



INTERNATIONAL JOURNAL OF HUMAN RIGHTS LAW REVIEW

An International Open Access Double Blind Peer Reviewed, Referred Journal

Volume 5 | Issue 5 | 2026

Art. 28

Who Bears the Loss? Rethinking Consumer Liability in QR-Code Payment Fraud in India

Chandani Khatoon

Law Student,

4th Year, BA.LL.B.,

City Academy Law College, University of Lucknow

Recommended Citation

Chandani Khatoon, *Who Bears the Loss? Rethinking Consumer Liability in QR-Code Payment Fraud in India*, 5 IJHRLR 315-329 (2026).
Available at www.ijhrlr.in/current-issues/.

This Article is brought to you for free and open access by the International Journal of Human Rights Law Review by an authorized Lex Assisto & Co. administrator.

For more information,
please contact submission.ijhrlr@gmail.com

Who Bears the Loss? Rethinking Consumer Liability in QR-Code Payment Fraud in India

ABSTRACT

The rapid adoption of QR-code-based digital payments in India has created new forms of consumer vulnerability, particularly where fraudsters manipulate customers into voluntarily authorising transactions. The existing regulatory framework of the Reserve Bank of India (RBI) primarily addresses “unauthorised electronic banking transactions”, providing a liability framework where the customer has not authorised the transaction or where third-party fraud occurs without customer involvement. However, QR-code payment fraud presents a more complex situation: the customer may technically authenticate and authorise the payment, but such consent is obtained through deception, manipulation, or fraudulent misrepresentation. Consequently, the transaction is formally “authorised” while being substantively induced by fraud, creating uncertainty regarding who should ultimately bear the financial loss. This article critically examines whether the existing Indian framework adequately protects consumers in such circumstances and questions the continued reliance on formal authorisation as the basis for allocating liability. It argues that consumer liability should be reconsidered where consent is obtained through fraudulent inducement, particularly when the customer has exercised reasonable care. The article comparatively analyses approaches adopted in the United Kingdom and European Union to identify possible models for allocating losses between consumers, payment service providers, and other relevant actors. It proposes a more balanced, technology-neutral liability framework for QR-code payment fraud that recognises the distinction between genuine authorisation and fraudulently induced consent.

KEYWORDS

Consumer Liability, Consumer, Payment Fraud, NPCI, Digital Payment

INTRODUCTION

India has witnessed a rapid expansion of digital payments, particularly UPI- based transactions, making QR-code payments an

increasingly common part of everyday financial activity.¹ NPCI specifically identifies that deception based on QR code is a recognized digital- payment fraud and explains that fraudsters use social engineering techniques to victimize gullible users and sometimes, users may be persuaded to scan a QR code and enter their UPI PIN that actually authorizes a payment.² The problem becomes particularly significant from a legal perspective because the transaction may appear to have been authorized by the customer, even though the payment was induced through deception.³ Substantial numbers of complaints have been reported by The Government through the Citizens Financial Cyber Fraud Reporting and Management System (CFCFRMS).

Let's see how deeply UPI has become embedded in India's payment system through⁴ NPCI'S official UPI statistics that provide monthly transaction volume and value, that allows us to demonstrate the value of digital transactions in which QR- based payments operate for e.g. In August 2026, the volume (In Mn.) is 24,508.96 and the value (In Cr.) is 29,82,355.95 and last month i.e. in July 2026, volume (In Mn.) is 23,658.35 and value (In Cr.) 29,87,880.49. From these two months we can see rapid expansion of UPI and the increasing value of digital transactions increases importance of secure digital payments and this e.g. also shows why even a relatively small fraud rate can affect a large number of consumers.⁵ The RBI's Annual Report shows frauds have occurred predominantly in the category of digital payments. The increase in the amount involved in the total frauds reported during 2024-25 over 2023-24 was mainly due to removal of fraud classification in 122 cases amounting to ₹ 18,674 crore reported during previous financial years and reporting afresh during the current financial year after re-examination and ensuring compliance with the judgement of the Hon'ble Supreme Court dated March 27,2023. It increases the importance of digital-payment security as well as regulatory concerns surrounding digital transactions.⁶ Up to 31 October 2025, the Citizen Financial Cyber Fraud

¹ NPCI, "Fraud Awareness," available at: <https://www.npci.org.in/fraud-awareness> (last visited September 8, 2026).

