ISSN: ISSN: 2583-5149 | Vol-4, Issue-1 | July 2026

Cybersecurity Risks in UPI Transactions: Legal Issues and Regulatory Responses

Khushi Mogha

B.B.A. LL.B. and LL.M. (Corporate Law).

Abstract

The Unified Payments Interface (UPI) has reshaped retail payments in India, processing over eighteen billion transactions every month and contributing to more than four-fifths of the country's digital payment volume. This rapid adoption, however, has been accompanied by a parallel rise in cyber-enabled financial fraud, ranging from phishing and SIM-swap attacks to fake QR codes and social engineering scams. This paper examines the cybersecurity risks associated with UPI transactions and the legal and regulatory framework that has developed in response, including the Information Technology Act 2000, the Reserve Bank of India's customer liability circular of 2017, the Digital Personal Data Protection Act 2023, and the Integrated Ombudsman Scheme. Using a doctrinal and analytical method supported by secondary data drawn from RBI annual reports, Parliament responses, NCRB trends and recent judicial decisions, the paper finds that while the zero-liability framework offers strong protection on paper, weak enforcement, low awareness, and slow grievance redressal continue to leave a large share of victims uncompensated. The paper concludes with recommendations for strengthening real-time fraud detection, harmonizing banking and criminal law remedies, and improving victim-centric reporting mechanisms.

Keywords: UPI fraud, cybersecurity law, digital payments, RBI regulation, zero liability

1. Introduction

The Unified Payments Interface, developed by the National Payments Corporation of India (NPCI) and launched in 2016, allows instant transfer of money between bank accounts using a mobile phone. It has become the backbone of India's digital payments ecosystem, valued for its convenience, interoperability across banks, and absence of transaction charges for ordinary users. The scale of adoption is striking: UPI volumes crossed 185 billion transactions in the financial year 2024-25, a rise of nearly 42 per cent over the previous year.

This scale, however, has created a correspondingly large attack surface for cybercriminals. Fraudsters exploit the trust users place in instant payment systems through phishing links, fake customer care numbers, malicious QR codes, screen-sharing applications and SIM-swap techniques. Because UPI transactions are typically irreversible once authenticated, victims often have very little time to act before funds are moved out of reach through a chain of mule accounts. This combination of speed, scale and irreversibility makes UPI fraud a distinct legal and regulatory challenge, sitting at the intersection of banking law, cybercrime law, consumer protection law and data protection law.

This paper studies the nature of cybersecurity risks in UPI transactions, traces the legal and regulatory response in India, and evaluates how effectively the existing framework protects consumers, drawing on recent statistics and case law.

2. Historical Developments

The legal response to UPI-related cybersecurity risk has evolved in stages rather than through a single comprehensive statute.

- 2000 - The Information Technology Act, 2000 created India's first general framework for electronic transactions, digital signatures and cyber offences, later amended in 2008 to widen the scope of cybercrime provisions and introduce Section 43A on protection of sensitive personal data.

ISSN: 2583-5149 | Vol-4, issue-1| July 2026 | License (CC BY 4.0)

- 2016 - NPCI launched UPI, building on the Immediate Payment Service (IMPS) infrastructure and the Aadhaar-enabled payment ecosystem, rapidly expanding the digital payment footprint, particularly after the 2016 demonetisation drive.
- 2017 - The RBI issued its circular on "Customer Protection - Limiting Liability of Customers in Unauthorised Electronic Banking Transactions" (6 July 2017), introducing the zero-liability, limited-liability and full-liability framework that still governs UPI fraud disputes today.
- 2019-2021 - The Consumer Protection Act, 2019 and the RBI's Integrated Ombudsman Scheme, 2021 strengthened the redressal architecture available to digital payment users.
- 2023 - The Digital Personal Data Protection Act, 2023 introduced obligations on data fiduciaries, including banks and payment apps, to secure personal data and report breaches, indirectly strengthening UPI cybersecurity governance.
- 2024-2026 - In response to a sharp rise in fraud volumes, RBI and NPCI introduced the Central Payment Fraud Information Registry (CPFIR), MuleHunter.AI, mandatory cooling periods for new payees and SIM changes, and proposals for a Digital Payments Intelligence Platform for real-time, network-wide fraud signal sharing.

