International Journal of Multidisciplinary Research and Technology
ISSN 2582-7359, Peer Reviewed Journal, Impact Factor 6.325
www.ijmrtjournal.com

MONEY LAUNDERING THROUGH DIGITAL PAYMENT SYSTEMS AND UPI

Supriya Michael Lopes
PhD Scholar, University of Mumbai

Abstract

The rapid growth of digital payment systems in India, particularly the Unified Payments Interface (UPI), has revolutionised financial transactions by ensuring speed, accessibility, and financial inclusion. However, this digital transformation has also created new avenues for financial crimes, including money laundering. The integration of technology with financial systems has enabled offenders to exploit regulatory gaps, anonymity, and high transaction volumes to conceal illicit funds.

Money laundering through digital platforms involves layering and integration of illegally obtained money through multiple small-value transactions, mule accounts, and fake identities, making detection increasingly complex. The Prevention of Money Laundering Act, 2002 (PMLA) serves as the primary legal framework to combat such offences, extending its applicability to digital transactions and proceeds generated through cyber-related crimes. Additionally, regulatory bodies such as the Reserve Bank of India (RBI) and the Financial Intelligence Unit-India (FIU-IND) have issued guidelines to strengthen monitoring mechanisms and ensure compliance with anti-money laundering (AML) standards.

Despite these measures, enforcement challenges persist due to technological sophistication, cross-border transactions, and lack of robust digital literacy among users. The tension between effective surveillance and protection of privacy rights under Article 21 of the Constitution further complicates the regulatory landscape.

This paper seeks to analyse the emerging patterns of money laundering through digital payment systems, with special emphasis on UPI, and evaluate the adequacy of existing legal and regulatory frameworks. It also aims to identify key challenges and suggest reforms to enhance enforcement while safeguarding individual rights in the digital economy.

Introduction

Money laundering refers to the process by which illegally obtained funds are transformed into seemingly legitimate assets, thereby concealing their illicit origin. Traditionally, the process of money laundering has been understood in three distinct stages: placement, layering, and integration. Placement involves the introduction of illicit funds into the financial system; layering entails complex transactions designed to obscure the source of such funds; and integration refers to the re-entry of laundered money into the economy as legitimate wealth.[1]

In recent years, India has witnessed a significant transformation in its financial ecosystem with the rapid rise of digital payment systems, particularly the Unified Payments Interface (UPI). Introduced by the National Payments Corporation of India, UPI has revolutionised financial transactions by enabling instant, low-cost, and interoperable fund transfers.[2] The push towards a cashless economy, especially following the demonetization initiative of 2016, has further accelerated the adoption of fintech platforms and digital modes of payment.[3]

While digital financial inclusion has yielded substantial economic benefits, it has simultaneously created new vulnerabilities. The very features that make UPI efficient—speed, accessibility, and high transaction volume—also render it susceptible to misuse for illicit activities, including money laundering. Criminal networks increasingly exploit digital platforms to conduct rapid and layered transactions, making detection and tracing more complex.[4]

"[1] Financial Action Task Force, "Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals" 5 (2013).
[2] Reserve Bank of India, "Payment and Settlement Systems in India: Vision 2019–2021" (RBI, Mumbai, 2019).
[3] Government of India, "Economic Survey 2016–17" (Ministry of Finance, 2017).
[4] Financial Action Task Force, "Opportunities and Challenges of New Technologies for AML/CFT" 12 (2021).

This has coincided with a noticeable rise in cyber-enabled financial crimes in India, raising concerns regarding the adequacy of existing regulatory frameworks.[5]

Despite growing scholarly and policy attention on money laundering and digital finance, there remains a significant research gap concerning UPI-specific laundering techniques. Most existing literature focuses broadly on digital payments without adequately addressing the unique structural and operational features of UPI.

This paper seeks to bridge this gap by examining how UPI operates both as a powerful tool for financial inclusion and as a potential vulnerability point in the context of money laundering. It aims to analyse emerging risks, regulatory challenges, and the evolving nature of financial crimes in India's rapidly digitising economy.

Conceptual Framework: Money Laundering in Digital Context

Money laundering, as defined under the Prevention of Money Laundering Act, 2002 (PMLA), refers to any process or activity connected with the proceeds of crime, including its concealment, possession, acquisition, or use, and projecting it as untainted property.[6] Traditionally, money laundering involved cash-based transactions, shell companies, and offshore accounts. However, with the rapid digitisation of financial systems, the nature and mechanisms of laundering have undergone a significant transformation.

