practice which is itself a symptom of the absence of a dedicated statutory framework.

This article proceeds in the following manner. Part II briefly situates the study within the existing literature and methodology. Part III examines the legal nature and operational framework of credit card transactions. Part IV traces the evolution of electronic payment systems in India. Part V maps the legal and regulatory framework governing digital payments. Part VI is devoted to consumer protection. Part VII addresses data protection, privacy and cybersecurity. Part VIII offers a comparative analysis of the United States and United Kingdom frameworks and draws lessons for India. Part IX identifies emerging challenges, and Part X sets out specific recommendations before the article concludes in Part XI.

II. LITERATURE REVIEW AND METHODOLOGY

The literature on Indian payments law can be grouped into three broad strands. The first is doctrinal commercial law scholarship represented by texts such as Avtar Singh's 'Law of Contract'[9] which addresses standard form contracting and unequal bargaining power without speaking directly to digital payments but supplies the conceptual vocabulary (unconscionability, adhesion contracts, implied duties of care) that later scholarship and case law apply to credit card agreements. The second is regulatory and institutional literature, principally the RBI's own 'Report on Trend and Progress of Banking in India'[10] and the publications of the National Payments Corporation of India (NPCI)[11], which document the empirical growth of UPI, IMPS, NEFT and RTGS and the operational infrastructure supporting them, but are naturally descriptive rather than critical of the legal framework. The third strand is constitutional and privacy scholarship, anchored by treatments of the Right to Privacy such as M.P. Jain's 'Indian Constitutional Law'[12], which becomes directly relevant to financial data

[7]Indian Med. Ass'n v. V.P. Shantha, (1995) 6 SCC 651 (India).
[8]Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
[9]Avtar Singh, Law of Contract 214-40 (11th ed. 2017).
[10]Reserve Bank of India, Report on Trend and Progress of Banking in India (latest available edition).
[11]National Payments Corporation of India, Official Reports and Publications, https://www.npci.org.in.
[12]M.P. Jain, Indian Constitutional Law 1027-55 (8th ed. 2019).

only after the Puttaswamy decision. International and comparative commentary on FinTech regulation for instance Arner, Barberis and Buckley's work[13] on the relationship between FinTech and RegTech, and IMF working papers on financial services regulation provides a further comparative lens, though this literature is written primarily for a global audience and requires adaptation to the Indian statutory context.

What is comparatively underdeveloped is scholarship that draws these three strands together into a single, integrated account of the legal position of the Indian cardholder or UPI user one that moves from contract, through regulation, to consumer remedy and privacy, in a single analytical frame. This article attempts that synthesis.

Methodologically, the analysis is doctrinal, drawing on primary legal sources the Indian Contract Act, 1872, the Information Technology Act, 2000, the Payment and Settlement Systems Act, 2007, the Consumer Protection Act, 2019, RBI master directions and circulars, and the relevant body of Supreme Court and High Court jurisprudence supplemented by comparative material from the United States and the United Kingdom. The research questions that structure the article are: (i) what is the legal nature of credit card and electronic payment transactions in India; (ii) does the existing legal framework adequately regulate digital payment systems; (iii) how effective are consumer protection mechanisms in addressing unauthorised transactions and digital fraud; (iv) to what extent does the current legal regime safeguard data privacy in financial transactions; and (v) what reforms are necessary to strengthen the regulatory framework. The working hypothesis is that the existing framework, while functionally adequate for routine supervision, is insufficiently codified and coordinated to address the scale of fraud, data-protection and cross-border risk that a payments ecosystem of India's size now generates.

III. CREDIT CARD SYSTEMS: LEGAL NATURE AND OPERATIONAL FRAMEWORK

3.1 Concept, Evolution and the Underlying Contractual Logic

A credit card is, in its simplest legal description, a mechanism by which a bank extends a pre-approved and revolving line of credit to a consumer, who may draw on it to pay a merchant, with the bank undertaking to reimburse the merchant and the consumer undertaking to repay

[13]Douglas W. Arner, Jànos Barberis & Ross P. Buckley, FinTech and RegTech in a Nutshell, and the Future of Regulation, 3 J. Banking Reg. 118 (2017).

the bank on agreed terms. Beneath the plastic (or, increasingly, the tokenised digital credential) lies nothing more exotic than a contract of guarantee coupled with a contract of loan, both governed by the general law of contract. What has changed historically is not the underlying legal form but its scale and infrastructure: informal trader credit gave way to bank-mediated credit, which in turn was industrialised through centralised processing, standard-form documentation and, eventually, real-time digital authorisation.

In the Indian context, the growth of credit card usage tracks the broader liberalisation of the banking sector from the 1990s onward, with the RBI progressively building out a supervisory apparatus most recently consolidated in the Master Direction on Credit Card and Debit Card Issuance and Conduct[14] that governs everything from eligibility criteria to grievance redressal timelines. The integration of Information and Communication Technology (ICT) has been the single largest driver of change in this period: transaction authorisation that once took minutes and relied on manual signature verification is now completed in milliseconds through One-Time Password (OTP) and Additional Factor Authentication (AFA) protocols, and the card itself has become largely incidental to a transaction that may be initiated from a mobile application without the physical instrument ever being presented.