This trajectory shows a shift from a purely facilitative regulatory posture in the early UPI years towards an increasingly protective and risk-based approach as fraud volumes grew.

3. Key Terms

- Unified Payments Interface (UPI): A real-time payment system enabling inter-bank fund transfers through a mobile application using a Virtual Payment Address (VPA).
- Phishing: A deceptive practice of sending fraudulent communications, typically through SMS, email or messaging apps, designed to trick a user into revealing confidential banking credentials.
- SIM Swap Fraud: A technique by which a fraudster obtains a duplicate SIM card linked to a victim's registered mobile number to intercept one-time passwords (OTPs).

ISSN: 2583-5149 | Vol-4, issue-1| July 2026 |

- Mule Account: A bank account used by fraudsters, often opened in the name of an unsuspecting or complicit individual, to receive and quickly route away stolen funds.
- Zero Liability: The RBI rule under which a customer bears no financial loss for an unauthorised transaction reported within three working days, provided the loss did not arise from the customer's own negligence.
- Social Engineering: Psychological manipulation of a victim into voluntarily disclosing sensitive information or performing an action, such as approving a UPI collect request, that benefits the fraudster.

4. Literature Review

Existing commentary on UPI security and law can be grouped into three broad strands. The first strand consists of regulatory and government reports. The RBI's Annual Report for FY2024-25 records 13,516 digital payment fraud cases, accounting for 56.5 per cent of all reported banking frauds, with cumulative losses of about Rs 520 crore, while Parliament responses placed by the Finance Ministry show that domestic UPI fraud incidents rose by 85 per cent in FY2023-24 over the previous year. These official sources establish the scale of the problem but offer limited legal analysis.

The second strand is legal-practitioner commentary analyzing bank liability under the 2017 RBI circular, the Information Technology Act and the Consumer Protection Act. This literature generally agrees that liability turns on whether the bank or the customer was negligent, and that courts and consumer forums have increasingly placed a duty of care on banks to maintain secure systems and respond promptly to fraud complaints, while still penalizing customers who share OTPs or UPI PINs.

The third strand consists of survey-based and industry studies. A Local Circles survey of over 32,000 UPI users found that one in five households had experienced UPI fraud at least once in the preceding three years, and that 51 per cent of victims never filed any formal complaint, suggesting that official fraud statistics significantly understate the real scale of the problem. Industry trend reports similarly note that fraud tactics have shifted from simple phishing links towards more

ISSN: 2583-5149 | Vol-4, issue-1| July 2026 | License (CC BY 4.0)

sophisticated methods such as QR code swapping, fake UPI collect requests and deepfake voice phishing.

Taken together, this literature documents the scale of UPI fraud and the broad contours of bank liability, but pays comparatively little attention to how criminal law, banking regulation and data protection law interact in practice, or to why a large share of victims remains unprotected despite a formally strong zero-liability framework. This paper attempts to address that gap.

5. Research Gaps

- Limited integration of banking regulation, criminal law and data protection law in a single analytical framework specific to UPI.
- Sparse academic analysis of recent judicial and consumer forum decisions specifically dealing with UPI (as opposed to card or net-banking) fraud.
- Insufficient examination of why over half of UPI fraud victims do not pursue formal complaints despite the existence of the zero-liability rule.
- Limited assessment of the effectiveness of newer technological interventions such as MuleHunter.AI and the proposed Digital Payments Intelligence Platform.

6. Objectives of the Study

- To identify and classify the principal cybersecurity risks affecting UPI transactions in India.
- To examine the legal and regulatory framework governing UPI fraud, including statutory provisions, RBI circulars and recent case law.
- To assess the effectiveness of existing grievance redressal and liability allocation mechanisms using recent data.
- To recommend measures for strengthening the legal and regulatory response to UPI-related cyber fraud.

ISSN: 2583-5149 | Vol-4, issue-1| July 2026 | License (CC BY 4.0)

7. Scope and Limitations

The scope of this paper is confined to the Indian legal and regulatory framework governing UPI transactions, with particular focus on developments between 2017 and 2026. It addresses civil and regulatory liability questions, along with relevant criminal law provisions, but does not extend to a comparative study of payment systems in other jurisdictions, nor to the technical architecture of UPI's payment-switching infrastructure beyond what is necessary to understand the legal issues.