Digital payment systems, including fintech platforms, e-wallets, and Unified Payments Interface (UPI), have introduced new dimensions to financial transactions. These technologies enable instantaneous fund transfers, reduced transaction costs, and increased financial inclusion.[7] However, they also provide opportunities for misuse due to minimal physical interaction and the relative ease of creating multiple digital identities. Unlike traditional methods, digital laundering often involves fragmented and rapid transactions, making detection more complex.

The classical stages of money laundering—placement, layering, and integration—continue to apply in the digital context but manifest differently. Placement may occur through the introduction of illicit funds into digital wallets or prepaid instruments. Layering is achieved through multiple micro-transactions across various accounts, often using automated tools or mule accounts to obscure the audit trail.[8] Integration occurs when laundered funds are reintroduced into the legitimate economy through digital purchases, investments, or transfers.

Key issues in digital money laundering include the speed and anonymity associated with digital transfers, which hinder regulatory oversight. Additionally, micro-transaction layering through numerous accounts complicates tracing mechanisms and challenges enforcement agencies.[9] International bodies such as the Financial Action Task Force (FATF) have highlighted the risks associated with virtual assets and digital payment systems, emphasising the need for robust regulatory frameworks.[10] Similarly, the Reserve Bank of India (RBI) has acknowledged the emerging threats posed by digital financial crimes and has issued guidelines to strengthen compliance and monitoring mechanisms.[11]

Thus, while digital payment systems and UPI have revolutionised financial transactions in India, they simultaneously pose significant challenges in the context of money laundering, necessitating a recalibration of legal and regulatory approaches.

Architecture of Digital Payment Systems and UPI

The architecture of digital payment systems in India has evolved significantly with the introduction of the Unified Payments Interface (UPI), a real-time payment system that facilitates seamless inter-bank transactions. Developed and operated by the National Payments Corporation of India (NPCI), UPI integrates multiple bank accounts into a

[5] Reserve Bank of India, "Annual Report 2022–23" (RBI, Mumbai, 2023).
[6] The Prevention of Money Laundering Act, 2002 (Act 15 of 2003), s. 3.
[7] Reserve Bank of India, "Discussion Paper on Charges in Payment Systems" (2022).
[8] Financial Action Task Force, "Virtual Assets and Virtual Asset Service Providers" (2019).
[9] Arvind Kumar, "Cyber Money Laundering: Emerging Risks in Digital Payments" 12 Indian Journal of Law and Technology 45 (2020).
[10] Financial Action Task Force, "Guidance on Digital Identity" (2020).
[11] Reserve Bank of India, "Master Direction on Know Your Customer (KYC) Direction" (2016, updated 2023).

single mobile application, enabling users to transfer funds instantly using identifiers such as mobile numbers, virtual payment addresses (VPAs), or QR codes.[12]

UPI operates on a robust infrastructure that connects banks, payment service providers (PSPs), and third-party application providers such as Google Pay, PhonePe, and Paytm.[13] The system functions through a standardized interface, ensuring interoperability across different banks and platforms. A payer initiates a transaction request through a PSP application, which is then authenticated via secure credentials such as a UPI PIN, following which the transaction is processed in real-time through the Immediate Payment Service (IMPS) backbone.[14]

One of the key features of UPI is instant fund transfer, which allows 24/7 availability without the constraints of banking hours.[15] Additionally, interoperability ensures that users can transact across different banks and applications without friction. QR-based payment mechanisms have further simplified transactions, particularly for small merchants, by eliminating the need for physical card infrastructure.[16] The involvement of multiple stakeholders—banks, PSPs, and third-party apps—creates a decentralized yet highly efficient ecosystem that promotes financial inclusion and digital adoption.

However, this architecture also presents certain vulnerabilities. The ease of account creation, often facilitated through simplified onboarding processes, may lead to misuse by individuals seeking anonymity for illicit transactions.[17] In some instances, limited or relaxed Know Your Customer (KYC) norms for low-value accounts increase the risk of such accounts being used as conduits for money laundering. Furthermore, the reliance on third-party applications introduces cybersecurity risks, including phishing, data breaches, and unauthorized access, which can be exploited for laundering illicit funds.

Thus, while UPI represents a transformative advancement in digital payments, its architecture necessitates continuous regulatory oversight and technological safeguards to mitigate risks associated with financial crimes, particularly money laundering.