This dematerialisation has not simplified the legal picture if anything, it has multiplied the number of actors whose conduct may be relevant to a dispute, from payment gateways to tokenisation service providers to the mobile operating system through which a wallet application runs. The doctrinal core, however, remains contractual, and it is to that core that the analysis now turns.

3.2 Parties and Transaction Structure

A credit card transaction is rarely, if ever, a bilateral affair. At minimum, it involves the cardholder, the issuing bank, the acquiring bank, the merchant, and the payment network (such as Visa, Mastercard or RuPay) that provides the messaging rail connecting the issuing and acquiring sides. The cardholder's relationship with the issuing bank is documented in a cardholder agreement a Legal Agreement in the terminology this article uses that sets out the credit limit, interest rate, fees, billing cycle and default consequences. The merchant's relationship is with the acquiring bank, which onboards the merchant and settles funds into the

[14]Reserve Bank of India, Master Direction – Credit Card and Debit Card – Issuance and Conduct Directions, 2022, RBI/2022-23/92 DoR.AUT.REC.No.27/24.01.041/2022-23 (Apr. 21, 2022, as updated Mar. 7, 2024).

merchant's account once a transaction clears. The issuing and acquiring banks are, in turn, bound to each other through the operating rules of the payment network, which prescribe interchange fees, dispute (chargeback) procedures and technical standards.

The practical effect of this structure is that a single consumer complaint say, an unauthorised transaction may implicate conduct at several points in the chain: a security lapse at the merchant's payment gateway, a failure of the issuing bank's fraud-detection system, or negligence on the part of the cardholder in safeguarding an OTP. Determining where liability should rest is accordingly a fact-intensive exercise, and Indian courts addressing analogous banker-customer disputes Canara Bank v. Canara Sales Corporation[15] on the duty of care owed by banks in processing transactions, and State Bank of India v. Shyama Devi[16] on the fiduciary character of the banker-customer relationship supply general principles that continue to be applied, by extension, to the digital card context, even though neither case arose from a card transaction. Later decisions such as Punjab National Bank v. Leader Valves Ltd.[17] and Federal Bank Ltd. v. Sagar Thomas[18] reinforce the proposition that a bank's obligations to its customer are not exhausted by mechanical compliance with instructions but extend to a broader duty of diligence.

3.3 The Legal Nature of the Cardholder Agreement

The cardholder agreement is, without much room for debate, a standard form contract: it is drafted entirely by the issuing bank, offered on a take-it-or-leave-it basis, and rarely negotiated in any individual case. Standard form contracting is not inherently objectionable it is, in fact, indispensable to any business that must contract at scale but Indian courts have long recognised that such contracts carry a heightened risk of one-sidedness precisely because the drafting party has no incentive to moderate terms that will never be individually bargained over. The Supreme Court's judgment in Central Inland Water Transport Corporation v. Brojo Nath Ganguly, holding that a contractual term may be struck down as unconscionable and contrary to public policy where it is the product of grossly unequal bargaining power, remains the principal doctrinal resource available to a court reviewing a credit card agreement for fairness, notwithstanding that the case itself concerned a service contract rather than a financial

[15]Canara Bank v. Canara Sales Corp., (1987) 2 SCC 666 (India).
[16]State Bank of India v. Shyama Devi, AIR 1978 SC 1263 (India).
[17]Punjab National Bank v. Leader Valves Ltd., (2006) 13 SCC 375 (India).
[18]Federal Bank Ltd. v. Sagar Thomas, (2003) 10 SCC 733 (India).

instrument.

A second doctrinal development of direct relevance is the judicial acceptance of contracts concluded entirely through electronic means. In Trimex International FZE Ltd. v. Vedanta Aluminium Ltd.[19], the Supreme Court confirmed that an agreement formed through electronic communication is enforceable provided it satisfies the ordinary requirements of offer, acceptance and consideration a proposition that, while decided outside the consumer context, underwrites the validity of the "click-to-accept" mechanism by which most cardholders today agree to the terms and conditions of a card or a UPI-linked application.

3.4 Rights and Liabilities of the Parties

The issuing bank's obligations run in two directions. Toward the payment network and acquiring bank, it must honour authorised transactions and participate in the settlement cycle according to network rules. Toward the cardholder, it owes what the case law has variously described as a duty of care and, in State Bank of India v. Shyama Devi, a fiduciary obligation to safeguard the customer's interests an obligation that, transposed to the digital environment, extends to maintaining adequate fraud-detection systems, promptly flagging suspicious activity, and providing accurate and timely account statements.

The cardholder's principal obligation, correspondingly, is to use the card in accordance with the terms of the agreement and to exercise reasonable care over authentication credentials — PINs, OTPs, CVVs and passwords. The RBI's framework on customer liability for unauthorised electronic transactions, discussed in greater depth in Part VI below, calibrates the cardholder's exposure according to the degree of negligence (if any) on the part of the bank, a third party, or the cardholder, and this calibration is arguably the single most consequential piece of consumer-facing regulation in the entire sector, because it determines who bears the loss in the overwhelming majority of digital fraud disputes.

