Page: 1713-1744 *URL: www.lijdlr.com*

LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

ISSN: 2583-7753

LawFoyer International Journal of Doctrinal Legal Research

[ISSN: 2583-7753]

Volume 4 | Issue 1

2026

DOI: https://doi.org/10.70183/lijdlr.2026.v04.76

© 2026 LawFoyer International Journal of Doctrinal Legal Research

Follow this and additional research works at: www.lijdlr.com
Under the Platform of LawFoyer – www.lawfoyer.in

After careful consideration, the editorial board of LawFoyer International Journal of Doctrinal Legal Research has decided to publish this submission as part of the publication.

In case of any suggestions or complaints, kindly contact (info.lijdlr@gmail.com)
To submit your Manuscript for Publication in the LawFoyer International Journal of Doctrinal Legal Research, To submit your Manuscript Click here

FEAR OF DIGITAL FRAUD: A COMPARISON BETWEEN PERCEIVED EASE OF USE AND ACTUAL ADOPTION IN RURAL UTTAR PRADESH

Ria Singh[1], Dr. Arvind Kumar Singh[2] & Dr Priya Dwivedi[3]

I. ABSTRACT

This paper examines whether perceived ease of use in digital payment systems actually translates into meaningful and sustained adoption in rural Uttar Pradesh, or whether fear of digital fraud disrupts that transition. The study situates the issue within India's rapidly expanding digital payments ecosystem, where national growth figures coexist with uneven user confidence at the rural level. It argues that access to internet connectivity and payment interfaces does not by itself establish real digital inclusion. Rather, actual adoption depends upon legal confidence, procedural awareness, and the perceived availability of timely redress. Drawing on the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Digital Personal Data Protection Act, 2023, RBI consumer protection norms, and official government data, the paper shows that rural users often experience digital participation under conditions of mistrust, asymmetric information, and structural vulnerability. The contrast between widespread household internet access and much lower capacity to conduct online banking or report cyber fraud demonstrates that interface simplicity alone cannot secure lawful and confident participation. The paper concludes that fear of digital fraud operates not merely as a private hesitation, but as a governance barrier that weakens financial inclusion and requires stronger user-centred legal and regulatory safeguards.

II. KEYWORDS

Digital fraud, rural Uttar Pradesh, perceived ease of use, actual adoption, digital financial inclusion.

[1] 10th Semester Student at Amity Law School, Lucknow Campus (India). Email: ria.singh4@s.amity.edu
[2] Associate Professor at Amity Law School, Lucknow Campus (India).
[3] Associate Professor at Institute of Professional Education and Research, Bhopal, MP (India).

© 2026. LawFoyer International Journal of Doctrinal Legal Research (ISSN: 2583-7753)

III. INTRODUCTION

A. Background of Research

India's digital payment landscape has expanded at a remarkable pace, and that expansion forms the immediate background of this research. The Ministry of Finance stated in March 2026 that retail digital payment transactions reached 22,167.90 crore in FY 2024-25 and that UPI alone accounted for 81 percent of retail digital payments. This growth reflects a policy shift in which everyday exchange, welfare distribution, merchant settlement, and low-value household transactions increasingly move through digital rails. The legal question, therefore, no longer concerns whether digital payments exist in India. It concerns whether citizens, especially rural users, can trust these systems enough to use them with confidence.[4]

Rural Uttar Pradesh presents a particularly important site for that inquiry. The National Statistical Office's *Comprehensive Modular Survey: Telecom, 2025* reports that 85.1 percent of rural households in Uttar Pradesh had internet facility within household premises. At the same time, among persons aged 15 years and above, only 36.7 percent of rural persons in the State reported the ability to perform online banking transactions. This contrast is crucial. It shows that access and capability do not move together in equal measure. A household may possess connectivity, yet the individual user may still hesitate at the point of payment, authorisation, or complaint.[5]

That hesitation is not irrational. It arises within a visible fraud environment. The Ministry of Home Affairs reported in March 2026 that the Citizen Financial Cyber Fraud Reporting and Management System had, till 31 January 2026, helped save more than Rs. 8,690 crore

[4] Press Information Bureau, Ministry of Finance, Coordinated Efforts of Government, RBI and NPCI Accelerate Growth in Digital Payments, UPI Emerges as World's Largest Real-Time Retail Payment System, Accounting for 81% of Retail Digital Payments in FY 2024-25 (Mar. 16, 2026), https://www.pib.gov.in/PressReleasePage.aspx?PRID=2240723 (last visited Mar. 25, 2026).
[5] Ministry of Statistics & Programme Implementation, National Statistical Office, NSS Report No. 593, Comprehensive Modular Survey: Telecom, 2025 tbls. 12, 14 (May 2025), https://www.mospi.gov.in/sites/default/files/publication_reports/CMST_report_m.pdf (last visited Mar. 25, 2026).

across more than 24.65 lakh complaints, while the 1930 helpline had been operationalised for immediate assistance in online cyber complaints. These figures show that digital fraud is not peripheral to India's payment story. It is one of its central risks. For a first-generation rural user, the fear of wrongful debit, impersonation, OTP theft, or failed recovery can easily become stronger than the convenience of the interface itself.[6]

This research also emerges from India's broader financial inclusion strategy. The Reserve Bank of India's *National Strategy for Financial Inclusion 2019-2024* emphasised that digital inclusion in rural areas depends on better networking of bank branches, business correspondent outlets, micro-ATMs, Point of Sale terminals, stable connectivity, and participation of local institutions such as panchayats and Common Service Centres. That policy vision implicitly recognises that digital adoption is social and institutional, not merely technical. The present study builds on that insight and examines whether perceived ease of use in rural Uttar Pradesh actually matures into secure and sustained adoption, or whether fear of digital fraud interrupts that transition.[7]

B. Research Questions

1. To what extent does fear of digital fraud affect the actual adoption of digital payment systems in rural Uttar Pradesh despite the apparent ease of use of such platforms?
2. How far does the distinction between perceived ease of use and actual adoption explain the cautious, partial, or assisted use of digital payment services among rural users?
3. Whether the existing Indian legal and regulatory framework, including the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the

[6] Government of India, Ministry of Home Affairs, Lok Sabha Unstarred Question No. 4118, Cyber Crime in the Country (Mar. 17, 2026), https://www.mha.gov.in/MHA1/Par2017/pdfs/par2026-pdfs/LS17032026/4118.pdf (last visited Mar. 25, 2026).
[7] Reserve Bank of India, National Strategy for Financial Inclusion 2019-2024 30-31, https://www.rbi.org.in/commonman/Upload/English/Content/PDFs/English_16042021.pdf (last visited Mar. 25, 2026).

Digital Personal Data Protection Act, 2023, and the Reserve Bank of India's consumer protection framework, adequately addresses fear as a barrier to lawful digital participation?

4. What role do digital literacy, procedural awareness, grievance redress mechanisms, and institutional trust play in shaping user confidence in digital payment ecosystems in rural Uttar Pradesh?
5. What legal, regulatory, and policy reforms are necessary to convert formal digital access into secure, informed, and sustained digital financial adoption in rural areas?

C. Research Objectives

1. To examine the relationship between perceived ease of use of digital payment platforms and their actual adoption in rural Uttar Pradesh.
2. To analyse how fear of digital fraud, perceived vulnerability, and lack of legal confidence influence user behaviour in rural digital payment ecosystems.
3. To evaluate the adequacy of the existing Indian statutory and regulatory framework in preventing digital fraud and in strengthening user trust, protection, and redress.
4. To identify the structural barriers that hinder meaningful adoption, including limited digital literacy, weak complaint capacity, asymmetric information, and dependence on assisted transactions.
5. To propose legal and policy recommendations for building a safer, more accessible, and trust-oriented digital payment environment for rural users in Uttar Pradesh.