² NPCI, UPI FAQs, available at: <https://www.npci.org.in/what-we-do/upi/faqs> (last visited September 8, 2026).

³ MoHA, GoI, Lok Sabha Unstarred Question No. 3913: Cyber Crime, 17 March 2026, available at: <https://www.mha.gov.in/MHA1/Par2017/pdfs/par2026-pdfs/LS17032026/3913.pdf> (last visited September 8, 2026).

⁴ NPCI, *Unified Payments Interface (UPI) Product Statistics*, available at: <https://www.npci.org.in/product/upi/product-statistics> (last visited Sep. 8, 2026).

⁵ RBI, *Annual Report 2024-25*, May 29, 2025, available at: <https://www.rbi.org.in/scripts/AnnualReportPublications.aspx?Id=1436> (last visited September 8, 2026).

⁶ MoHA, GoI, Lok Sabha Unstarred Question No. 5124: Cyber Secure Bharat, 24 March

Reporting and Management System had helped save more than ₹7,130 crore across more than 23.02 lakh complaints stated by a government of India parliamentary response.⁷

The electronic payment transactions and customer protection in India has already been governed by a regulatory framework, specifically through the directions of RBI concerning liability for unauthorized electronic transactions. The framework of RBI distinguishes circumstances involving bank negligence, customer negligence, and third-party breaches and shows customer liability differently in each of these circumstances. RBI introduces two types of liability for customers – 1. Zero Liability of a Customer (where wrong committed on the part of bank or a third-party breach) 2. Limited Liability of a Customer (Negligence by a customer or where there is a delay on part of customer in notifying the bank).⁸ Consumers have a formal grievance – redressal mechanism named The RBI ombudsman Scheme for customers for grievances including deficiency in services provided by regulated entities.⁹ The RBI integrates the three Ombudsman schemes- (i) the Banking Ombudsman Scheme, 2006, (ii) the Ombudsman Scheme for Non- Banking Financial Companies, 2018, and (iii) the Ombudsman Scheme for Digital Transactions, 2019 into the Reserve Bank – Integrated Ombudsman Scheme, 2021.¹⁰ For certain forms of digital deception, the IT Act, 2000 provides the criminal-law framework. Section 66D deals with cheating by personation using a computer resource. So, whether QR/UPI fraud is a banking dispute or not, it depends upon the facts, it can also have a criminal-law dimension.¹¹

The framework built by RBI only deals with the “unauthorized electronic banking transactions” where the wrong caused on the part

2026, available at: <https://www.mha.gov.in/MHA1/Par2017/pdfs/par2026-pdfs/LS24032026/5124.pdf>.

⁷ RBI, *Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions*, RBI/2017-18/15, July 6, 2017, available at: https://systemhealth.rbi.org.in/Scripts/NotificationUser.aspx_Id%3D11040%26Mode%3D0.html.

⁸ RBI, *RBI System Health – Complaint Management System*, available at: <https://systemhealth.rbi.org.in/cms.rbi.org.in/cms/indexpage.html>.

⁹ RBI, *Reserve Bank – Integrated Ombudsman Scheme, 2021*, Notification Ref. CEPD. PRD. No. S873/13.01.001/2021-22, November 12, 2021, available at: https://systemhealth.rbi.org.in/Scripts/NotificationUser.aspx_Id%3D12192%26Mode%3D0%281%29.html.

¹⁰ GoI, *The Information Technology Act, 2000*, Act No. 21 of 2000, available at: <https://www.indiacode.nic.in/handle/123456789/13683>.