Acquiring banks and merchants bear parallel, if less visible, obligations: the former to process transactions securely and in compliance with network and regulatory standards, and the latter to follow prescribed protocols for verifying transaction details and safeguarding customer data at the point of sale. Failures at either level a compromised point-of-sale terminal, or a merchant's negligent storage of card data can and do generate liability that eventually flows

[19]Trimex Int'l FZE Ltd. v. Vedanta Aluminium Ltd., (2010) 3 SCC 1 (India).

back, through the network's dispute-resolution mechanisms, toward the party best placed to have prevented the loss.

Where fraud is established, criminal liability may also attach. Syed Asifuddin v. State of Andhra Pradesh[20] illustrates the willingness of Indian courts to treat unauthorised manipulation of electronic systems as a matter for the criminal law, reinforcing the point that the legal response to card fraud operates simultaneously on civil, regulatory and criminal registers.

3.5 Operational Stages: Authorisation, Clearing, Settlement and Billing

The operational life of a transaction proceeds through four broadly distinct stages, each carrying distinct legal significance. Authorisation is the point at which the issuing bank verifies the card's validity, the availability of credit, and through OTP or AFA the authenticity of the person initiating the transaction; it is at this stage that most disputes over unauthorised use ultimately turn, because authorisation is the moment at which the bank's fraud controls were either engaged correctly or were not. Clearing is the exchange of transaction data between the acquiring and issuing banks through the payment network, a largely technical process that nonetheless generates the record on which any subsequent dispute will be adjudicated. Settlement is the actual transfer of funds between banks, completing the financial cycle; the concept of settlement finality the principle that a completed settlement cannot ordinarily be unwound is itself a matter of some legal importance, since it underwrites confidence in the payment system as a whole. Billing, finally, is the point at which the cardholder's contractual liability crystallises into a stated sum, and it is the accuracy and clarity of the billing statement that most directly protects (or fails to protect) the consumer from being charged for a transaction they did not authorise or a fee they did not anticipate.

Judicial recognition of the validity of technologically mediated processes visible, for instance, in State of Maharashtra v. Dr. Praful B. Desai[21]'s acceptance of remote testimony as a legitimate mode of legal proceeding has by extension supported the acceptance of electronically executed banking processes as legally sound, notwithstanding the absence of the physical documentation that once accompanied every stage of a transaction.

[20]Syed Asifuddin v. State of Andhra Pradesh, 2005 Cri LJ 4314 (AP HC) (India).
[21]State of Maharashtra v. Dr. Praful B. Desai, (2003) 4 SCC 601 (India).

3.6 Fraud, Mis-selling and Other Recurring Legal Issues

Two categories of dispute recur with particular frequency in credit card practice. The first is fraud and unauthorised use, arising from phishing, malware, card skimming or outright data breach, where the central legal question is almost always one of allocation: did the loss occur because of the bank's negligence, a third party's wrongdoing, or the cardholder's own carelessness in protecting authentication credentials? The evidentiary standards laid down in Anvar P.V. v. P.K. Basheer and Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal are frequently decisive here, since the only reliable record of what actually happened is the electronic transaction log, and its admissibility depends on strict compliance with certification requirements that many complainants and, at times, banks themselves struggle to satisfy.

The second recurring category is mis-selling: the unsolicited issuance of cards, the imposition of undisclosed charges, or promotional representations that do not match the actual terms of the product. The Consumer Protection Act, 2019 treats such conduct as an unfair trade practice, and the extension of "service" to banking transactions in Lucknow Development Authority v. M.K. Gupta and Indian Medical Association v. V.P. Shantha means that a consumer aggrieved by mis-selling now has a forum in which to seek redress that did not clearly exist before those decisions. NASSCOM v. Ajay Sood[22], while concerned with phishing in a different commercial context, supplies principles on deceptive digital practices that are readily transposable to card-related fraud.

IV. ELECTRONIC PAYMENT SYSTEMS IN INDIA: EVOLUTION AND ARCHITECTURE

4.1 From Manual Clearing to Real-Time Transfer

Indian banking transitioned from an almost entirely manual clearing system cheques, demand drafts, physical passbooks toward electronic settlement in stages that roughly track the country's broader liberalisation trajectory. The Electronic Clearing Service (ECS) and Electronic Funds Transfer (EFT) mechanisms of the 1990s were the first meaningful departures from paper-based settlement, reducing processing times from days to hours. The subsequent creation of the National Payments Corporation of India (NPCI) as a centralised, not-for-profit umbrella organisation for retail payments marked a genuine inflection point: NPCI's Immediate

[22]Nat'l Ass'n of Software & Serv. Cos. v. Ajay Sood, 119 (2005) DLT 596 (Del. HC) (India).

Payment Service (IMPS), launched to enable real-time, twenty-four-hour interbank transfer, and later the Unified Payments Interface (UPI), which allows a consumer to link multiple bank accounts to a single mobile-based virtual payment address and transact instantly, have between them done more to reshape everyday Indian financial behaviour than perhaps any other piece of financial infrastructure in the country's post-liberalisation history.