D. Research Methodology

This study adopts a mixed doctrinal and analytical socio legal research methodology to examine the gap between perceived ease of use and actual adoption of digital payment

systems in rural Uttar Pradesh. The doctrinal component analyses the applicable Indian legal and regulatory framework, including the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Digital Personal Data Protection Act, 2023, relevant RBI consumer protection directions, and cyber fraud reporting mechanisms, in order to assess how law addresses trust, liability, redress, and digital security. The analytical component evaluates official statistical and policy materials relating to internet access, digital capability, online banking use, cyber fraud reporting, and rural digital inclusion, with specific focus on Uttar Pradesh. The methodology is therefore designed not merely to measure technical usability, but to investigate whether formal digital access matures into secure, informed, and sustained adoption in conditions shaped by fear of fraud, weak complaint capacity, and uneven legal confidence. In this sense, the study treats digital adoption as a legal and governance question rather than a purely technological one.

IV. CONCEPTUALISING "FEAR OF DIGITAL FRAUD" IN LAW AND GOVERNANCE

A. Meaning of digital fraud in the Indian legal context

"Digital fraud" does not appear in Indian law as one closed and self-contained statutory definition. Indian law treats it as an umbrella expression for deception carried out through a computer resource, communication device, digital payment interface, or stolen authentication credentials. Its legal core lies in dishonest digital conduct that induces a person to part with money, data, access, or transactional authority. The Information Technology Act, 2000 gives the most direct cyber-specific content to this idea through section 66 on computer related offences, section 66C on identity theft, and section 66D on cheating by personation by using a computer resource.[8]

The penal meaning of digital fraud now also rests within the Bharatiya Nyaya Sanhita, 2023. Section 318 defines cheating as deception that fraudulently or dishonestly induces

[8] Information Technology Act, 2000, No. 21 of 2000, §§ 66, 66C, 66D (India).

delivery of property, retention of property, or an act or omission likely to cause harm to body, mind, reputation, or property. The Explanation makes dishonest concealment of facts a form of deception. Section 319 separately punishes cheating by personation. In digital settings, this captures fake bank officials, impersonation through cloned profiles, false KYC requests, and fraudulent payment demands made under a fabricated identity.[9]

In banking regulation, the expression carries a broader functional meaning. The Reserve Bank of India's framework on unauthorised electronic banking transactions treats fraud risk across remote and online payment transactions, including internet banking, mobile banking, card-not-present transactions, and prepaid payment instruments. It requires banks to maintain robust fraud detection systems, customer alerts, and round-the-clock reporting channels. Thus, digital fraud in Indian governance is not only a criminal wrong after loss occurs. It is also a regulated risk within the architecture of consumer protection and payment security.[10]

The Digital Personal Data Protection Act, 2023 adds a further layer by requiring Data Fiduciaries to adopt appropriate technical and organisational measures and reasonable security safeguards to prevent personal data breach. That matters because many fraud events begin with credential theft, unauthorised access, or misuse of personal data. In Indian legal context, therefore, digital fraud covers cyber deception, personation, unauthorised transaction inducement, and data-enabled economic harm. The law addresses the same injury through different statutory routes, so the victim often sees one fraud while the legal system sees several connected violations.[11]

B. Fear, Mistrust and Perceived Vulnerability as Barriers to Lawful Digital Participation

Lawful digital participation is not secured merely because a payment rail exists in law. It depends on whether the user believes the system can prevent loss, record a complaint,

[9] Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023, §§ 318, 319 (India).
[10] Reserve Bank of India, Limiting Liability of Customers in Unauthorised Electronic Banking Transactions, DBR.No.Leg.BC.78/09.07.005/2017-18 (July 6, 2017).
[11] Digital Personal Data Protection Act, 2023, No. 22 of 2023, § 8 (India).

and stop further dissipation of funds. Indian governance now treats that anxiety as a real compliance issue. The National Cybercrime Reporting Portal and the Citizen Financial Cyber Fraud Reporting and Management System connect banks, payment intermediaries, wallets and the 1930 helpline for immediate reporting of financial cyber fraud. That institutional design shows mistrust is not a private feeling alone. It is a public barrier to participation, and the State now manages it through coordinated redress.[12]

Fear also grows where the user lacks control over personal data and transactional identity. In *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, the Supreme Court treated informational privacy as part of dignity, autonomy and personal liberty. That reasoning matters here. A large share of digital payment fraud begins with misuse of KYC data, OTPs, mobile numbers, credentials or impersonation. Section 8 of the Digital Personal Data Protection Act, 2023 now requires appropriate technical and organisational measures and reasonable security safeguards. Yet the rural user often experiences the law after the breach, not before it, so vulnerability still shapes behaviour.[13]

In *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637, the Supreme Court held that speech and trade through the internet receive constitutional protection under Articles 19(1)(a) and 19(1)(g). That principle carries weight beyond shutdown cases. When a citizen avoids digital banking or online payment systems because the medium appears unsafe, the loss is not only transactional. It affects practical access to markets, services, communication and lawful economic activity. Fear of digital fraud therefore operates as a governance barrier. It narrows the real exercise of rights even where the legal framework formally permits digital inclusion.[14]

C. Distinguishing Perceived Ease of Use from Actual Adoption

Perceived ease of use is a narrower idea than adoption. Fred D. Davis described it as the degree to which a person believes that using a system would be free of effort. That

[12] Indian Cybercrime Coordination Centre, National Cybercrime Reporting Portal (NCRP), Ministry of Home Affairs, Government of India, https://i4c.mha.gov.in/ncrp.aspx (last visited Mar. 25, 2026).
[13] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1.
[14] Anuradha Bhasin v. Union of India, (2020) 3 S.C.C. 637.

concept explains interface comfort. It does not, by itself, prove trust. Actual adoption is more demanding. It requires repeated, voluntary and self-directed use under conditions of risk, uncertainty and possible loss. A payment application may look simple on screen, yet remain only shallowly accepted when the user fears deception, mistaken transfers, or delayed reversals.[15]

Indian payments data makes this distinction sharper. The Ministry of Finance reported in March 2026 that retail digital payment transactions reached 22,167.90 crore in FY 2024-25 and that UPI accounted for 81% of retail digital payments in that year. The same official statement also noted that challenges remain in cyber security, digital adoption, literacy and awareness, and that no demographic or geographic segment-wise contribution data is maintained. So scale at the national level cannot be read as proof of settled trust in rural districts. Aggregate success may still coexist with cautious, low-value, assisted or reversible use.[16]

That caution becomes more visible in rural Uttar Pradesh. A recent MoSPI analysis reported that ICT skill penetration stands at 13.23% in rural India but only 7.94% in rural Uttar Pradesh. This gap matters. It suggests that apparent ease, such as QR scanning, voice prompts, or simplified icons, may coexist with weak independent digital capability. In such settings, actual adoption often remains partial. Sometimes delegated. Sometimes fragile. The user may transact, but not with confidence. That is the space where perceived ease of use and actual adoption clearly part ways.[17]

---

[15] Fred D. Davis, Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology, 13 MIS Q. 319 (1989), https://misq.umn.edu/misq/article-abstract/13/3/319/191/Perceived-Usefulness-Perceived-Ease-of-Use-and?redirectedFrom=fulltext (last visited Mar. 25, 2026).

[16] Press Information Bureau, Ministry of Finance, Coordinated Efforts of Government, RBI and NPCI Accelerate Growth in Digital Payments (Mar. 16, 2026), https://www.pib.gov.in/PressReleasePage.aspx?PRID=2240723&lang=1&reg=3.

[17] Ministry of Statistics & Programme Implementation, Sarvekshana, Combined Issue 118-119, at 67, https://www.mospi.gov.in/uploads/publications_reports/publications_reports1764138233782_4e47b439-d884-428e-a431-cf99c5346384_Sarvekshana_Final_-_118-119_Issue_%2824-11-2025%29_%282%29.pdf (last visited Mar. 25, 2026).