The study relies on secondary data, including RBI publications, Parliament responses, NCRB-based estimates and reported judicial decisions, rather than primary empirical research such as victim surveys conducted by the author. Some statistics, particularly state-wise and year-wise fraud projections, are drawn from third-party analyses of government data and may be subject to revision once complete official figures are published. The paper also does not cover purely technical cybersecurity solutions, such as cryptographic protocol design, except where they intersect with legal or regulatory obligations.

8. Materials and Methods

This study adopts a doctrinal and analytical research method. Primary legal sources examined include the Information Technology Act, 2000 (as amended), the Reserve Bank of India's 2017 circular on customer liability, the Consumer Protection Act, 2019, the RBI Integrated Ombudsman Scheme, 2021, and the Digital Personal Data Protection Act, 2023. Secondary sources include RBI Annual Reports for FY2024-25, responses furnished by the Ministry of Finance to the Lok Sabha and Rajya Sabha, NCRB-linked fraud trend analyses, NPCI statistical releases, and a recent industry survey on UPI fraud experience. Case law was identified through review of recent reported decisions of the Supreme Court of India, High Courts and Consumer Disputes Redressal Commissions dealing with unauthorized electronic transactions and bank liability. Data on fraud volumes and values were compiled into comparative tables and charts to illustrate trends over the period FY2022 to FY2026.

9. Results and Discussion

ISSN: 2583-5149 | Vol-4, issue-1| July 2026 | License (CC BY 4.0)

9.1 Scale and Trend of UPI Fraud

Reported UPI fraud rose sharply between FY2022 and FY2024, before showing early signs of moderation. Figure 1 sets out the value of UPI fraud reported in each financial year. The amount involved increased nearly fivefold between FY2022 and FY2024, reaching Rs 1,087 crore on 13.42 lakh reported incidents, the highest level recorded since UPI became mainstream. In FY2025, the reported amount declined to Rs 981 crore across 12.64 lakh incidents, and provisional data for FY2026 (up to November) shows Rs 805 crore across 10.64 lakh incidents, suggesting that recent regulatory and technological interventions may be having some restraining effect, even as absolute volumes remain high.

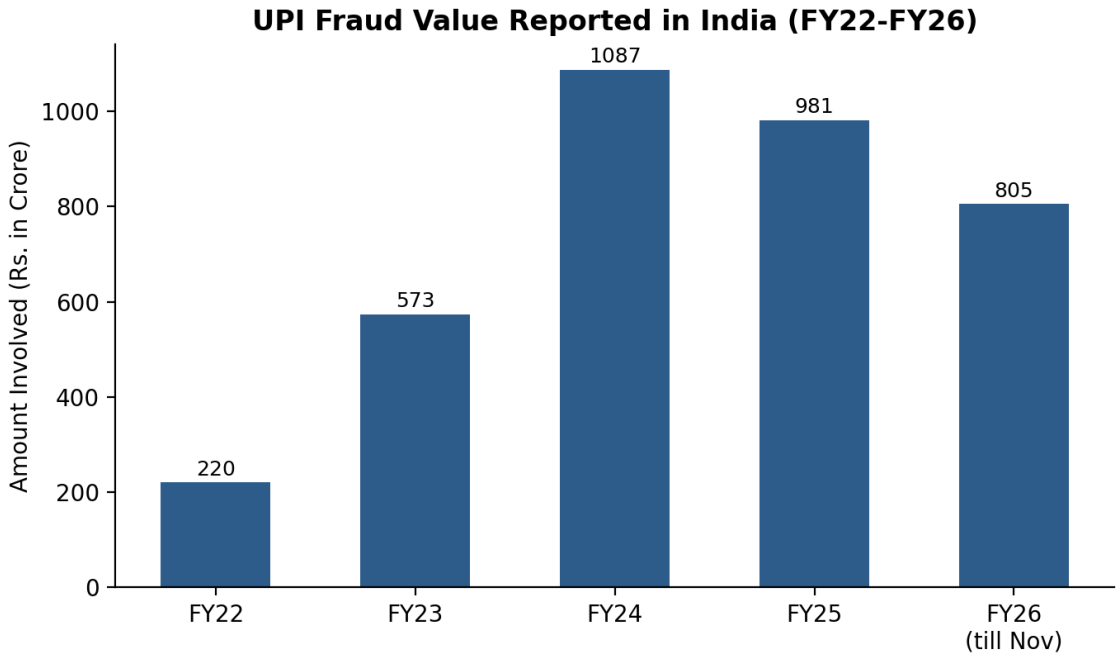

Figure 1: Value of UPI Fraud Reported in India, FY2022-FY2026 (Rs. in Crore). Source: Compiled from Finance Ministry responses to Parliament and RBI Annual Report data.