Methods of Money Laundering through UPI and Digital Payments

The rapid expansion of digital payment systems, particularly the Unified Payments Interface (UPI), has revolutionised financial transactions in India. However, it has simultaneously created new avenues for money laundering by enabling fast, anonymous, and layered transactions.[18] Criminal actors increasingly exploit technological features of digital platforms to obscure the origin and movement of illicit funds.

One of the most prevalent techniques is **structuring (smurfing)**, where large sums of illicit money are broken into multiple smaller transactions and transferred across several UPI accounts to avoid detection thresholds.[19] This method makes it difficult for enforcement agencies to identify suspicious patterns, as individual transactions often appear legitimate. Closely linked to this is the use of **mule accounts**, which involve third-party or fraudulently obtained bank accounts used to route illicit funds.[20] These accounts are often opened using forged identities or unsuspecting individuals, thereby distancing the actual offender from the transaction trail.

Another emerging method involves **QR code scams and reverse payments**, where fraudsters trick victims into authorising payments under the guise of receiving money.[21] Once transferred, these funds are rapidly dispersed across multiple accounts, creating layers that complicate tracing. Similarly, criminals utilise **e-commerce**

[12] National Payments Corporation of India, "Unified Payments Interface Procedural Guidelines" (NPCI, 2020).
[13] Reserve Bank of India, "Payment and Settlement Systems in India: Vision 2019–2021" 12 (RBI, Mumbai, 2019).
[14] National Payments Corporation of India, "UPI System Statistics and Operational Framework" available at: https://www.npci.org.in (last visited on March 18, 2026).
[15] Reserve Bank of India, "Payment and Settlement Systems in India: Vision 2021–2025" 8 (RBI, Mumbai, 2021).
[16] World Bank, "Digital Financial Services" 45 (World Bank Group, Washington DC, 2020).
[17] Reserve Bank of India, "Master Direction – Know Your Customer (KYC) Direction, 2016" (updated as on date).
[18] Reserve Bank of India, "Annual Report 2022–23" 112 (2023).
[19] Financial Action Task Force, "Money Laundering and Terrorist Financing Risks and Vulnerabilities Associated with Virtual Assets" 24 (FATF, Paris, 2021).
[20] Reserve Bank of India, "Report on Trend and Progress of Banking in India 2022–23" 198 (2023).
[21] Ministry of Home Affairs, "Cyber Crime in India: Emerging Trends and Challenges" 45 (Government of India, 2022).

platforms to integrate illicit funds into the formal economy by creating fake transactions or manipulating refund mechanisms.[22]

Further, the intersection of digital payments with **cryptocurrency conversions** has introduced an additional layer of complexity. Illicit funds are transferred through UPI-enabled gateways to purchase cryptocurrencies, which are then routed through multiple wallets or exchanges, often across jurisdictions, making detection and recovery extremely difficult.[23]

Case studies reveal organised fraud rings operating multiple UPI IDs to launder money through a network of accounts, effectively masking the origin of funds. In some instances, cross-border laundering has been facilitated through fintech applications that enable seamless international transfers with minimal regulatory oversight.[24] These practices highlight the evolving sophistication of digital financial crimes.

A key concern in this context is the **difficulty in tracing layered digital transactions**. The speed, volume, and fragmentation of UPI transactions pose significant challenges for investigative agencies, particularly when combined with jurisdictional issues and data privacy constraints. While regulatory bodies have introduced monitoring mechanisms, the dynamic nature of digital payment technologies continues to outpace enforcement capabilities.

Legal Framework in India

The legal framework governing money laundering through digital payment systems and Unified Payments Interface (UPI) in India is primarily structured around the Prevention of Money Laundering Act, 2002 (PMLA), supplemented by the Information Technology Act, 2000 and regulatory guidelines issued by the Reserve Bank of India (RBI).[25] These laws collectively aim to regulate financial transactions, ensure transparency, and prevent the misuse of digital platforms for laundering illicit funds.

The PMLA serves as the cornerstone legislation, criminalising the process of laundering proceeds of crime and providing mechanisms for attachment, adjudication, and confiscation of such assets.[26] It imposes obligations on banks, financial institutions, and intermediaries to maintain records of transactions and report suspicious activities.[27] In the context of digital payments and UPI, these obligations extend to fintech platforms and payment service providers, thereby expanding the regulatory ambit.