4.2 The Principal Instruments: NEFT, RTGS, UPI and Prepaid Instruments

National Electronic Funds Transfer (NEFT) processes transfers in batches and is suited to transactions where near-instant settlement is not essential, while Real Time Gross Settlement (RTGS) is reserved for high-value transactions requiring immediate, transaction-by-transaction settlement the "gross" in its name signalling that each transaction is settled individually rather than netted against others. UPI occupies a distinct niche: built for low-value, high-frequency peer-to-peer and person-to-merchant transactions, it has become the default instrument for everyday retail payment precisely because it removes the friction of entering account and routing details for every transaction. Prepaid Payment Instruments (PPIs) digital wallets and prepaid cards supply a further layer, particularly useful for consumers who may not hold a full banking relationship but can still load and spend a defined value electronically.

Each instrument sits within its own RBI framework, but all are ultimately traceable to the same statutory root: the Payment and Settlement Systems Act, 2007, which is the subject of the next Part.

4.3 The Institutional Role of NPCI

NPCI's significance extends beyond any single product. As the entity that operates the interbank messaging infrastructure underlying IMPS, UPI, the National Financial Switch (which connects the country's ATM network) and the Bharat Bill Payment System (BBPS), NPCI functions as something close to a public utility for retail payments, notwithstanding its formally private, not-for-profit structure. This institutional design a centralised infrastructure operator working under RBI oversight but outside the traditional banking regulatory perimeter has proved operationally effective but raises a recurring question addressed in Part IX below: what happens, from an accountability and liability perspective, when the infrastructure itself, rather than any individual bank, is implicated in a systemic failure?

4.4 Technological Underpinnings: Tokenisation and Encryption

Two technological measures deserve brief mention because of their direct legal consequence. Tokenisation the substitution of an actual card number with a unique, merchant- and device-specific token reduces the volume of sensitive card data that merchants and intermediaries need to store, thereby narrowing the attack surface available to a data breach. Encryption, applied both to data in transit and data at rest, is the baseline technical safeguard that RBI directions increasingly treat as a mandatory rather than optional feature of any payment system. Neither measure is, by itself, a legal doctrine, but both have become embedded in regulatory expectation to the point that their absence in a given system would now likely be treated as evidence of a failure to exercise reasonable care.

4.5 Risk and Vulnerability in a Rapidly Scaling System

The same features that have made India's digital payment infrastructure a global reference point speed, interoperability, low transaction cost, minimal friction are also what make it an attractive target. Cyber fraud and data breaches are addressed in detail in Part VII; the point worth registering here is a structural one: because UPI and similar systems are designed to minimise friction, they necessarily minimise the number of checkpoints at which a fraudulent transaction can be intercepted before it is executed, which places a correspondingly greater weight on ex-ante authentication and ex-post liability allocation both of which are examined in the Parts that follow.

V. LEGAL AND REGULATORY FRAMEWORK GOVERNING DIGITAL PAYMENTS

5.1 The Payment and Settlement Systems Act, 2007

The PSS Act is the foundational statute for the regulation of payment systems in India. It vests the RBI with authority to authorise, supervise and, where necessary, penalise operators of payment systems, and it establishes the principle of settlement finality that a settlement, once effected, is final and irrevocable which underwrites confidence in high-value systems such as RTGS. The Act's structure is deliberately broad and enabling rather than prescriptive: it authorises the RBI to issue directions and regulations rather than itself specifying the operational detail of, say, authentication requirements. This design has allowed the regulatory

perimeter to expand to cover instruments UPI, for instance that did not exist when the Act was passed, without requiring fresh primary legislation each time.

Judicial engagement with the RBI's regulatory authority in the payments space has generally been deferential. In Reserve Bank of India v. Peerless General Finance & Investment Co. Ltd.[23], decided outside the digital-payments context but frequently cited within it, the Supreme Court underscored the legitimacy of regulatory oversight in the interest of financial stability. More directly relevant is Internet and Mobile Association of India v. Reserve Bank of India[24], in which the Court, while upholding the RBI's general authority to regulate financial systems, insisted that such regulation must be proportionate and adequately reasoned a principle of real consequence for a regulator that increasingly governs through circular rather than statute, since proportionality review is one of the few external checks available against regulatory overreach in a circular-based regime.

5.2 The Reserve Bank of India: Regulatory Role and Guidelines

The RBI's regulatory function in this space operates through its Department of Payment and Settlement Systems (DPSS) and extends across authentication standards (mandating OTP and AFA for card-not-present transactions), data-security requirements (including tokenisation mandates and, controversially, data-localisation requirements for payment data), customer-liability rules for unauthorised transactions, and grievance-redressal obligations, including the Banking Ombudsman Scheme. This is, in effect, a rulebook built almost entirely through delegated legislation, and its principal virtue the speed with which it can be updated in response to new risks is inseparable from its principal drawback, namely that a consumer's substantive protection can shift with a circular in a way that would require full legislative process in a codified regime.