9.2 Geographic Concentration of Fraud

Fraud incidence is not evenly distributed across the country. Technology-dense states with high UPI penetration report a disproportionate share of cases. Figure 2 shows that Maharashtra, Karnataka and the Delhi-NCR region together account for over half of reported cases nationally,

ISSN: 2583-5149 | Vol-4, issue-1| July 2026 | License (CC BY 4.0)

broadly correlating with transaction volume, urban smartphone penetration and the concentration of technology-sector employees who are frequently targeted through professional-sounding social engineering scripts. Tier-2 cities show comparatively lower reported numbers, though this likely reflects weaker cyber-infrastructure and under-reporting rather than a genuinely lower incidence of fraud.

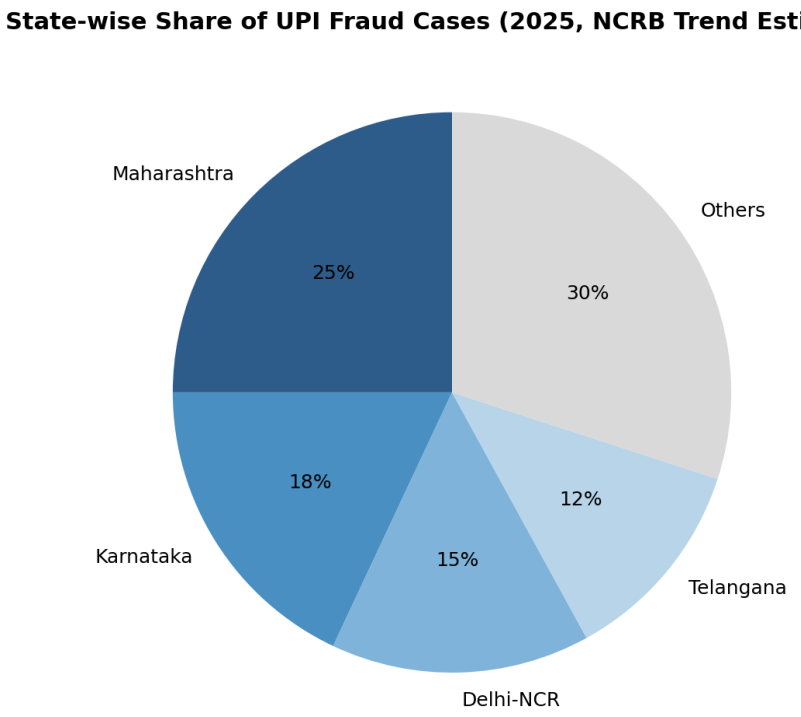

Figure 2: State-wise Share of UPI Fraud Cases, 2025 (NCRB-linked Trend Estimates). Source: Compiled from NCRB-based fraud trend analyses.

9.3 Grievance Redressal Performance

The zero-liability framework is only as effective as the speed and reliability of the redressal mechanism behind it. According to data placed before Parliament, only 22 per cent of fraud complaints were acted upon within seven days during April-September 2025, although the figure rose to 92 per cent within thirty days. More strikingly, only about 6 per cent of fraud chargebacks were actually recovered, underlining the limited value of post-facto remedies once funds have

Abhinavdhara
IJIIS- International Journal of Innovation in Indic Studies
ISSN: 2583-5149 | Vol-4, issue-1| July 2026 | License (CC BY 4.0)

moved through a chain of mule accounts. This is compounded by a significant reporting gap: the LocalCircles survey found that 51 per cent of UPI fraud victims never filed any formal complaint with their bank, the police or a regulator, meaning that official figures substantially understate the true scale of victimisation.