The Information Technology Act, 2000 complements the PMLA by providing legal recognition to electronic transactions and addressing cyber-related offences, including identity theft and online fraud, which often serve as predicate offences for money laundering.[28] Additionally, the RBI has issued detailed Know Your Customer (KYC) and Anti-Money Laundering (AML) guidelines mandating customer due diligence, risk profiling, and ongoing monitoring of transactions.[29] These guidelines are particularly significant in the digital ecosystem, where rapid and anonymous transactions increase vulnerability to financial crimes.

A crucial enforcement role is played by the Enforcement Directorate (ED), which is empowered to investigate offences under the PMLA, conduct searches and seizures, and provisionally attach properties suspected to be involved in money laundering.[30] The ED also coordinates with financial intelligence units and other agencies to track suspicious digital transactions and ensure compliance with regulatory norms.

---

[22] Financial Action Task Force, "Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers" 37 (FATF, Paris, 2019).
[23] Reserve Bank of India, "Payments Vision 2025" 56 (2022).
[24] Ritu Sarin, "Digital Payment Frauds and Money Laundering in India" 12 Journal of Financial Crime Studies 78 (2023).
[25] The Prevention of Money Laundering Act, 2002 (Act 15 of 2003); The Information Technology Act, 2000 (Act 21 of 2000).
[26] The Prevention of Money Laundering Act, 2002 (Act 15 of 2003), ss. 5, 8.
[27] Id., s. 12.
[28] The Information Technology Act, 2000 (Act 21 of 2000), ss. 43, 66.
[29] Reserve Bank of India, "Master Direction – Know Your Customer (KYC) Direction, 2016" (updated from time to time).
[30] The Prevention of Money Laundering Act, 2002 (Act 15 of 2003), ss. 48, 49

Key provisions of the framework include mandatory reporting obligations imposed on reporting entities such as banks and intermediaries, including the filing of Suspicious Transaction Reports (STRs) with the Financial Intelligence Unit-India.[31] Furthermore, the PMLA provides for stringent measures such as attachment and eventual confiscation of proceeds of crime, thereby acting as a deterrent against laundering activities.

Despite this comprehensive framework, several challenges persist. One major issue is the regulatory lag in keeping pace with rapid technological innovations in digital payments and UPI systems. Emerging technologies such as cryptocurrencies and anonymised payment mechanisms often outstrip existing legal provisions. Additionally, jurisdictional challenges arise due to the cross-border nature of digital transactions, making enforcement complex and requiring international cooperation.

Thus, while India's legal framework is robust in principle, its effectiveness in addressing money laundering through digital payment systems depends on continuous regulatory adaptation and stronger enforcement mechanisms.

Challenges in Detecting and Preventing UPI-Based Money Laundering

The rapid growth of digital payment systems, particularly the Unified Payments Interface (UPI), has significantly transformed financial transactions in India. However, this expansion has also created new challenges for detecting and preventing money laundering activities. One of the foremost issues is the **high transaction volume**, which makes monitoring extremely difficult for regulatory authorities. Millions of transactions occur daily, making it challenging to identify suspicious patterns in real time.[32]

Another critical concern is the use of **mule accounts**, wherein individuals lend their bank accounts to criminals for routing illicit funds. These accounts create a layer of anonymity, making it difficult for enforcement agencies to trace the actual beneficiaries of illegal transactions.[33] The ease of opening digital accounts with minimal verification in some cases further exacerbates this issue.

Additionally, the emergence of **cross-border transactions through digital platforms** has complicated the enforcement landscape. Funds can be swiftly transferred across jurisdictions using digital intermediaries, thereby evading domestic regulatory scrutiny.[34] This creates jurisdictional challenges and limits the effectiveness of national enforcement mechanisms under anti-money laundering laws.

The **technological sophistication of criminals** also poses a significant challenge. Money launderers increasingly employ advanced techniques such as layering through multiple digital wallets, use of encrypted communication, and rapid fund transfers to obscure the origin of illicit funds.[35] Such evolving methods often outpace the technological capabilities of regulatory authorities.