¹¹ RBI, *Customer Protection – Limiting Liability of Customers of Co-operative Banks in Unauthorised Electronic Banking Transactions*, RBI/2017-18/109, DCBR.BPD.(PCB/RCB).Cir.No.06/12.05.001/2017-18, December 14, 2017, available at: <https://rbi.org.in/scripts/NotificationUser.aspx?Id=11188>.

of bank, customer, or third-party breach and have different consequences (liability) but the Actual problem is that deception induces transactions may be technically authorised by the customer.¹² In RBI's own report on consumer protection in digital payments recognises that digital payment security is an essential for wider adoption, and that the consumer trust and financial stability can undermine by the cybersecurity threats and it also states that consumer – protection concerns arising from digital payments.¹³ A 2025 academic study on “Authorised Push Payment Fraud” through which a victim is deceived into authorising fund transfers to a fraudster, often converged on normative questions of victim negligence and liability. Recent regulatory changes in the UK, which introduced a new mandatory reimbursement scheme for APPF victims while in India, the framework only deals with the “unauthorised electronic banking transactions” but the existing regulatory and academic discussions have addressed unauthorised electronic transactions and broader digital-payment fraud, comparatively less focused attention to be given to the liability implications of QR/UPI transactions in which the consumer is induced through deception to authenticate the payment personally”.

The objective behind this research paper is to examine the nature and emerging forms of QR-CODE/UPI payment fraud in India, specially frauds involving deception or social engineering. Also to analyse the existing framework governing consumer liability. To examine whether the existing framework adequately addresses transactions particularly where customers are deceived by making fake promises. To suggest practical legal and regulatory measures for improving consumer protection, liability allocation and grievance redressal in QR-code /UPI payment fraud cases.

LITERATURE REVIEW

The enormous growth of the use of digital payment system in India has generated academic as well as legal discussion relating to digital-payment fraud, consumer protection and allocation of liability. Existing scholarships have analyzed various dimensions of electronic payment fraud, related the nature, responsibilities and the legal protection available to customers. However the existing literature dealt these issues but from different perspectives, and it became necessary to examine the

¹² RBI, *Report on Currency and Finance 2023–24: India's Digital Revolution*, July 29, 2024, available at: <https://www.rbi.org.in/scripts/PublicationsView.aspx?id=22459> (last visited September 8, 2026).

¹³ Ngan, Jane, “The View from Below: Resistance and Change in Authorised Push Payment Fraud,” *Journal of Economic Criminology*, Vol. 9, 2025, Article 100166, available at: <https://www.sciencedirect.com/science/article/pii/S2949791425000429>

extent to which the exiting framework dealt frauds in which customers are induced through deception to authorize QR-code or UPI transactions.

Scholarships have largely explained how the law should distribute losses between the payment users and the financial institutions when fraudulent transactions occurred on electronic payment liability.¹⁴ The study of EU's Payment Services Directive 2 talks about the allocation of liability for unauthorized payment transactions and argues that three framework strengthen the consumer protection by reducing the payer's potential liability and requiring evidence of fraud or gross negligence before liability can be imposed. The study also highlights the importance of a transaction whether it is genuinely authorised or whether the customer consented to the transaction because liability differs.¹⁵ Similarly, bank-payment liability scholarships considered gross negligence as an important basis for deciding when a customer should bear a loss. In recent research conducted by Jo Braithwaite states that a significant role played by gross negligence in deciding bank's obligation to refund disputed payments and examines how customer conduct is evaluated within common-law and regulatory frameworks.¹⁶

A relevant body of scholarship has examined Authorized Push Payment (APP) Fraud, it's a way through which victims are deceived personally to transfer money from their accounts. Jo Braithwaite's analysis shows that traditional legal and regulatory rules may leave victims without compensation because the payment received the customer consent. The study examines the UK's mandatory reimbursement method and tells that although such regulatory intervention provides essential protection, gaps may remain because different categories of APP fraud may fall outside the available reimbursement mechanisms.¹⁷

¹⁴ teennot, Reinhard, "Reduced Payer's Liability for Unauthorized Payment Transactions under the Second Payment Services Directive (PSD2)," *Computer Law & Security Review*, Vol. 34, Issue 4, 2018, pp. 954-964, available at:

<https://www.sciencedirect.com/science/article/pii/S0267364918301924>

¹⁵ Braithwaite, Jo, "Gross Negligence in Bank Payments Law," *Oxford Journal of Legal Studies*, Vol. 46, Issue 2, 2026, pp. 308-337, available at:

<https://academic.oup.com/ojls/article/46/2/308/8454854>

¹⁶ Braithwaite, Jo, "'Authorized Push Payment' Bank Fraud: What Does an Effective Regulatory Response Look Like?," *Journal of Financial Regulation*, Vol. 10, Issue 2, 2024, pp. 174-193, available at:

<https://academic.oup.com/jfr/article/10/2/174/7716141>

¹⁷ RBI, *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, available at:

https://systemhealth.rbi.org.in/Scripts/NotificationUser.aspx_Id%3D11040%26Mode%3D0.htm

Although many scholarships have discussed about the electronic-payment liability and increasingly examines deception-induced authorized payments with the help of APPfraud, but a more focused examination is needed of these problems within India's QR-code and UPI ecosystem. The RBI regulatory framework deals with unauthorized electronic banking transactions, including circumstances involving banks' negligence, customers' negligence, and third-party breaches.¹⁸ However, QR-code fraud may involve a different factual situation where a customer personally interacts with the payment interface and makes it authentic after being deceived. NPCI itself warns customers about fraudulent QR-code scanning and also emphasizes that scanning a QR code and entering UPI PIN is only for making payment not for receiving. This creates an important question concerning the application of existing consumer-liability principles when the payment is technically authorized, but the consent of customers has been obtained through deception. Therefore, this study wants to examine whether India's existing legal and regulatory framework adequately addresses QR-code payment fraud, how responsibilities should be allocated among consumers and financial institutions, and whether clearer liability and grievance-redressal mechanisms are required.

RESEARCH METHODOLOGY

Research Design:

This study adopts a doctrinal, analytical, and comparative research design. It examines Indian laws and regulations governing QR-code/UPI payment fraud and analyses whether the existing framework adequately determines consumer liability where a payment is authorized after deception.

Sources of Data:

The study relies primarily on primary and secondary sources, including RBI circulars and directions, NPCI guidelines, the Information Technology Act, 2000, the Payment and Settlement Systems Act, 2007, judicial decisions, academic articles, government reports and credible empirical data. The RBI's customer-liability framework and NPCI's fraud-awareness material will be particularly relevant.

Scope:

¹⁸ RBI, "Prepaid Payment Instruments (PPIs)," Frequently Asked Questions, updated November 22, 2022, available at:

<https://rbi.org.in/Commonman/English/Scripts/FAQs.aspx?Id=2812>.

The research focuses on QR-code and UPI payment fraud in India, particularly social-engineering/deception-based transactions and the allocation of loss between consumers, banks and other payment-system participants. It also considers grievance-redress mechanisms and selected international approaches to Authorised Push Payment (APP) fraud.

Limitations:

The study is primarily desk-based and does not independently collect extensive primary data. The rapidly changing nature of digital-payment fraud and possible under-reporting of incidents may also limit the completeness of available data.

Analytical Framework:

The study firstly creates distinction between unauthorised transactions and deception-induced authorised transactions. After that It examines the existing liability rules, assess them on the basis of legal framework, consumer protection, institutional responsibility and effectiveness of remedies, and finally compare selected international approaches to identify possible reforms for India.

DISCUSSION AND ANALYSIS

Nature and Statistical Trends Of QR-Code/ UPI Fraud

We all are witnessed of Rapid growth of UPI but not witnessed only the growth but also on greater dependence on digital payments due to which India became a currency less country, from the above chart we can easily understand the growing nature of digital payments.¹⁹ From month to month we can understand the growth of UPI transactions due to which it also increases dependence on QR- based payments. We agree to the benefits of it but also we can't refuse its consequences also, one of its consequences is trends in digital-payment/ cyber fraud. From the Annual report of RBI we can under the trends in digital payment let's see their assessment and goals for 2025-2026 VI.61²⁰

An assessment of bank group-wise fraud cases over the last three years indicates that while private sector banks reported maximum

¹⁹ National Payments Corporation of India (NPCI), "UPI Product Statistics," *UPI Statistics*, available at: <https://www.npci.org.in/what-we-do/upi/product-statistics> (last visited September 8, 2026).