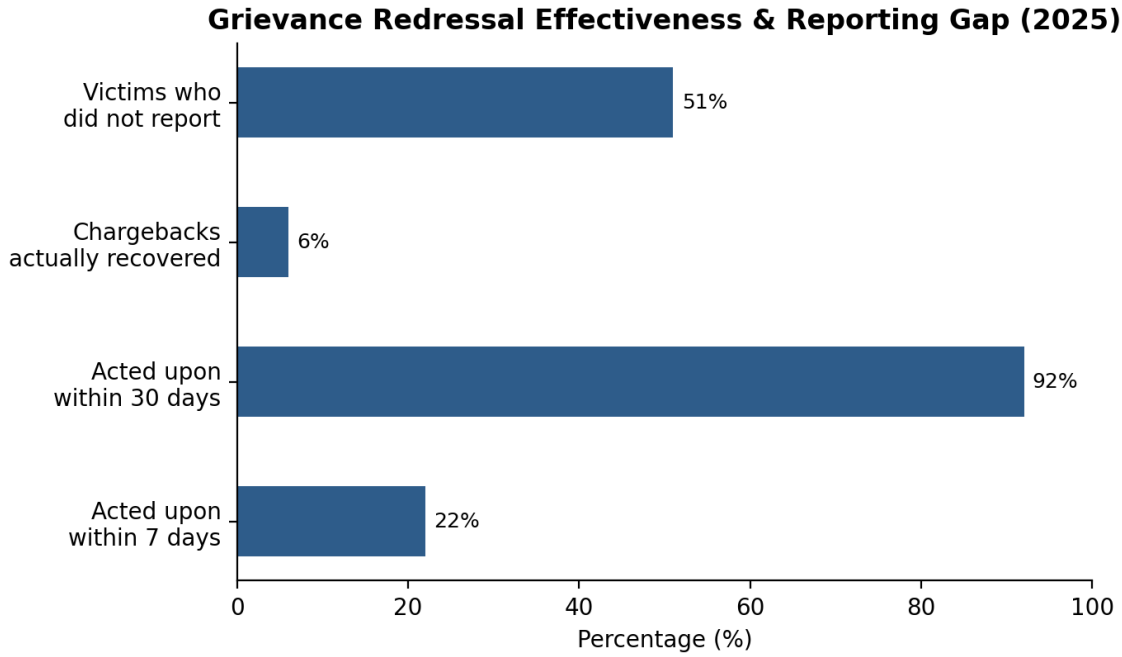

Figure 3: Grievance Redressal Effectiveness and Reporting Gap in UPI Fraud Cases, 2025. Source: Compiled from Parliament responses and LocalCircles survey data.

9.4 Judicial and Regulatory Trends

Recent decisions illustrate how courts and forums are applying the 2017 RBI circular. In a Special Leave Petition dismissed by the Supreme Court on 3 January 2025, the Court upheld concurrent findings that disputed bank transactions were unauthorised and fraudulent, and that no negligence could be attributed to the customer, applying clauses 8 and 9 of the RBI circular dated 6 July 2017 to affirm the customer's entitlement to relief. This reflects a broader trend in which appellate courts decline to interfere with factual findings on customer negligence once lower forums have carefully examined the evidence.

ISSN: 2583-5149 | Vol-4, issue-1| July 2026 | License (CC BY 4.0)

At the same time, forums have consistently held that voluntary disclosure of a UPI PIN or OTP amounts to contributory negligence that can defeat a zero-liability claim, as seen in disputes where banks successfully resisted refund claims after establishing that the customer had shared sensitive credentials with a fraudster posing as a bank official. Conversely, several District Consumer Disputes Redressal Commissions have ruled in favour of complainants where banks could not demonstrate that they had implemented adequate security measures or had responded to fraud complaints with reasonable promptness, reaffirming that banks owe a heightened duty of care as custodians of public money. Read together, these decisions show that liability outcomes are highly fact-sensitive, turning on rapid reporting, the presence or absence of credential-sharing, and the adequacy of the bank's own security and response systems.

9.5 Regulatory and Technological Responses

In response to rising fraud, regulators have layered technological and procedural safeguards onto the existing legal framework. These include device binding and two-factor PIN authentication, mandatory cooling periods for first-time payees and SIM changes, the Central Payment Fraud Information Registry for centralized fraud reporting, MuleHunter.AI for identifying mule accounts using AI and machine learning, dedicated banking-sector internet domains to curb phishing, and the proposed Digital Payments Intelligence Platform for real-time, network-level sharing of suspicious transaction data across banks and fintech companies. NPCI has also tightened application programming interface usage, capping high-frequency balance-enquiry and account-look-up requests that fraudsters had exploited for reconnaissance.