D. Adoption as a Question of Legal Confidence, Not Merely Interface Simplicity

Digital adoption in payment law turns on legal confidence, not on visual ease alone. A simple interface can attract first use. It cannot secure repeated lawful participation unless the user believes that loss will be traceable, complaints will be recorded, and liability will be fairly allocated. RBI's framework on unauthorised electronic banking transactions makes this plain. It directs banks to design systems that "make customers feel safe," mandates 24x7 reporting channels, provides for zero or limited customer liability in defined cases, requires shadow reversal within ten working days, and places the burden of proving customer liability on the bank. The later ODR framework for digital payments follows the same logic. Adoption survives where remedy feels real. Not where design merely feels smooth.[18]

That is why adoption must be read as a legal relation of trust. Not as a narrow usability metric. In *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1, the Supreme Court linked privacy with dignity, autonomy, and informational self-determination. In digital payment spaces, that principle matters in a very practical sense. A user who fears misuse of mobile number, OTP, biometric identity, or transaction trail does not merely fear inconvenience. The user fears loss of control. Sections 66C and 66D of the Information Technology Act, 2000 and the security obligations under the Digital Personal Data Protection Act, 2023 reflect that same concern. So, lawful adoption depends on whether the user trusts the legal order to protect identity, data, and consent before and after the transaction.[19]

E. Rural Users, Asymmetric Information and Structural Susceptibility

National payment growth should not be confused with uniform confidence. The Ministry of Finance reported on 16 March 2026 that retail digital payments reached 22,167.90 crore

[18] Reserve Bank of India, Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions, RBI/2017-18/15, DBR.No.Leg.BC.78/09.07.005/2017-18 (July 6, 2017), https://www.rbi.org.in/commonman/english/scripts/Notification.aspx?Id=2336 (last visited Mar. 25, 2026).
[19] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1.

transactions in FY 2024-25 and that UPI accounted for 81 percent of retail digital payments. Yet the same official statement accepted that cyber security risk, literacy, awareness, and adoption challenges persist, and also stated that no demographic or geographic segment-wise contribution data is maintained. That caveat is important. It means macro-scale success does not prove secure or informed adoption in rural Uttar Pradesh. The numbers show spread. They do not prove trust.[20]

Structural susceptibility becomes sharper when digital capability remains thin. MoSPI's *Sarvekshana* reports ICT skill penetration at 13.23 percent in rural India but only 7.94 percent in rural Uttar Pradesh. That gap is legally significant. A person may know how to press a payment button and still not understand a collect request, a remote access prompt, a fake KYC link, or the reporting timeline after unauthorised debit. In such settings, fraud exposure is not simply a matter of carelessness. It grows out of unequal comprehension. Rural users often enter digital systems with weaker ability to detect deception and weaker capacity to contest it quickly. Interface simplicity can therefore hide a deeper asymmetry of risk.[21]

Information asymmetry deepens that exposure. World Bank work on digital financial inclusion identifies confusing terms, limited transparency, poor usability, and lack of financial awareness as recurring frictions even where services formally exist. That analysis fits rural payment markets in India rather well. Banks, platforms, telecom actors, and intermediaries understand transaction architecture, fraud-detection logic, escalation routes, and data processing practices far better than the end user. The Consumer Protection Act, 2019 and the DPDP Act, 2023 move toward fairer disclosure and safer

[20] Press Information Bureau, Ministry of Finance, Coordinated Efforts of Government, RBI and NPCI Accelerate Growth in Digital Payments, UPI Emerges as World's Largest Real-Time Retail Payment System, Accounting for 81% of Retail Digital Payments in FY 2024-25 (Mar. 16, 2026), https://www.pib.gov.in/PressReleasePage.aspx?PRID=2240723 (last visited Mar. 25, 2026).
[21] Ministry of Statistics & Programme Implementation, Sarvekshana, Combined Issue 118-119 (2025), https://www.mospi.gov.in/uploads/publications_reports/publications_reports1764138233782_4e47b439-d884-428e-a431-cf99c5346384_Sarvekshana_Final_-_118-119_Issue_%2824-11-2025%29_%282%29.pdf (last visited Mar. 25, 2026).

processing, but they do not eliminate the knowledge gap at the moment of consent. The rural user often agrees first and understands later, sometimes too late.[22]

The State's own fraud-control design confirms that this vulnerability is structural, not anecdotal. In a Lok Sabha reply dated 2 December 2025, the Ministry of Home Affairs stated that the Citizen Financial Cyber Fraud Reporting and Management System had, since 2021, helped save more than Rs. 7,130 crore across more than 23.02 lakh complaints, alongside the 1930 helpline and the Cyber Fraud Mitigation Centre. Such an architecture exists because digital fraud moves in real time and recovery depends on immediate intervention. For rural users, delays caused by language barriers, poor connectivity, reliance on assisted use, or uncertainty about where to complain may decide whether funds are frozen or gone. Structural susceptibility, then, lies in unequal access to prevention and redress not merely in individual caution.[23]

V. DIGITAL FRAUD IN RURAL PAYMENT ECOSYSTEMS

Rural payment ecosystems now sit inside India's wider digital payment surge. The Ministry of Finance stated in March 2026 that retail digital payment transactions reached 22,167.90 crore in FY 2024-25 and that UPI alone accounted for 81 percent of retail digital payments. That scale matters for rural Uttar Pradesh because State welfare transfer systems, merchant payments, peer transfers, and small-value retail exchanges increasingly travel through the same digital rails. Fraud risk therefore does not remain urban or exceptional. It enters ordinary payment life.[24]

---

[22] Arjun Patwardhan, Financial Inclusion in the Digital Age (World Bank Group 2018), https://documents1.worldbank.org/curated/en/586641525332812963/pdf/125912-WP-Financial%20-%20Inclusion-in-the-Digital-Age-PUBLIC.pdf (last visited Mar. 25, 2026).

[23] Government of India, Ministry of Home Affairs, Lok Sabha Unstarred Question No. 431, Cybercrime Targeting Senior Citizens (Dec. 2, 2025), https://www.mha.gov.in/MHA1/Par2017/pdfs/par2025-pdfs/LS02122025/431.pdf (last visited Mar. 25, 2026).

[24] Press Information Bureau, Ministry of Finance, Coordinated Efforts of Government, RBI and NPCI Accelerate Growth in Digital Payments, UPI Emerges as World's Largest Real-Time Retail Payment System, Accounting for 81% of Retail Digital Payments in FY 2024-25 (Mar. 16, 2026), https://www.pib.gov.in/PressReleasePage.aspx?PRID=2240723 (last visited Mar. 25, 2026).

The rural payment ecosystem is not limited to smartphones and bank apps. RBI's National Strategy for Financial Inclusion recognised that digital access in such spaces depends on BC outlets, micro-ATMs, stable connectivity, and local access points such as panchayat offices, fair price shops, and Common Service Centres. This makes rural digitisation partly assisted and partly delegated. That structure expands reach, but it also multiplies points of vulnerability. A user may rely on another person's device, explanation, or handling of the transaction, and that weakens informational control a little.[25]

Indian law captures these harms through cyber and penal provisions rather than one single definition of rural payment fraud. Section 66 of the Information Technology Act, 2000 addresses computer related offences. Section 66C punishes identity theft. Section 66D punishes cheating by personation by using a computer resource or communication device. These provisions map neatly onto common payment fraud patterns such as OTP extraction, fake customer-care calls, fraudulent KYC links, remote-access app misuse, and impersonation of bank or platform officials.[26]

The penal law now reinforces that cyber layer. Sections 318 and 319 of the Bharatiya Nyaya Sanhita, 2023 punish cheating and cheating by personation. In rural payment settings, deception often works through trust rather than technical hacking. The victim is induced to scan a QR code, approve a collect request, share credentials, or believe that the caller represents a bank, telecom company, or state authority. That is why digital fraud in these ecosystems is both a technology offence and a deception offence at once.[27]