5.3 The Information Technology Act, 2000: Electronic Transactions and Cyber Offences

The IT Act, 2000[25] supplies two distinct but related functions in the payments context. First, it confers legal recognition on electronic records and digital signatures, which is the statutory basis on which electronic contracting including the "click-to-accept" acceptance of cardholder

[23]Reserve Bank of India v. Peerless Gen. Fin. & Inv. Co. Ltd., (1987) 1 SCC 424 (India).
[24]Internet & Mobile Ass'n of India v. Reserve Bank of India, (2020) 10 SCC 274 (India).
[25]The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

terms rests. Second, it criminalises a range of conduct directly relevant to payment fraud, including unauthorised access to computer systems and identity-related offences, giving the criminal justice system jurisdiction over the more serious forms of card and payment fraud alongside the civil and regulatory remedies discussed elsewhere in this article. The evidentiary provisions relevant to electronic records under this framework, as interpreted in Anvar P.V. v. P.K. Basheer and Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, determine in practice whether a bank's server logs or a consumer's digital communications can be relied upon in any subsequent dispute making these decisions as important to payments litigation as any provision of the PSS Act itself.

5.4 Banking Law and the Role of Financial Institutions

General banking statutes the Reserve Bank of India Act, 1934[26] and the Banking Regulation Act, 1949[27] continue to supply the institutional scaffolding within which payment-specific regulation operates: they define what a bank is, what it may do, and the RBI's general supervisory authority over banking companies, into which the more specific payment-systems regulation is grafted. This layering means that a dispute concerning, say, a credit card issued by a bank may in principle draw on general banking law, contract law, the IT Act, the PSS Act and consumer protection law simultaneously a multiplicity of applicable frameworks that itself contributes to the interpretational uncertainty noted throughout this article.

5.5 KYC, Anti-Money Laundering and Compliance

Know Your Customer (KYC) and Anti-Money Laundering (AML) obligations, principally under the Prevention of Money Laundering Act, 2002[28] and RBI's KYC master directions, form a further compliance layer over card issuance and electronic payments, aimed at preventing the payments system from being used to launder proceeds of crime or finance terrorism. Electronic KYC (e-KYC) and Central KYC (CKYC) mechanisms have themselves become significant enablers of the shift toward digital-first onboarding, illustrating how compliance infrastructure and consumer-facing convenience have, in this instance, developed in tandem rather than in tension.

[26]The Reserve Bank of India Act, 1934, No. 2, Acts of Parliament, 1934 (India).
[27]The Banking Regulation Act, 1949, No. 10, Acts of Parliament, 1949 (India).
[28]The Prevention of Money Laundering Act, 2002, No. 15, Acts of Parliament, 2002 (India).

VI. CONSUMER PROTECTION IN CREDIT CARDS AND DIGITAL PAYMENTS

6.1 Consumer Rights and the Structural Asymmetry of Digital Finance

The consumer in a credit card or electronic payment relationship is structurally disadvantaged in at least three respects: the contract is standard form and non-negotiable; the technology underlying the transaction is opaque to the ordinary user, who has no realistic means of independently verifying whether a security failure originated with the bank, the merchant or an intermediary; and the consumer typically discovers a problem an unauthorised debit, an unexplained fee only after it has already occurred. Consumer protection law in this space is therefore less about preventing disputes than about ensuring that, once a dispute has arisen, the burden of proof and the burden of loss do not fall automatically and unfairly on the weaker party.

6.2 The Consumer Protection Act, 2019

The CPA, 2019 provides the general statutory mechanism[29] through which a cardholder or digital-payment user can seek redress for deficiency in service or unfair trade practice. Its relevance to banking and payments is not self-evident from the text of the Act alone but was established through judicial interpretation: Lucknow Development Authority v. M.K. Gupta read "service" broadly enough to capture public and quasi-public service providers, and Indian Medical Association v. V.P. Shantha extended that reading to professional and institutional services more generally a lineage of interpretation that collectively brings banking and digital-payment services within the CPA's reach, notwithstanding that neither decision was concerned with cards or electronic payments as such.

6.3 The RBI Framework on Customer Liability: Zero and Limited Liability

The most consequential piece of sector-specific consumer protection is the RBI's framework distinguishing zero liability, limited liability and full liability[30] scenarios for unauthorised electronic banking transactions. In broad terms: a customer bears zero liability where the unauthorised transaction results from a contributory fraud, negligence or deficiency on the part of the bank, or from a third-party breach where the system itself was not compromised through

[29]The Consumer Protection Act, 2019, No. 35, Acts of Parliament, 2019 (India).
[30]Reserve Bank of India, Master Direction on Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions, RBI/DOR/2023-24/106 (Jul. 6, 2017, as consolidated 2023).

the customer's fault, provided the customer reports the transaction promptly. Limited liability applies in a narrower band of circumstances typically where there is a delay in reporting, but the delay is not excessive with liability capped according to the reporting delay. Beyond these categories, liability may shift more substantially toward the customer where the loss arises from the customer's own negligence, such as sharing an OTP or PIN.