10. Findings

- UPI fraud value rose nearly fivefold between FY2022 and FY2024, before moderating in FY2025 and FY2026, suggesting that recent regulatory interventions are beginning to have a measurable effect, even though absolute volumes remain a serious concern.
- Fraud is geographically concentrated in technologically advanced, high-UPI-penetration states, indicating that awareness campaigns need to be targeted rather than uniform across the country.

ISSN: 2583-5149 | Vol-4, issue-1| July 2026 | License (CC BY 4.0)

- The formal zero-liability framework is undermined in practice by slow redressal, with a large share of complaints unresolved within seven days and very low chargeback recovery rates.
- Significant under-reporting, with about half of victims never filing a formal complaint, means that official statistics substantially understate the true prevalence of UPI fraud.
- Courts and consumer forums apply a fact-sensitive negligence standard, generally protecting customers who report promptly and did not share credentials, while denying relief where credential-sharing is established.
- Newer technological tools such as MuleHunter.AI and the proposed Digital Payments Intelligence Platform represent a shift towards proactive, network-level fraud prevention, but remain at an early stage of deployment.

11. Recommendations

- Simplify and unify the fraud-reporting process into a single-click mechanism linking the bank, NPCI, the National Cybercrime Reporting Portal and the RBI Ombudsman, reducing the friction that currently discourages victims from complaining.
- Mandate stricter time-bound action on initial fraud complaints, with clear escalation triggers, given that only 22 per cent of complaints are currently acted upon within seven days.
- Expand real-time, network-wide fraud-signal sharing under the proposed Digital Payments Intelligence Platform to all scheduled banks and major fintech players, not merely a pilot group.
- Strengthen mule-account detection and the speed of account freezing, since fund recovery falls sharply once money passes through multiple mule accounts.
- Conduct targeted, vernacular cybersecurity awareness campaigns in both high-fraud metropolitan regions and under-served Tier-2 and rural areas, addressing the very different risk profiles in each.

ISSN: 2583-5149 | Vol-4, issue-1| July 2026 |

- Clarify, through updated RBI guidance, the evidentiary standard for establishing customer negligence in UPI PIN and OTP disclosure cases, to reduce inconsistency across consumer forums.
- Align obligations under the Digital Personal Data Protection Act, 2023 with RBI cybersecurity directions to ensure consistent breach-reporting and data-security standards across banks and third-party UPI applications.

12. Conclusion

UPI has delivered enormous gains in financial inclusion and payment convenience, but its scale and speed have also made it an attractive target for increasingly sophisticated cybercriminals. India's legal and regulatory response, anchored in the Information Technology Act, the RBI's 2017 liability circular, consumer protection law and more recent data protection legislation, provides a reasonably comprehensive framework on paper. The evidence examined in this paper, however, shows a persistent gap between the formal strength of the zero-liability rule and its practical delivery: redressal remains slow, recovery rates are low, and a large share of victims never come forward at all. Closing this gap will require not new legislation so much as better enforcement, faster and more unified grievance redressal, wider deployment of real-time fraud-detection technology, and sustained public awareness, so that the legal protections already on the books translate into real outcomes for ordinary UPI users.

References

1. Reserve Bank of India, Annual Report 2024-25 (RBI, 2025).

2. Reserve Bank of India, Master Circular on Customer Protection - Limiting Liability of Customers in Unauthorized Electronic Banking Transactions, RBI/2017-18/15 (6 July 2017).

3. Ministry of Finance, Government of India, Reply to Unstarred Question on Domestic UPI Frauds, Lok Sabha/Rajya Sabha, Winter Session (25 November 2024).

4. Local Circles, Survey on UPI Fraud Experience Among Indian Households (June 2025).

ISSN: 2583-5149 | Vol-4, issue-1| July 2026 | License (CC BY 4.0)

5. Information Technology Act, 2000 (as amended by the Information Technology (Amendment) Act, 2008).

6. Digital Personal Data Protection Act, 2023 (No. 22 of 2023).

7. Consumer Protection Act, 2019 (No. 35 of 2019).

8. Special Leave Petition (Civil), Supreme Court of India, Order dated 3 January 2025 (unauthorized UPI/bank transaction liability).

ISSN: 2583-5149 | Vol-4, issue-1| July 2026 |