The reporting architecture also shows how fast these harms travel. The Ministry of Home Affairs stated in March 2026 that the Citizen Financial Cyber Fraud Reporting and Management System had helped save more than Rs. 8,690 crore across more than 24.65

[25] Reserve Bank of India, National Strategy for Financial Inclusion 2019-2024 30-31, https://www.rbi.org.in/commonman/Upload/English/Content/PDFs/English_16042021.pdf (last visited Mar. 25, 2026).
[26] Information Technology Act, 2000, No. 21 of 2000, §§ 66, 66C, 66D (India).
[27] Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023, §§ 318, 319 (India).

lakh complaints, and that the 1930 helpline operates for immediate assistance in online cyber complaints. The legal significance is plain. Recovery depends on speed. A delayed complaint in a rural setting can turn a reversible transaction into an irretrievable loss.[28]

Rural Uttar Pradesh carries a sharper structural risk because digital ability remains uneven. MoSPI reported ICT skill penetration at 13.23 percent in rural India but only 7.94 percent in rural Uttar Pradesh. That gap helps explain why adoption may appear visible while comprehension remains shallow. The user may know the payment path but not the fraud script behind it. In such ecosystems, digital fraud is not merely an unlawful extraction of money. It becomes a recurring force that disturbs trust, slows lawful adoption, and pushes people back toward cash or assisted dependence.[29]

VI. STATUTORY AND REGULATORY FRAMEWORK

A. Information Technology Act, 2000

The Information Technology Act, 2000 does not merely punish cyber misconduct. It first makes the digital transaction legally intelligible. Sections 4 and 5 give legal recognition to electronic records and electronic signatures. Section 10A protects contracts formed through electronic means from being denied validity only because they were concluded electronically. Section 13 fixes the rules for dispatch and receipt of electronic records. For rural payment systems this matters greatly.

A UPI instruction, an app-based consent flow, an electronically acknowledged transfer, or a digital service contract must stand on a recognised legal base before fraud law can even begin to operate upon it.[30] The same Act then builds a layered liability structure for digital fraud. Section 43 creates a compensation-oriented regime for unauthorised access,

[28] Government of India, Ministry of Home Affairs, Lok Sabha Unstarred Question No. 4118, Cyber Crime in the Country (Mar. 17, 2026), https://www.mha.gov.in/MHA1/Par2017/pdfs/par2026-pdfs/LS17032026/4118.pdf (last visited Mar. 25, 2026).
[29] Ministry of Statistics & Programme Implementation, Sarvekshana, Combined Issue 118-119, https://www.mospi.gov.in/uploads/publications_reports/publications_reports1764138233782_4e47b439-d884-428e-a431-cf99c5346384_Sarvekshana_Final_-_118-119_Issue_%2824-11-2025%29_%282%29.pdf (last visited Mar. 25, 2026).
[30] Information Technology Act, No. 21 of 2000, §§ 4, 5, 10A, 13 (India).

copying or extraction of data, introduction of contaminants, disruption of systems, denial of access, and even charging services to another person's account by tampering or manipulation.

Section 66 converts the contraventions listed in section 43 into criminal offences where the conduct is done dishonestly or fraudulently. That architecture is especially important in payment fraud. Many rural scams involve credential capture, unauthorised access to a device or account, diversion of authentication, or manipulation of payment flows. The Act therefore recognises that digital fraud can injure both property and informational control, and that compensation and punishment may need to move together.[31]

Sections 66C and 66D are the real workhorses in this field. Section 66C criminalises dishonest or fraudulent use of another person's electronic signature, password, or unique identification feature. Section 66D criminalises cheating by personation through a communication device or computer resource. These provisions closely match fake KYC calls, cloned customer-care numbers, fraudulent collect requests, OTP extraction, and impersonation of banks or payment platforms.

Section 72A adds another protective layer where personal information obtained under a lawful contract is disclosed without consent in a manner likely to cause wrongful loss or wrongful gain. The Supreme Court in *Sharat Babu Digumarti v. Govt. of NCT of Delhi*, (2017) 2 S.C.C. 18, underscored the special position of the IT Act in matters that bear a direct nexus to electronic records. That logic remains important. It reminds investigators that digital fraud should not be reduced to a vague cheating complaint when cyber-specific ingredients are plainly present.[32]

B. Bharatiya Nyaya Sanhita, 2023

The Bharatiya Nyaya Sanhita, 2023 supplies the broader penal grammar of deception. Section 318 defines cheating in wide terms. It covers deception that fraudulently or

[31] Information Technology Act, No. 21 of 2000, §§ 43, 66 (India).
[32] Sharat Babu Digumarti v. Govt. of NCT of Delhi, (2017) 2 S.C.C. 18.

dishonestly induces delivery of property, consent to retention of property, or an act or omission likely to cause harm to body, mind, reputation, or property. The Explanation makes dishonest concealment of facts a form of deception. This is highly relevant to digital payment fraud. A fraudster may not always hack a device. Often he lies, suppresses the true nature of a transaction, misstates the purpose of a payment request, or conceals that a QR code will debit rather than credit funds. Section 318 is therefore well suited to the human layer of digital fraud where the victim is manipulated before the screen is touched.[33]

Section 319 sharpens that position by specifically punishing cheating by personation. It covers pretending to be another person, substituting one person for another, or representing that oneself or another is a person other than who one really is. The section expressly states that the personated identity may be real or imaginary. That is doctrinally useful in cyber-fraud cases. Rural victims are often deceived by fabricated bank officers, imagined government agents, false grievance executives, or cloned identities of known traders and relatives. Section 319 therefore works beside section 66D of the IT Act, but with a wider penal vocabulary and a higher punishment ceiling. The IT Act captures the technological medium. The BNS captures the deception as a classic criminal wrong. Taken together, they form the core statutory frame through which Indian law presently understands digital fraud in payment ecosystems.[34]

C. Digital Personal Data Protection Act, 2023 and DPDP Rules, 2025

The Digital Personal Data Protection Act, 2023 does not function as a classic anti-fraud penal statute. Its role is different. It tries to reduce the conditions in which digital fraud thrives. Sections 5 and 6 require notice and valid consent. The notice must identify the personal data and the purpose of processing. Consent must be free, specific, informed, unconditional, unambiguous, and tied to a clear affirmative act. The Act also requires that consent requests be presented in clear and plain language and in English or any

[33] Bharatiya Nyaya Sanhita, No. 45 of 2023, § 318 (India).
[34] Bharatiya Nyaya Sanhita, No. 45 of 2023, § 319 (India).

language in the Eighth Schedule. Section 8 places duties on the Data Fiduciary to ensure completeness and accuracy where necessary, build reasonable security safeguards, publish grievance redress details, and erase data when retention is no longer necessary. Sections 11, 12 and 13 give rights of access, correction, erasure and grievance redressal. For digital payment users this matters because fraud often begins much before the final unauthorised debit. It begins with weak notice, vague consent, careless retention, poor security, or absence of an accessible remedy.[35]

The Digital Personal Data Protection Rules, 2025 deepen that architecture, but their commencement structure is uneven and legally significant. The Gazette states that Rules 1, 2 and 17 to 21 came into force on publication, Rule 4 will come into force one year after publication, and Rules 3, 5 to 16, 22 and 23 will come into force eighteen months after publication. That means, as on 25 March 2026, many of the most operational provisions on notice detail, security safeguards, breach intimation and erasure timelines had not yet become operative. Still, the text of those rules is important because it reveals the regulatory direction. Rule 3 requires a notice that stands independently and gives, in clear and plain language, an itemised description of the personal data and the specified purpose. Rule 6 requires minimum safeguards such as encryption, masking, access controls, logging for detection and investigation of unauthorised access, and retention of relevant logs and personal data for one year for remediation and recurrence control. Rule 7 requires intimation of a personal data breach to each affected Data Principal and to the Board, with further detail generally within seventy-two hours. The framework is therefore visibly trust-oriented, though still partly deferred in operation.[36]

The Rules also give special attention to Consent Managers. Rule 4 read with the First Schedule sets registration conditions, while Part B of the First Schedule requires the Consent Manager to maintain a website or app as the primary access route, act in a fiduciary capacity toward the Data Principal, avoid conflict of interest with Data

[35] Digital Personal Data Protection Act, No. 22 of 2023, §§ 5, 6, 8, 11, 12, 13 (India).
[36] Digital Personal Data Protection Rules, 2025, rr. 1, 3, 6, 7 (India), Gazette of India, Extraordinary, Nov. 14, 2025.