This framework represents a genuinely consumer-protective innovation, but its practical value depends heavily on two variables that the framework itself does not fully control: how quickly a bank actually credits a disputed amount pending investigation (delay here can functionally defeat the protection even where the customer is ultimately vindicated), and how readily a consumer can establish, evidentially, that a transaction was in fact unauthorised a burden that circles back to the electronic-evidence requirements discussed in Part III and V.

6.4 Grievance Redressal: Institutional Mechanisms and the Banking Ombudsman

Every regulated entity is required to maintain an internal grievance redressal mechanism, and unresolved complaints may in principle escalate to the Banking Ombudsman Scheme, which offers a cost-free avenue for dispute resolution outside the court system. In practice, the effectiveness of these mechanisms varies considerably: complainants frequently report generic responses, procedural delays, and difficulty escalating a complaint once an initial (and often unsatisfactory) internal resolution has been offered. Where an institution's grievance mechanism functions poorly enough to itself constitute a deficiency in service, the reasoning in Lucknow Development Authority v. M.K. Gupta suggests that the institution's conduct and not merely the underlying transaction dispute may become an independent basis for liability under the CPA.

6.5 Judicial Contribution to Consumer Protection

In the continued absence of a single, comprehensive statute addressing digital financial transactions, courts have done substantial work adapting general principles to this context. The banker's duty of care recognised in Canara Bank v. Canara Sales Corporation and the fiduciary character of the banker-customer relationship articulated in State Bank of India v. Shyama Devi remain foundational, and have been read, in later commentary and lower-court application, as extending naturally to digital-era obligations such as maintaining adequate fraud-detection systems and responding promptly to reported suspicious activity. The evidentiary framework

established in Anvar P.V. v. P.K. Basheer and Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal shapes, as a practical matter, which disputes can even be adjudicated on the merits, since a complainant unable to produce properly certified electronic evidence may find a meritorious claim dismissed on a threshold, procedural ground.

The judicial treatment of intermediary liability Avnish Bajaj v. State (NCT of Delhi)[31] and Shreya Singhal v. Union of India[32], both concerned primarily with online platforms rather than payment intermediaries has nonetheless contributed a set of balancing principles (accountability without disproportionate liability that would chill innovation) that are increasingly relevant as payment gateways, aggregators and application providers multiply within the transaction chain.

Taken together, this body of case law demonstrates both the strength and the limitation of judicial adaptation: courts have been consistently protective of consumer interests where a dispute reaches them, but case-by-case adjudication cannot substitute for the certainty that comprehensive legislation would provide, and disparities in outcome across different fora remain a real risk in the absence of codification.

VII. DATA PROTECTION, PRIVACY AND CYBERSECURITY CONCERNS

7.1 Why Data Protection Matters in the Payments Context

Every digital payment generates a trail of data far richer than the transaction amount alone: identity, location, device fingerprint, merchant category, spending pattern and, increasingly, behavioural metadata used for fraud scoring and credit assessment. This data is collected, stored and processed by banks, Payment Service Providers (PSPs) and a growing number of downstream technology intermediaries, and its concentration creates risk at two distinct levels the individual level, where a breach can lead to financial loss, identity theft or reputational harm, and the systemic level, where a large-scale breach can undermine confidence in digital payments generally, with knock-on effects for financial inclusion objectives that depend on public trust in these very systems.

7.2 The Constitutional Foundation: Justice K.S. Puttaswamy v. Union of India

The Supreme Court's recognition, in Justice K.S. Puttaswamy v. Union of India, that privacy

[31]Avnish Bajaj v. State (NCT of Delhi), 150 (2008) DLT 769 (Del. HC) (India).
[32]Shreya Singhal v. Union of India, (2015) 5 SCC 1 (India).

is an intrinsic facet of the right to life and personal liberty under Article 21 fundamentally altered the legal register in which financial data protection is discussed in India, moving it from a matter of contractual or regulatory good practice to one of constitutional entitlement. The judgment's insistence that any intrusion into privacy satisfy the tests of legality, necessity and proportionality has direct application to payments data: a financial institution's collection of data must rest on a valid legal basis, serve a legitimate and clearly articulated purpose, and be proportionate to that purpose rather than expansive merely because the technology permits expansive collection.

A further dimension the Puttaswamy framework foregrounds is the quality of consent. Consumers routinely "consent" to data collection through standard-form digital agreements they have neither the time nor, often, the technical literacy to meaningfully evaluate a concern that parallels, and compounds, the unconscionability concerns raised in Part III in relation to cardholder agreements generally. Consent obtained in this manner is formally valid but substantively thin, and the gap between the two is precisely where regulatory intervention (discussed in Part X) is most needed.

7.3 Cybersecurity: Threats and the Existing Legal Response

The threat landscape facing digital payment systems includes phishing and vishing (voice-based social engineering), malware, card skimming, credential-stuffing attacks, and outright data breaches at any of the several institutions and intermediaries that touch a given transaction. India's legal response to these threats currently rests primarily on the IT Act's cyber-offence provisions and RBI's cybersecurity directions to regulated entities (mandating, for instance, security operations centres and periodic vulnerability assessments at banks), rather than on a unified, sector-specific cybersecurity statute. This is a narrower response than the scale of the threat arguably warrants: cyber-attacks on payment infrastructure routinely cross institutional and jurisdictional boundaries in ways that a bank-by-bank compliance regime, however rigorously enforced, is not fully designed to address.