²⁰ RBI, "Regulation, Supervision and Financial Stability," *Annual Report 2024-25*, Chapter VI (May 29, 2025), available at: [RBI Annual Report 2024-25 – Chapter VI](#) (last visited September 8, 2026).

number of frauds, public sector banks continued to contribute maximum to the fraud amount ([Table VI.2](#)). Frauds have occurred predominantly in the category of digital payments (card/internet) in terms of number and primarily in the loan portfolio (advances) in terms of value ([Table VI.3](#)). While card/internet frauds contributed maximum to the number of frauds reported by private sector banks, frauds in public sector banks were mainly in loan portfolio. The increase in the amount involved in the total frauds reported during 2024-25 over 2023-24 was mainly due to removal of fraud classification in 122 cases amounting to ₹18,674 crore reported during previous financial years and reporting afresh during the current financial year after re-examination and ensuring compliance with the judgement of the Hon'ble Supreme Court dated March 27, 2023.

AGENDA FOR 2025-26

The Department has set out the following goals for 2025-26:

- Strengthening liquidity stress tests of SCBs by developing a cash flow analysis to ensure banks remain resilient during episodes of stress. The process would evaluate the potential impact of extreme but plausible scenarios on a bank's liquidity position, ensuring it can meet obligations even during crises. It would provide forward-looking perspective and assess the stability of banks' liquidity positions under adverse conditions. By identifying vulnerabilities and ensuring adequate liquidity buffers, stress testing would aid in ensuring resilience of banks, protect depositor interest and prevent systemic risks;
- Further strengthening the supervisory framework for PBs and SFBs;
- Digital services are important channels for servicing customers and ensuring resilience of the channels is of paramount importance. A framework will be devised with specific parameters for operational resilience of digital channels in REs;
- Issuance of guidelines on digital forensic readiness; and
- To provide a near-real-time view and analytics on the uptime of select digital services for the benefit of customers of banks, a dynamic online dashboard would be developed and the banks would be onboarded in a phased manner.

Reserve Bank of India (RBI) reviews the cyber security developments and threats on an ongoing basis in order to strengthen security of digital transactions and necessary measures are taken to strengthen the

cyber resilience of banks. RBI has advised the banks to establish robust procedures and processes to imbibe “security by design” principle in development of mobile banking applications including UPI applications, with appropriate testing mechanism through confidential circulars/advisories/alerts/caution advice.

A Suspect Registry of identifiers of cyber criminals has been launched by I4C on 10.09.2024 in collaboration with Banks/Financial Institutions. Till 31.01.2026, more than 23.05 lakh suspect identifier data received from Banks and 27.37 lakh Layer 1 mule accounts have been shared with the participating entities of Suspect Registry and declined transactions worth Rs. 9518.91 crores saved through CFCFRMS and the role of the 1930 helpline. However, it must be clear who bears the resulting losses.²¹

STATUTORY AND REGULATORY FRAMEWORK

According to the RBI Customer Protection Circular, 2017, the customer has zero liability where wrong has been done on the part of bank,²² customer has also zero liability in case of third-party breach but the transaction must be reported within 3 working days, and if the negligence has been made by customer then the customer may bear the loss until the transaction is reported to the bank and in some cases customer has also limited liability, see RBI framework mainly deals with the unauthorized electronic transactions. Therefore, in QR-code fraud, a victim may personally scan the QR code and after that enter the UPI PIN and they have been deceived has not been dealt by the existing rules and technically it seems authorised transaction but it is a deception-induced authorised payments. On the other side we can see that the circular also recognises the institutional responsibility on the part of bank such as the burden of proof is on bank and it doesn't mean that the bank is liable in every QR scam and the RBI provides a reimbursement mechanism for the loss.²³ IT Act, 2000 contains certain criminal provisions such as section 66C and section 66D but it can help to punish the fraudster but does not determine who bear the loss.²⁴

²¹ GoI, Lok Sabha, *Unstarred Question No. 5124*, 24 May 2026, available at: <https://sansad.in/lb>

²² RBI, *Customer Protection – Limiting Liability of Customers of Co-operative Banks in Unauthorised Electronic Banking Transactions*, RBI/2017-18/109, DCBR.BPD.(PCB/RCB). Cir. No.06/12.05.001/2017-18, December 14, 2017, available at: <https://www.rbi.org.in/commonman/English/scripts/Notification.aspx?Id=2623> (last visited September 8, 2026).