Fiduciaries, maintain audit mechanisms, and publish transparency disclosures. This design matters in rural payment ecosystems where people frequently click first and understand later. A regulated consent architecture can reduce blind assent. Yet its practical value will depend on linguistic accessibility, local awareness, and whether such mechanisms actually become usable beyond metropolitan digital markets. On paper, the model is promising. In field conditions, much will depend on execution.[37]

D. CERT-In Directions, 2022

The CERT-In Directions of 28 April 2022 bring cyber incident response into the everyday legal environment of digital payments. Issued under section 70B(6) of the Information Technology Act, 2000, they require service providers, intermediaries, data centres, body corporate and government organisations to designate a Point of Contact, enable and securely maintain ICT system logs for a rolling period of 180 days, and furnish those logs to CERT-In when reporting an incident or when directed. The Directions also identify the kinds of incidents that must be reported. These expressly include identity theft, spoofing and phishing attacks, data breaches, data leaks, attacks affecting digital payment systems, attacks through malicious mobile applications, and fake mobile apps. For a payment ecosystem increasingly dependent on apps, APIs and remote authentication, these Directions provide the evidentiary backbone of detection and response.[38]

CERT-In's own FAQ document makes the compliance burden even sharper. It states that cyber incidents must be reported within six hours of noticing the incident or being informed about it. It also clarifies that the reporting obligation is not transferable, that any affected entity noticing the incident must report it, and that the Directions apply broadly to service providers offering services to users in India. The FAQ further explains that even if all details are not available within six hours, initial reporting must still be

[37] Digital Personal Data Protection Rules, 2025, r. 4 & First Sched. (India), Gazette of India, Extraordinary, Nov. 14, 2025.

[38] Indian Computer Emergency Response Team, Directions Relating to Information Security Practices, Procedure, Prevention, Response and Reporting of Cyber Incidents for Safe & Trusted Internet (Apr. 28, 2022), https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf (last visited Mar. 25, 2026).

made and additional information can follow later. For digital fraud law this has two consequences. First, speed becomes part of compliance, not merely good practice. Second, the Directions strengthen systemic cyber hygiene but do not themselves provide direct compensation to retail victims. They are institutional response tools. They help preserve evidence and improve mitigation, but they do not replace consumer remedy frameworks.[39]

E. RBI Consumer Protection Framework

RBI's consumer protection framework is the most immediate legal shield for victims of unauthorised digital banking transactions. The 6 July 2017 circular on limiting customer liability shifts the analysis away from a simple negligence narrative. It grants zero liability where the deficiency lies on the bank's side or where a third-party breach occurs and the customer reports within three working days. It creates limited liability where the fault lies elsewhere in the system and the customer reports within four to seven working days, subject to caps. It requires banks to provide customers with 24x7 reporting access through multiple channels. It mandates shadow reversal within ten working days from notification and places the burden of proving customer liability on the bank. This is not a minor procedural rule. It directly shapes legal confidence. A rural user who believes a wrongly debited sum may be quickly restored is far more likely to stay within digital systems.[40]

The 2019 framework on harmonisation of Turn Around Time for failed transactions addresses another trust problem. Not every harmful digital event is a fraud in the strict sense. Many are failed or incomplete transactions caused by technical breakdown, timeout, communication failure, non-credit to the beneficiary, or cash non-dispensation

[39] Indian Computer Emergency Response Team, FAQs on Cyber Security Directions of 28.04.2022 (May 2022), https://www.cert-in.org.in/PDF/FAQs_on_CyberSecurityDirections_May2022.pdf (last visited Mar. 25, 2026).

[40] Reserve Bank of India, Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions, RBI/2017-18/15, DBR.No.Leg.BC.78/09.07.005/2017-18 (July 6, 2017), https://www.rbi.org.in/commonman/english/scripts/Notification.aspx?Id=2336 (last visited Mar. 25, 2026).

despite account debit. RBI treated this inconsistency as a consumer confidence issue and prescribed a uniform outer limit for resolution along with a compensation framework. In rural settings, where connectivity failures and assisted transactions remain common, this framework matters as much as fraud law proper. Users rarely separate technical failure from deception in their lived experience. Repeated unresolved failures produce the same behavioural result. They drive withdrawal from digital channels.[41]

RBI's Online Dispute Resolution system for digital payments and the Reserve Bank - Integrated Ombudsman Scheme, 2021 complete the remedial chain. The ODR framework requires a simple complaint process using only necessary minimum details, automatic fetching of available transaction information, confidentiality-conscious design, unique reference numbers, and status tracking. The Integrated Ombudsman Scheme then provides cost-free redress for deficiency in service where the regulated entity does not resolve the complaint within thirty days or fails to satisfy the complainant. Its "One Nation One Ombudsman" model removes jurisdictional confusion and allows online complaint filing through a centralised mechanism. These features matter acutely for rural Uttar Pradesh. Where branch distance, language barriers, and procedural uncertainty already discourage claims, a fragmented complaint structure itself becomes part of the exclusion. RBI's consumer framework therefore does more than settle grievances. It tries, though imperfectly, to manufacture trust in digital payment law.[42]

[41] Reserve Bank of India, Harmonisation of Turn Around Time (TAT) and Customer Compensation for Failed Transactions Using Authorised Payment Systems, DPSS.CO.PD No.629/02.01.014/2019-20 (Sept. 20, 2019), https://www.rbi.org.in/CommonPerson/english/Scripts/Notification.aspx?Id=3074 (last visited Mar. 25, 2026).

[42] Reserve Bank of India, Online Dispute Resolution (ODR) System for Digital Payments, DPSS.CO.ODR.No.2785/01.03.001/2019-20 (Aug. 6, 2020), https://www.rbi.org.in/commonperson/english/scripts/Notification.aspx?Id=3194 (last visited Mar. 25, 2026); Reserve Bank of India, The Reserve Bank - Integrated Ombudsman Scheme, 2021 (Nov. 12, 2021), https://www.rbi.org.in/commonman/english/scripts/PressReleases.aspx?Id=3340 (last visited Mar. 25, 2026).

VII. PERCEIVED EASE OF USE: THE LEGAL MEANING OF "USABILITY"

Perceived ease of use, in the classic technology-acceptance sense, refers to the belief that using a system will require little effort. That idea is useful, but legally incomplete. A payment interface may look simple, load quickly, and reduce steps, yet still remain unsafe for a first-generation user who does not understand consent screens, debit authorisations, reversal options, or fraud warnings. In legal terms, usability must therefore include intelligibility of risk. A system is not truly usable merely because it is easy to touch. It must also be easy to understand, verify, and contest.[43]

Indian data protection law quietly supports this broader meaning. Sections 5 and 6 of the Digital Personal Data Protection Act, 2023 require notice and consent in clear and plain language. The consent request must be specific, informed, unambiguous, and linked to a clear affirmative act. Section 8 further requires reasonable security safeguards and an accessible grievance mechanism. These duties show that usability is not a decorative design value. It is tied to legal comprehension. If the user cannot understand what data is being taken, why it is being processed, or how to complain after misuse, the interface may be simple but the legal experience remains unusable.[44]

RBI's Online Dispute Resolution framework makes the same point from the side of consumer remedy. It requires that the process of lodging a dispute be simple and involve only the necessary minimum details, while the system should automatically fetch available transaction information where possible. This is a strong legal clue. Usability in financial regulation means low-friction redress. It includes the ability to complain without technical vocabulary, the ability to track the grievance, and the ability to seek correction before harm becomes final. A rural user often judges a digital system not by