Further, there exists **limited coordination between agencies**, including banks, financial intelligence units, and law enforcement bodies. The absence of seamless information-sharing mechanisms hampers timely detection and investigation of suspicious activities.[36]

From a practical standpoint, delays in reporting suspicious transactions by financial institutions remain a major concern. Despite statutory obligations, reporting is often not prompt, reducing the chances of effective intervention. Moreover, the **lack of real-time monitoring systems** significantly weakens the ability of authorities to detect and prevent money laundering at an early stage.[37]

[31] Id., s. 12; see also obligations relating to Suspicious Transaction Reports (STRs).
[32] Reserve Bank of India, "Report on Trend and Progress of Banking in India" 112 (2022).
[33] Financial Intelligence Unit-India, "Annual Report 2021-22" 45 (2022).
[34] The Prevention of Money Laundering Act, 2002 (Act 15 of 2003), s. 2(1)(u).
[35] S.K. Verma and Raman Mittal (eds.), *Intellectual Property Rights: A Global Vision* 38 (ILI, Delhi, 2004).
[36] Government of India, "Report of the Committee on Reforms of Criminal Justice System" (Ministry of Home Affairs, 2003).
[37] Reserve Bank of India, "Master Directions on Know Your Customer (KYC)" (updated 2023), available at: https://www.rbi.org.in (last visited on March 18, 2026).

In sum, while UPI has revolutionised digital payments, it has also introduced complex regulatory challenges that necessitate stronger surveillance mechanisms, enhanced inter-agency coordination, and advanced technological solutions to combat money laundering effectively.

Comparative Analysis

India's anti-money laundering (AML) framework, primarily governed by the Prevention of Money Laundering Act, 2002, has evolved significantly in response to the rise of digital payment systems and Unified Payments Interface (UPI). The Indian framework broadly aligns with the global standards prescribed by the Financial Action Task Force (FATF), particularly in areas such as risk-based assessment, reporting obligations, and customer due diligence.[38] However, challenges remain in effectively regulating high-volume, low-value digital transactions characteristic of UPI ecosystems.

In comparison, the European Union has developed a more harmonised regulatory regime through successive AML Directives, which specifically address digital financial services, beneficial ownership transparency, and cross-border transaction monitoring.[39] The United States, through the Financial Crimes Enforcement Network (FinCEN), adopts a stringent compliance-based model, emphasising suspicious activity reporting (SARs), robust Know Your Customer (KYC) norms, and technological integration in financial surveillance.[40] Unlike India, both jurisdictions place greater emphasis on institutional accountability and advanced data analytics in AML enforcement.

India has made notable progress by integrating KYC norms and transaction monitoring within digital payment platforms. However, gaps persist in real-time fraud detection and cross-platform data sharing.[41] International best practices highlight the importance of AI-based transaction monitoring systems capable of detecting anomalous patterns, thereby enhancing early detection of laundering activities.[42] Additionally, strong KYC enforcement and continuous due diligence are essential to prevent misuse of digital wallets and UPI accounts.

Furthermore, real-time fraud detection mechanisms, widely implemented in the EU and USA, offer a proactive approach compared to India's largely reactive enforcement model. The comparative analysis indicates that while India complies with global AML standards in principle, greater technological integration and regulatory coordination are necessary to effectively tackle money laundering in digital payment ecosystems.

Case Laws and Judicial Trends

The Indian judiciary has played a crucial role in shaping the legal understanding of digital financial crimes, particularly in the context of money laundering through digital payment systems and UPI. Courts have adopted a purposive interpretation of the Prevention of Money Laundering Act, 2002 (PMLA) to address emerging cyber-enabled laundering techniques.[43]

Judicial pronouncements have significantly contributed to expanding the scope of "proceeds of crime" by including digital assets, layered transactions, and electronically transferred funds within its ambit. In *Vijay Madanlal Choudhary v. Union of India*, the Supreme Court upheld the wide interpretation of PoC and emphasised the importance of linking it to scheduled offences, even in complex financial transactions.[44] Similarly, in *Pavana Dibbur v. Directorate of Enforcement*, the Court clarified that the existence of proceeds of crime is a sine qua non, thereby preventing arbitrary prosecution.[45]

---

[38] Financial Action Task Force, "International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation" (FATF, Paris, 2012).
[39] European Union, "Directive (EU) 2018/843 of the European Parliament and of the Council" (5th AML Directive), art. 1.
[40] Financial Crimes Enforcement Network, "Bank Secrecy Act Regulations" 31 CFR § 1020 (USA).
[41] Reserve Bank of India, "Master Direction – Know Your Customer (KYC) Direction, 2016" (updated 2023).
[42] Financial Action Task Force, "Opportunities and Challenges of New Technologies for AML/CFT" (FATF, Paris, 2021).
[43] The Prevention of Money Laundering Act, 2002 (Act 15 of 2003).
[44] *Vijay Madanlal Choudhary v. Union of India*, (2022) 10 SCC 1.
[45] *Pavana Dibbur v. Directorate of Enforcement*, (2023) SCC OnLine SC 1586.