7.4 The Regulatory Gap: The Absence of a Fully Operative, Payments-Specific Data Protection Regime

India's general data protection legislation the Digital Personal Data Protection Act, 2023[33] establishes cross-sectoral principles for the processing of personal data, but its practical

[33]The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

operation in the financial sector depends on rules and sectoral guidance that continue to develop, and payments data carries sensitivities (transaction-level financial behaviour, in particular) that arguably warrant treatment as a distinct category with heightened safeguards, in the manner that health data is often treated elsewhere. Until such sector-specific calibration is fully in place, the RBI's own data-security and data-localisation directions remain the primary operative safeguard for payments data specifically a state of affairs that, as with the liability framework discussed in Part VI, places significant weight on regulatory circulars rather than codified statutory protection.

VIII. COMPARATIVE ANALYSIS: INTERNATIONAL FRAMEWORKS AND LESSONS FOR INDIA

8.1 The United States: Codified Consumer-Finance Statutes

The United States regulates consumer credit and electronic transfers through detailed, codified statutes most notably the Truth in Lending Act (TILA)[34], which mandates standardised disclosure of credit terms, and the Electronic Fund Transfer Act (EFTA)[35], which establishes clear liability limits for unauthorised electronic transfers. Enforcement is centralised in a dedicated regulator, the Consumer Financial Protection Bureau (CFPB)[36], which possesses rulemaking, supervisory and enforcement powers specifically oriented toward consumer financial protection, distinct from the broader prudential regulation of banks. The American model's principal strength, from an Indian comparative perspective, is precisely its codification: a consumer's rights are set out in statute and accompanying federal regulation, not primarily in the equivalent of an RBI circular, which affords a degree of permanence and judicial predictability that India's circular-heavy framework does not currently replicate.

8.2 The United Kingdom: Data-Integrated, Open-Banking Regulation

The United Kingdom's framework is distinguished by two features of particular relevance here. First, its consumer-finance regulation, principally through the Financial Conduct Authority (FCA), operates in close integration with data protection law under the UK GDPR[37], producing

[34]Truth in Lending Act, 15 U.S.C. § 1601 et seq. (2018).
[35]Electronic Fund Transfer Act, 15 U.S.C. § 1693 et seq. (2018).
[36]Dodd-Frank Wall Street Reform and Consumer Protection Act § 1011, 12 U.S.C. § 5491 (2010) (establishing the CFPB).
[37]Data Protection Act 2018, c. 12 (UK), incorporating Regulation (EU) 2016/679 (General Data Protection Regulation) as retained EU law.

a regime in which financial regulation and data protection are treated as facets of the same regulatory problem rather than as separate silos a contrast with the Indian position, where payments regulation (RBI) and general data protection law currently operate through substantially separate institutional channels. Second, the UK's open-banking regime, which mandates secure, standardised data-sharing between banks and authorised third-party providers (subject to customer consent), illustrates a model for fostering competition and innovation in payments while keeping data-sharing within a clearly regulated, auditable structure a design consideration India's own account-aggregator framework has begun to approximate, though on a narrower footing.

8.3 What India Can and Cannot Import

The value of this comparison lies less in identifying provisions for wholesale transplantation than in isolating design principles that are transferable notwithstanding India's very different scale, demographic diversity and financial-inclusion priorities. Three lessons stand out. First, statutory codification of core consumer protections disclosure standards, liability limits, dispute-resolution timelines would reduce India's current dependence on RBI circulars for substantive consumer rights, without displacing the RBI's continued role in technical and prudential regulation. Second, closer institutional integration between payments regulation and data protection law would address the structural gap identified in Part VII, where payments-specific data safeguards currently sit somewhat apart from the general data protection regime. Third, a codified, statute-backed liability framework akin to EFTA's clear caps would strengthen the predictability of India's existing, but circular-based, zero/limited-liability rules.

At the same time, direct transplantation is neither feasible nor necessarily desirable: the CFPB's institutional model presupposes a regulatory capacity and a degree of institutional separation from prudential banking supervision that would require significant restructuring to replicate in India, and the UK's open-banking regime presupposes levels of digital and financial literacy, and of uniform technological access, that remain unevenly distributed across India's population. India's own RBI-driven, sandbox-oriented model has, notably, enabled faster and more inclusive innovation UPI's rapid, near-universal adoption has few genuine international parallels and any reform agenda should aim to graft greater codification and institutional coordination onto that model rather than discard what has, on its own terms, worked.

IX. CHALLENGES AND EMERGING ISSUES

9.1 Digital Fraud and Identity Theft

Phishing, vishing, malware and card-cloning schemes increasingly exploit human vulnerability rather than purely technical weakness, which complicates liability determination precisely along the fault lines discussed in Part VI: was the loss attributable to bank negligence, third-party wrongdoing, or the consumer's own lapse in safeguarding credentials? Identity theft, where financial and personal data is misappropriated to impersonate a consumer, compounds this problem by generating harm that outlasts the immediate transaction affecting creditworthiness and long-term financial standing in ways a single unauthorised-transaction reversal cannot fully remedy. The cross-border character of much digital fraud perpetrators frequently operating from outside Indian jurisdiction further strains an enforcement architecture built primarily around domestic criminal process.