[43] Fred D. Davis, Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology, 13 MIS Q. 319 (1989), https://aisel.aisnet.org/misq/vol13/iss3/6/ (last visited Mar. 25, 2026).
[44] Digital Personal Data Protection Act, No. 22 of 2023, §§ 5, 6, 8 (India).

how fast payment is made, but by whether help appears when something goes wrong. That is real usability, though law rarely names it so.[45]

The Reserve Bank's National Strategy for Financial Inclusion also links access with literacy, awareness, and appropriate consumer protection. That linkage matters for rural Uttar Pradesh. A platform may seem easy because it uses icons, QR codes, or local language prompts. But if the same user cannot distinguish a collect request from a receive request, or cannot identify a fake customer-care interaction, ease becomes deceptive. Legal usability must therefore combine interface simplicity, meaningful disclosure, fraud awareness, grievance access, and institutional trust. Without these features, perceived ease of use becomes a shallow metric. It measures surface comfort, not lawful participation.[46]

VIII. ACTUAL ADOPTION IN RURAL UTTAR PRADESH

Actual adoption in rural Uttar Pradesh cannot be read straight from national payment growth figures. The Union Government itself stated in March 2026 that retail digital payments touched 22,167.90 crore transactions in FY 2024-25 and that UPI accounted for 81 percent of retail digital payments, yet it also clarified that demographic or geographic segment-wise contribution data is not maintained. That admission is important. It means rural adoption in Uttar Pradesh must be inferred from narrower state and rural indicators, not from aggregate celebration of scale alone.[47]

[45] Reserve Bank of India, Online Dispute Resolution (ODR) System for Digital Payments, DPSS.CO.ODR.No.2785/01.03.001/2019-20 (Aug. 6, 2020), https://www.rbi.org.in/commonperson/english/scripts/Notification.aspx?Id=3194 (last visited Mar. 25, 2026).

[46] Reserve Bank of India, National Strategy for Financial Inclusion 2019-2024, https://www.rbi.org.in/commonman/Upload/English/Content/PDFs/English_16042021.pdf (last visited Mar. 25, 2026).

[47] Press Information Bureau, Ministry of Finance, Coordinated Efforts of Government, RBI and NPCI Accelerate Growth in Digital Payments, UPI Emerges as World's Largest Real-Time Retail Payment System, Accounting for 81% of Retail Digital Payments in FY 2024-25 (Mar. 16, 2026), https://www.pib.gov.in/PressReleasePage.aspx?PRID=2240723 (last visited Mar. 25, 2026).

Those narrower indicators show meaningful access, but not total absorption. The National Statistical Office's *Comprehensive Modular Survey: Telecom, 2025* reports that 85.1 percent of rural households in Uttar Pradesh had internet facility within household premises. Among such rural households, 98.7 percent accessed internet through mobile networks, while fixed or Wi-Fi use remained extremely low at 1.6 percent. This shows that the rural digital environment in Uttar Pradesh is mobile-first, low-cost, and technically reachable. It also shows that adoption rests on fragile infrastructure because access depends overwhelmingly on handheld connectivity rather than stable fixed networks.[48]

The same survey also reveals the unfinished side of that transition. In rural Uttar Pradesh, 14.9 percent of households still lacked internet facility within household premises. Among those households, 29.4 percent reported that they did not know how to use it, 26.1 percent said they did not need the internet, and 14.6 percent stated that available internet service did not correspond to household need. So non-adoption is not explained only by absence of signal. It emerges from skill deficit, weak perceived usefulness, and mismatch between available service and lived need. That gap is doctrinally relevant because formal availability does not by itself create real digital inclusion.[49]

User-level capability data makes the position still sharper. For Uttar Pradesh, the same 2025 survey shows that among persons aged 15 years and above, only 36.7 percent of rural persons reported the ability to perform online banking transactions. Even among the younger 15-29 cohort, the rural figure rises only to 54.8 percent. These numbers matter because actual adoption in payment ecosystems requires more than account ownership or device possession. It requires an independent capacity to execute a transaction,

[48] Ministry of Statistics & Programme Implementation, National Statistical Office, NSS Report No. 593, Comprehensive Modular Survey: Telecom, 2025 tbl. 14 (May 2025), https://www.mospi.gov.in/sites/default/files/publication_reports/CMST_report_m.pdf (last visited Mar. 25, 2026).

[49] Ministry of Statistics & Programme Implementation, National Statistical Office, NSS Report No. 593, Comprehensive Modular Survey: Telecom, 2025 tbl. 14.1 (May 2025), https://www.mospi.gov.in/sites/default/files/publication_reports/CMST_report_m.pdf (last visited Mar. 25, 2026).

interpret prompts, and complete the process without unsafe dependence on others. Rural adoption in Uttar Pradesh therefore appears present, but partial and uneven.[50]

That weakness becomes starker at the redress stage. Among persons aged 15 years and above in Uttar Pradesh, only 11.2 percent of rural persons reported the ability to complain about cybercrime or report cyber fraud on the cybercrime reporting portal. For rural women in the State, the figure stood at only 7.0 percent. This suggests that actual adoption remains institutionally thin. A person may be able to initiate payment, yet still lack the procedural confidence to seek remedy after fraud. In legal terms, that is not deep adoption. It is conditional participation under uncertainty.[51]

The threat environment in Uttar Pradesh also supports a cautious reading. The Ministry of Home Affairs reported that cybercrime cases registered in Uttar Pradesh rose from 8,829 in 2021 to 10,117 in 2022 and 10,794 in 2023. In the same broader enforcement ecosystem, the Citizen Financial Cyber Fraud Reporting and Management System had, by 31 January 2026, saved more than Rs. 8,690 crore across more than 24.65 lakh complaints. These figures do not prove that every complaint came from rural areas. But they do confirm that digital fraud risk is systemic and that quick reporting determines whether money is frozen or gone. In such an environment, actual adoption naturally becomes cautious, episodic, and sometimes reversible.[52]

[50] Ministry of Statistics & Programme Implementation, National Statistical Office, NSS Report No. 593, Comprehensive Modular Survey: Telecom, 2025 tbl. 12 (May 2025), https://www.mospi.gov.in/sites/default/files/publication_reports/CMST_report_m.pdf (last visited Mar. 25, 2026).
[51] Ministry of Statistics & Programme Implementation, National Statistical Office, NSS Report No. 593, Comprehensive Modular Survey: Telecom, 2025 tbl. 10 (May 2025), https://www.mospi.gov.in/sites/default/files/publication_reports/CMST_report_m.pdf (last visited Mar. 25, 2026).
[52] Government of India, Ministry of Home Affairs, Lok Sabha Unstarred Question No. 4118, Cyber Awareness (Mar. 17, 2026), https://www.mha.gov.in/MHA1/Par2017/pdfs/par2026-pdfs/LS17032026/4118.pdf (last visited Mar. 25, 2026).

IX. COMPARATIVE ANALYSIS: PERCEIVED EASE OF USE VERSUS ACTUAL ADOPTION

Perceived ease of use and actual adoption plainly diverge in rural Uttar Pradesh. Fred D. Davis described perceived ease of use as the degree to which a person believes that using a system would be free of effort. That concept captures interface simplicity. It does not capture legal confidence. Rural Uttar Pradesh already shows the gap. Internet access within rural households is high enough to suggest that many users can reach the digital system, yet the proportion of rural persons aged 15 years and above who report ability to perform online banking remains only 36.7 percent. Ease at the entry point does not become full adoption at the transaction point.[53]

The broader payments literature supports this distinction. The CPMI-World Bank framework on payment aspects of financial inclusion treats access and usage as separate concerns and stresses that transaction accounts must be safe, functional, and frequently usable if they are to advance inclusion. It also warns that fintech is not a panacea and that risks must be managed within wider country-level reforms. That approach fits rural Uttar Pradesh rather well. A QR code may appear easy. A voice prompt may feel friendly. Yet where fraud risk remains high, complaints remain hard, and users depend on assisted handling, adoption stays shallow. It looks present in statistics but fragile in practice.[54]

RBI's customer protection architecture points in the same direction. The 2017 framework on limiting liability in unauthorised electronic banking transactions and the 2020 Online Dispute Resolution system both assume that trust depends on remedy, traceability, and a simple complaint path. That is the legal heart of the comparison. Perceived ease of use concerns whether the system feels simple before the transaction. Actual adoption

[53] Fred D. Davis, Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology, 13 MIS Q. 319 (1989), https://aisel.aisnet.org/misq/vol13/iss3/6/ (last visited Mar. 25, 2026).