²³ *The Information Technology Act, 2000*, Act No. 21 of 2000, enacted on June 9, 2000, available at: <https://www.indiacode.nic.in/handle/123456789/15442> (last visited September 8, 2026).

²⁴ Reserve Bank of India, “Reserve Bank – Integrated Ombudsman Scheme, 2021,”

The remedy provided by the RBI Integrated Ombudsman Scheme, 2021 provides remedy for unauthorised transactions and provides remedy according to that so, the remedy is not completely effective.

JUDICIAL ANALYSIS

Reliance Retail Limited vs. Ashok Kumar & Ors. (2025)

The Delhi High Court issued an injunction to stop fraudsters from misusing Reliance's beauty brand trademark 'Tira'. The anonymous defendants (referred to as "Ashok Kumar") were executing financial scams by posing as Tira representatives on WhatsApp and phone calls. They tricked victims into making fraudulent UPI payments using fake identity proofs. To protect consumers and the brand's reputation, the court ordered telecom and financial intermediaries to block the fraudulent accounts and reveal the scammers' KYC details. This case shows that it's not about only customer and bank there are many more intermediaries who can be held responsible

State Bank of India vs. Rajesh Garg (2024)

In *State Bank of India vs. Rajesh Garg*,²⁵ the consumer commission held the bank liable for financial losses caused by unauthorized UPI transactions. The customer shared a QR code via WhatsApp to receive an OLX payment but was instead fraudulently debited ₹64,000. The bank refused to refund the money, arguing that the transactions required a PIN or OTP. However, the court ruled the customer was not negligent, as sharing a receiving scan code does not expose secure credentials, and ordered SBI to compensate for the loss.

Authorised Based Induced Payment

It is basically a way by which the victim is deceived by the fraudster to make the transaction with the consent of victim that makes it authorised even though it is not because the fraudster induced the victim and then received consent. NPCI itself warns that QR codes can be used for fraudulent purposes and that scanning a QR code and entering the UPI PIN is only for making the money not for receiving. This creates a legal issue who bears the loss if the transaction is technically authorised.

Comparative Analysis: India vs International App Fraud

Notification Ref. CEPD. PRD. No. S873/13.01.001/2021-22, November 12, 2021, available at: RBI Official Notification (last visited September 8, 2026).

²⁵ *Reliance Retail Limited v. Ashok Kumar & Ors.*, CS(COMM) 647/2025, Delhi High Court, Order dated July 7, 2025, available at: <https://indiankanoon.org/doc/19151040/> (last visited September 8, 2026).

India

RBI's Framework of India specifically focuses on "unauthorised electronic transactions and decides the liability according to the bank/customer fault and reporting time²⁶. The main issue arises when the customer personally authenticates a UPI/QR payment after being deceived and such transaction is considered authorised technically but now India recognising this problem more clearly and RBI has noted that most digital payment frauds are now APP Frauds, where payments are initiated by victims after being deceived. RBI has also proposed stronger safeguards, including delayed credit for certain payments, additional authentication for vulnerable users and customer-controlled payment limits.²⁷

United Kingdom

By making mandatory reimbursement for eligible APP scam victims, the UK has moved beyond the traditional distinction between authorised and unauthorised payments and this approach imposes more burden on payment-service providers rather than making responsible to the customer merely because the payment is technically authorised and India and others countries can take it as an example how to share responsibility for deception-based payment fraud.

European Union

- Under PSD2, liability of customer for unauthorised transactions is restricted, while strong customer authentication is used to improve payment security.
- However, the traditional framework has also faced difficulty in dealing with transactions that are technically authorised but obtained through deception. This makes the EU experience relevant to India's emerging APP-fraud problem.