9.2 Regulatory Challenges in FinTech

FinTech entities digital wallet operators, peer-to-peer payment platforms, payment aggregators frequently perform functions functionally similar to banks without being subject to identical regulatory obligations, producing a category ambiguity that the existing bank-centred regulatory perimeter is not fully designed to resolve. The RBI's use of regulatory sandboxes represents a constructive, proportionate response, consistent with the Supreme Court's insistence in Internet and Mobile Association of India v. Reserve Bank of India that regulation of this sector be proportionate and well-reasoned rather than reflexively restrictive; but sandboxes are, by design, limited in scale and duration, and the harder question of how FinTech entities should be regulated once they exit the sandbox and operate at national scale remains only partially settled.

9.3 Financial Inclusion and the Digital Divide

The same digitisation that has expanded access to formal financial services for many previously underserved consumers risks excluding those without reliable internet connectivity, smartphone access, or digital literacy a risk that is not hypothetical in a country as demographically and geographically diverse as India. Regulatory design that assumes uniform digital fluency risks entrenching, rather than narrowing, existing inequality, which is why

continued investment in multilingual interfaces, offline or low-connectivity payment channels, and financial literacy initiatives remains as much a legal-policy priority as a purely developmental one.

X. SUGGESTIONS AND RECOMMENDATIONS

10.1 Legislative Consolidation

The single most structurally significant reform available to Indian policymakers is the consolidation of the currently fragmented framework spread across the PSS Act, the IT Act, RBI circulars and CPA provisions into a dedicated digital payments statute that codifies the core consumer protections (liability limits, disclosure standards, dispute-resolution timelines) currently found only in circulars, while preserving the RBI's flexibility to update technical and operational detail through subordinate rule-making. Codification of this kind would not eliminate the RBI's regulatory role; it would simply relocate the consumer's substantive rights to a more stable and judicially accessible instrument.

10.2 Strengthened and Coordinated Enforcement

Regulatory overlap across banking, information technology, consumer protection and data privacy domains calls for clearer jurisdictional boundaries and structured inter-agency coordination, potentially through a standing coordination mechanism linking the RBI, the Ministry of Electronics and Information Technology, and consumer protection authorities, so that a single incident a data breach with both cybersecurity and consumer protection dimensions, for instance does not fall through gaps between separately administered regimes.

10.3 Standardised, Layered Disclosure

Cardholder and digital-payment agreements should be required to present key terms interest rates, fees, liability conditions, dispute-resolution channels in a standardised, simplified format at the point of acceptance, with full legal terms available separately. Layered disclosure of this kind directly addresses the "thin consent" problem identified in Part VII without requiring wholesale prohibition of standard-form contracting, which would be neither feasible nor desirable at the scale digital payments now operate.

10.4 A Codified Liability Framework with Enforceable Timelines

The existing zero/limited-liability principles should be elevated from circular to statute, and coupled with binding timelines for provisional credit pending investigation of a disputed transaction, so that consumers are not left bearing the practical cost of fraud during what can otherwise be a protracted investigatory period even where they are ultimately vindicated.

10.5 Minimum Cybersecurity Baselines Across the Ecosystem

Cybersecurity obligations currently fall most heavily on regulated banks; smaller FinTech entities and intermediaries, which increasingly sit within the transaction chain, should be subject to enforceable minimum security standards encryption, tokenisation, periodic independent audit proportionate to their role, together with a centralised incident-reporting mechanism that allows regulators to identify systemic patterns that a single institution's isolated reporting would not reveal.

10.6 Financial and Digital Literacy as a Regulatory Priority

Sustained, well-funded financial and digital literacy initiatives should be treated as integral to consumer protection policy rather than as a peripheral public-awareness exercise, given how much of the existing liability and dispute-resolution framework depends on consumers understanding and promptly exercising rights they may not otherwise know they possess.

XI. CONCLUSION

The Indian legal system has, on the whole, kept pace with the extraordinary operational growth of credit cards and electronic payment systems, but it has done so unevenly: judicial adaptation of general contract, banking and constitutional doctrine has been consistently protective of consumer interests where a dispute actually reaches a court, and the RBI's circular-based regulatory apparatus has proved nimble enough to respond to new products and new risks as they emerge. What remains missing is architectural coherence a single, codified statute that would relocate the consumer's core protections from regulatory circular to legislative text, integrate data protection more closely with payments regulation, and establish enforceable, rather than merely aspirational, timelines for dispute resolution. None of the reforms proposed in this article require India to abandon what has, by any reasonable international comparison, been a genuinely successful model of payments innovation; they require, instead, that the next

phase of legal development be aimed deliberately at consolidation and codification rather than further incremental expansion. A payments system as large, as fast, and as central to everyday economic life as India's has become deserves a legal foundation commensurate with its scale one built on statute rather than circular, and on codified rights rather than case-by-case judicial improvisation.