[54] Committee on Payments and Market Infrastructures & World Bank Group, Payment Aspects of Financial Inclusion in the Fintech Era (Apr. 2020), https://documents1.worldbank.org/curated/en/230091592918282222/pdf/Payment-Aspects-of-Financial-Inclusion-in-the-Fintech-Era.pdf (last visited Mar. 25, 2026).

concerns whether the user believes the law and the institution will still stand with him after the transaction. In rural Uttar Pradesh, fear of digital fraud widens that distance. It turns ease into hesitation, and usage into selective, low-confidence participation.[55]

X. DO EXISTING LAWS ADEQUATELY ADDRESS FEAR AS A BARRIER?

The present legal framework addresses digital fraud more effectively than it addresses fear of digital fraud. The Information Technology Act, 2000 criminalises identity theft, cheating by personation, unauthorised access, and related misconduct. The Bharatiya Nyaya Sanhita, 2023 reinforces deception and personation offences in broader penal terms. Yet both statutes are largely incident-facing. They react to fraud after the harmful act, or after the unlawful inducement has already worked. They do not directly regulate user confidence, interface clarity, transaction comprehension, or the psychological chill that keeps a lawful user outside the digital economy. In that sense, the legal system punishes fraud, but only partially governs fear.[56]

The strongest response to fear appears in RBI's consumer protection design rather than in core penal law. The framework on unauthorised electronic banking transactions shifts liability away from the customer in defined situations, requires 24x7 reporting channels, mandates shadow reversal within ten working days, and places the burden of proving customer liability on the bank. The ODR framework for digital payments further insists on a simple complaint path, minimal data entry, tracking, and faster resolution architecture. These measures matter because fear diminishes when remedy looks real and reachable. Still, the protection remains remedy-centric. It assumes that the customer can

[55] Reserve Bank of India, Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions, RBI/2017-18/15, DBR.No.Leg.BC.78/09.07.005/2017-18 (July 6, 2017), https://www.rbi.org.in/commonman/english/scripts/Notification.aspx?Id=2336 (last visited Mar. 25, 2026).

[56] Information Technology Act, No. 21 of 2000, §§ 43, 66, 66C, 66D (India); Bharatiya Nyaya Sanhita, No. 45 of 2023, §§ 318, 319 (India).

identify the wrong, report it quickly, and navigate the complaint chain. In rural Uttar Pradesh that assumption is often too optimistic.[57]

The Digital Personal Data Protection Act, 2023 and the DPDP Rules, 2025 move closer to the conditions that generate fear. Clear notice, informed consent, reasonable security safeguards, grievance redress, and breach intimation all help reduce data-enabled fraud exposure. CERT-In's Directions also strengthen incident reporting discipline, logging, and systemic cyber hygiene. Yet these instruments remain institution-facing. They discipline entities. They do not sufficiently translate compliance into user-facing trust signals. A rural payment user rarely experiences "reasonable security safeguards" as a lived assurance unless the interface itself conveys risk in plain language and unless local remedy actually works. So the framework is normatively strong, but socially thin.[58]

The gap becomes sharper when one turns to the user's actual ability to seek protection. The National Statistical Office's 2025 telecom survey records that only 11.2 percent of rural persons in Uttar Pradesh aged 15 years and above reported the ability to complain about cybercrime or report cyber fraud on the cybercrime reporting portal. For rural women, the figure was only 7.0 percent. This is where the present laws begin to look inadequate. A right that cannot be operationalised by the affected population does not fully answer fear. It may exist in doctrine. It may even look sound on paper. But it does not yet produce legal confidence at the point of use.[59]

---

[57] Reserve Bank of India, Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions, RBI/2017-18/15, DBR.No.Leg.BC.78/09.07.005/2017-18 (July 6, 2017), https://www.rbi.org.in/commonman/english/scripts/Notification.aspx?Id=2336 (last visited Mar. 25, 2026).

[58] Digital Personal Data Protection Act, No. 22 of 2023, §§ 5, 6, 8, 13 (India); Digital Personal Data Protection Rules, 2025, rr. 3, 6, 7 (India); Indian Computer Emergency Response Team, Directions Relating to Information Security Practices, Procedure, Prevention, Response and Reporting of Cyber Incidents for Safe & Trusted Internet (Apr. 28, 2022), https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf (last visited Mar. 25, 2026).

[59] Ministry of Statistics & Programme Implementation, National Statistical Office, NSS Report No. 593, Comprehensive Modular Survey: Telecom, 2025 tbl. 10 (May 2025), https://www.mospi.gov.in/sites/default/files/publication_reports/CMST_report_m.pdf (last visited Mar. 25, 2026).

XI. RECOMMENDATIONS

The first reform must treat trust as a legal design obligation. RBI, NPCI, banks, and major payment intermediaries should be required to deploy plain-language, vernacular, transaction-stage disclosures for high-risk actions such as collect requests, device-binding changes, QR debit authorisations, new beneficiary additions, and remote-access permissions. A fraud warning buried in help pages is of little value. The warning should appear at the exact moment of legal and financial risk. This approach aligns with the DPDP Act's insistence on clear notice and informed consent, but it should be made more transaction-specific in payment regulation. Simplicity should no longer mean fewer words only. It should mean clearer consequences.[60]

The second reform must localise grievance redress. The 1930 helpline and the Citizen Financial Cyber Fraud Reporting and Management System already show that fast reporting can save money before it exits the system irretrievably. The Ministry of Home Affairs reported in March 2026 that the system had helped save more than Rs. 8,690 crore across more than 24.65 lakh complaints. That infrastructure should now be taken closer to the rural complainant. Common Service Centres, banking correspondents, panchayat digital service points, and district legal services institutions should be formally integrated into a first-mile cyber-fraud reporting protocol with standard forms, assisted complaint filing, and immediate escalation. Fear falls when the user knows exactly where to go in the first ten minutes after loss.[61]

The third reform must recognise structural asymmetry, not merely individual carelessness. Rural Uttar Pradesh remains mobile-first and uneven in digital skill. A significant share of non-connected rural households in the State either do not know how to use internet services or do not see a meaningful need for them. The same survey also shows that only 36.7 percent of rural persons aged 15 years and above reported the ability

[60] Digital Personal Data Protection Act, No. 22 of 2023, §§ 5, 6 (India).
[61] Government of India, Ministry of Home Affairs, Lok Sabha Unstarred Question No. 4118, Cyber Crime in the Country (Mar. 17, 2026), https://www.mha.gov.in/MHA1/Par2017/pdfs/par2026-pdfs/LS17032026/4118.pdf (last visited Mar. 25, 2026).

to perform online banking transactions. In such a setting, law should presume heightened vulnerability and insist on stronger duties for payment providers dealing with first-generation or assisted users. Safer defaults, delayed activation of certain high-risk features, verified support channels, and simplified reversal protocols would better reflect the real conditions of rural adoption.[62]

The fourth reform should place fear within the constitutional language of access and meaningful participation. In *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1, the Supreme Court tied informational privacy to dignity and autonomy. In *Anuradha Bhasin v. Union of India*, (2020) 3 S.C.C. 637, the Court recognised the importance of the internet as a medium through which protected activities are exercised. Read together, these decisions suggest that digital participation cannot be judged only by formal availability of a network or app. A citizen excluded by persistent fraud anxiety, opaque consent, and inaccessible remedy is not meaningfully included. The law should therefore move from mere anti-fraud enforcement to user-centred digital trust governance. That would answer fear more honestly, and more effectively.[63]

XII. CONCLUSION

The inquiry shows that rural digital adoption in Uttar Pradesh is real, but not yet settled. The stronger story is not absence of access. It is the weakness of confident use. The National Statistical Office's 2025 telecom survey records that 85.1 percent of rural households in Uttar Pradesh had internet facility within household premises, yet only 36.7 percent of rural persons aged 15 years and above reported the ability to perform online banking transactions, and only 11.2 percent reported the ability to complain about

[62] Ministry of Statistics & Programme Implementation, National Statistical Office, NSS Report No. 593, Comprehensive Modular Survey: Telecom, 2025 tbls. 12, 14.1 (May 2025), https://www.mospi.gov.in/sites/default/files/publication_reports/CMST_report_m.pdf (last visited Mar. 25, 2026).