POLICY AND REGULATORY DEVELOPMENT IN INDIA

A specifically important contemporary development is RBI'S March 2026 review instructions. The Reserve Bank of India (RBI) had issued the extant instructions on limiting liability of customers in unauthorised electronic banking transactions in 2017. However, in view of the rapid

²⁶ *State Bank of India v. Rajesh Garg*, First Appeal No. 208 of 2024, State Consumer Disputes Redressal Commission, U.T. Chandigarh, September 30, 2024, available at: <https://indiankanoon.org/doc/170728383/> (last visited September 8, 2026).

²⁷ RBI, *Discussion Paper: Exploring Safeguards in Digital Payments to Curb Frauds*, available at: <https://www.rbi.org.in/> (last visited September 8, 2026).

adoption of technology in the banking sector and payments systems, RBI reviewed its existing instructions. The revised instructions, including a compensation mechanism in case of small value fraudulent electronic banking transactions, have been issued for public / stakeholders' consultation on March 06, 2026. This revised instruction also demonstrates that regulatory framework also work on this issue.

CRITICAL EVALUATION OF LEGAL SHORTCOMINGS

1. First loophole is about authorisation – existing laws are only applicable on unauthorized transaction, but what happens if a victim is deceived by making fake promises.
2. In India there is lack of loss allocation- there may be uncertainty hoe loss should be divided.
3. Whenever we heard any case ralated to scam of digital payment then at prima facie we thought there must be customer negligence, but in every cases it is not true.
4. There is also a problem speed of recovery of amount.
5. There should be separation of criminal liability and loss-allocation liability.
6. The payment institutions should have greater responsibility to detect suspicious QR/UPI transactions than the customer.

In case of authorised but deception-induced Payments, the payment institutions should be grater responsible to detect suspicious QR/UPI transaction and it should bear the loss.

FINDINGS

- The RBI 2017 framework provides important protection for unauthorised electronic transactions, but QR-code fraud creates a difficult category where victims may personally authenticate payments after being deceived.²⁸
- Customer liability is strongly influenced by customer negligence and the time taken to report the fraud.
- QR-code fraud increasingly involves social engineering, making

²⁸ PIB, Government of India, *RBI Strengthens Framework on Unauthorised Electronic Banking Transactions*, March 24, 2026, available at: https://www.pib.gov.in/PressReleasePage.aspx?PRID=2244478&lang=1&re_g=3 (last visited September 8, 2026).

it difficult to determine whether the consumer or payment institution should bear the loss.

- Existing mechanisms for reporting and recovery provide protection, but instant UPI transactions can make recovery difficult once funds are transferred.
- The legal framework therefore needs greater clarity on “authorised but deception-induced” transactions.

RECOMMENDATIONS

- Recognise deception-induced authorised payments as a distinct category under the regulatory framework.
- Introduce a clear, risk-based liability model involving consumers, banks and payment intermediaries.
- Strengthen real-time fraud detection and warning systems for suspicious QR/UPI transactions.
- Improve coordination between banks, NPCI, payment apps and law-enforcement agencies for rapid freezing and recovery of fraudulent funds.
- Provide a simple and time-bound compensation/dispute-resolution mechanism for genuine victims.
- Increase consumer awareness that scanning a QR code and entering a UPI PIN authorises a payment, rather than receiving money.

CONCLUSION

QR-code payment fraud exposes a significant gap between the traditional concept of an “unauthorised transaction” and modern deception-based digital fraud.²⁹ Although India's regulatory framework provides meaningful protection to consumers, it does not completely resolve situations where victims themselves authenticate payments after being deceived. The solution should therefore move beyond simply asking “Who authorised the transaction?” and focus on who could reasonably have prevented the fraud and who should fairly bear the

²⁹ 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, available at: <https://www.rbi.org.in/commonman/Upload/English/Notification/PDFs/NOTI1506072017.PDF> (last visited September 8, 2026).

resulting loss. A clearer liability framework, stronger institutional safeguards and faster recovery mechanisms can make India's rapidly expanding digital -payment ecosystem more consumer-centric.