[63] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1; Anuradha Bhasin v. Union of India, (2020) 3 S.C.C. 637.

cybercrime or report cyber fraud on the cybercrime portal. That contrast captures the paper's central finding. Access has spread faster than legal confidence.[64]

The legal order does respond to digital fraud, but it responds unevenly. The Information Technology Act, 2000 criminalises identity theft, personation, and computer-related misconduct, which gives Indian law a recognisable anti-fraud core. Even so, penal prohibition does not by itself remove fear from daily payment behaviour. Criminal law punishes the wrong after it occurs. It does not automatically make the user feel safe at the moment of clicking, scanning, authorising, or sharing data.[65]

The most practical confidence-building rules come from banking regulation. RBI's framework on unauthorised electronic banking transactions provides zero or limited customer liability in defined cases, requires round-the-clock reporting channels, and mandates shadow reversal within ten working days after notification. That framework matters because fear falls when remedy looks prompt and intelligible. Still, this protection works best for users who can detect the fraud early, report it fast, and navigate the complaint process. In rural settings, that remains a serious limitation, maybe the most serious one.[66]

The data-protection framework also points in the right direction. The Digital Personal Data Protection Act, 2023 and the 2025 Rules insist on clearer notice, consent architecture, security safeguards, and breach-related duties. These are not marginal compliance details. They attack the background conditions in which fraud grows, such as vague consent, poor security, and informational imbalance. Yet much of this framework still

[64] Ministry of Statistics & Programme Implementation, National Statistical Office, NSS Report No. 593, Comprehensive Modular Survey: Telecom, 2025 tbls. 10, 12, 14 (May 2025), https://www.mospi.gov.in/sites/default/files/publication_reports/CMST_report_m.pdf (last visited Mar. 25, 2026).

[65] Information Technology Act, No. 21 of 2000, §§ 66, 66C, 66D (India).

[66] Reserve Bank of India, Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions, RBI/2017-18/15, DBR.No.Leg.BC.78/09.07.005/2017-18 (July 6, 2017), https://www.rbi.org.in/commonman/english/scripts/Notification.aspx?Id=2336 (last visited Mar. 25, 2026).

speaks more clearly to regulated entities than to first-generation users. So the law has moved forward, but social trust has not moved at the same pace.[67]

The enforcement picture confirms why fear remains rational. The Ministry of Home Affairs reported in March 2026 that the Citizen Financial Cyber Fraud Reporting and Management System had helped save more than Rs. 8,690 crore across more than 24.65 lakh complaints. That figure shows two things at once. Digital fraud is not speculative. It is widespread. It also shows that speed of reporting often decides whether a user is protected or abandoned. For rural Uttar Pradesh, actual adoption therefore depends less on visual ease and more on whether the law can convert vulnerability into timely protection.[68]

A constitutional reading strengthens the same conclusion. In *Justice K.S. Puttaswamy (Retd.) v. Union of India*, the Supreme Court linked privacy with dignity, autonomy, and control over personal information. Rural digital inclusion must therefore be judged not only by the number of users onboarded, but by whether people can transact without coercive fear, opaque consent, or helplessness after fraud. Perceived ease of use is a shallow metric when legal trust is weak. Actual adoption begins where safety feels believable.[69]

XIII. BIBLIOGRAPHY

A. Books and Articles

1. Arjun Patwardhan, *Financial Inclusion in the Digital Age* (World Bank Group 2018).
2. Committee on Payments and Market Infrastructures & World Bank Group, *Payment Aspects of Financial Inclusion in the Fintech Era* (Apr. 2020).

[67] Digital Personal Data Protection Act, No. 22 of 2023, §§ 5, 6, 8 (India).
[68] Government of India, Ministry of Home Affairs, Lok Sabha Unstarred Question No. 4118, Cyber Crime in the Country (Mar. 17, 2026), https://www.mha.gov.in/MHA1/Par2017/pdfs/par2026-pdfs/LS17032026/4118.pdf (last visited Mar. 25, 2026).
[69] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1.

3. Fred D. Davis, Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology, 13 *MIS Quarterly* 319 (1989).

B. Cases

4. *Anuradha Bhasin v. Union of India*, (2020) 3 S.C.C. 637.
5. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1.
6. *Sharat Babu Digumarti v. Govt. of NCT of Delhi*, (2017) 2 S.C.C. 18.

C. Statutes, Rules and Regulatory Instruments

7. Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023 (India).
8. Digital Personal Data Protection Act, 2023, No. 22 of 2023 (India).
9. Digital Personal Data Protection Rules, 2025 (India).
10. Information Technology Act, 2000, No. 21 of 2000 (India).
11. Indian Computer Emergency Response Team, *Directions Relating to Information Security Practices, Procedure, Prevention, Response and Reporting of Cyber Incidents for Safe & Trusted Internet* (Apr. 28, 2022).
12. Indian Computer Emergency Response Team, *FAQs on Cyber Security Directions of 28.04.2022* (May 2022).
13. Reserve Bank of India, *Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions*, RBI/2017-18/15, DBR.No.Leg.BC.78/09.07.005/2017-18 (July 6, 2017).
14. Reserve Bank of India, *Harmonisation of Turn Around Time (TAT) and Customer Compensation for Failed Transactions Using Authorised Payment Systems*, DPSS.CO.PD No.629/02.01.014/2019-20 (Sept. 20, 2019).
15. Reserve Bank of India, *Online Dispute Resolution (ODR) System for Digital Payments*, DPSS.CO.ODR.No.2785/01.03.001/2019-20 (Aug. 6, 2020).

16. Reserve Bank of India, *The Reserve Bank - Integrated Ombudsman Scheme, 2021* (Nov. 12, 2021).

D. Reports, Government Publications and Official Sources

17. Government of India, Ministry of Home Affairs, Lok Sabha Unstarred Question No. 4118, *Cyber Crime in the Country* (Mar. 17, 2026).

18. Government of India, Ministry of Home Affairs, Lok Sabha Unstarred Question No. 431, *Cybercrime Targeting Senior Citizens* (Dec. 2, 2025).

19. Indian Cybercrime Coordination Centre, Ministry of Home Affairs, *National Cybercrime Reporting Portal (NCRP)*.

20. Ministry of Statistics & Programme Implementation, National Statistical Office, *NSS Report No. 593, Comprehensive Modular Survey: Telecom, 2025* (May 2025).

21. Ministry of Statistics & Programme Implementation, *Sarvekshana*, Combined Issue 118-119 (2025).

22. Press Information Bureau, Ministry of Finance, *Coordinated Efforts of Government, RBI and NPCI Accelerate Growth in Digital Payments, UPI Emerges as World's Largest Real-Time Retail Payment System, Accounting for 81% of Retail Digital Payments in FY 2024-25* (Mar. 16, 2026).

23. Reserve Bank of India, *National Strategy for Financial Inclusion 2019-2024*.