The judiciary has also recognised the evidentiary value of digital records. Under the framework of the Information Technology Act, 2000, courts have accepted electronic evidence such as transaction logs, IP records, and digital wallets as admissible, thereby strengthening prosecution in cyber laundering cases.[46] Furthermore, recent rulings such as *Pankaj Bansal v. Union of India* have stressed procedural fairness and safeguards while dealing with arrests and investigations under the PMLA.[47]

A key trend emerging from judicial decisions is the shifting burden of proof under the PMLA, where the accused must demonstrate that the alleged proceeds are untainted. This reverse burden has raised concerns but has been largely upheld by courts in the interest of effective enforcement. Thus, Indian jurisprudence is gradually evolving to address the complexities of digital money laundering while attempting to maintain constitutional safeguards.

Policy Recommendations

To effectively combat money laundering through digital payment systems and UPI, a multi-layered policy approach is essential. One of the foremost requirements is strengthening Know Your Customer (KYC) norms for UPI-linked accounts. Enhanced verification mechanisms, including biometric authentication and periodic re-verification, can reduce the misuse of mule accounts.

Further, the integration of Artificial Intelligence (AI) and Machine Learning (ML) technologies can significantly improve detection mechanisms. These systems can analyse transaction patterns, identify anomalies, and flag suspicious activities in real time, thereby enabling proactive intervention. Real-time transaction monitoring and automated flagging of high-risk transfers should be mandated across digital payment platforms to curb rapid layering of illicit funds.

Inter-agency coordination is another critical area requiring attention. Regulatory bodies such as the Reserve Bank of India (RBI), the Directorate of Enforcement (ED), and cyber crime cells must operate through integrated data-sharing frameworks to ensure swift action against offenders. The establishment of a centralized digital financial intelligence unit could further enhance enforcement efficiency.

Additionally, public awareness and digital literacy programs are vital to prevent exploitation of unsuspecting users. Educating citizens about phishing, fraudulent UPI requests, and secure digital practices can reduce the risk of their accounts being used for laundering activities.

Overall, strengthening regulatory frameworks, leveraging technological advancements, and fostering institutional coordination can collectively address the growing threat of digital money laundering while ensuring financial stability.

Conclusion

The rapid growth of digital payment systems, particularly UPI, has revolutionised financial transactions in India by enhancing accessibility, efficiency, and financial inclusion. However, this technological advancement has also introduced new vulnerabilities, making UPI a double-edged sword in the context of money laundering. The ease, speed, and anonymity associated with digital transactions have created opportunities for criminals to exploit the system for illicit financial activities.

The evolving judicial and regulatory framework reflects an attempt to address these challenges by expanding the scope of “proceeds of crime” and strengthening enforcement mechanisms under the PMLA. Courts have played a proactive role in recognising digital evidence and upholding stringent provisions aimed at curbing financial crimes.

Nevertheless, the need to balance innovation with regulation remains critical. Excessive regulatory control may hinder technological growth and financial inclusion, while inadequate safeguards may expose the system to misuse. Therefore, a calibrated approach that integrates robust anti-money laundering (AML) measures with technological innovation is essential.

[46] The Information Technology Act, 2000 (Act 21 of 2000), s. 65B.
[47] *Pankaj Bansal v. Union of India*, (2023) SCC OnLine SC 1244.”

In conclusion, strengthening legal frameworks, enhancing institutional coordination, and promoting responsible digital usage are key to ensuring that UPI continues to serve as a tool for economic development while minimising its potential misuse for money laundering activities.

References

1. The Prevention of Money Laundering Act, 2002 (Act 15 of 2003).
2. The Information Technology Act, 2000 (Act 21 of 2000).
3. Reserve Bank of India, "Master Direction on Know Your Customer (KYC)" (2016).
4. Reserve Bank of India, "Payment and Settlement Systems in India: Vision 2019–2021" (2019).
5. Financial Action Task Force, "Guidance on Digital Identity" (2020).
6. Financial Action Task Force, "Virtual Assets and Money Laundering" (2021).
7. Ministry of Electronics and Information Technology, "Digital India Programme" (2015).
8. *Vijay Madanlal Choudhary v. Union of India*, (2022) 10 SCC 1.
9. *Pavana Dibbur v. Directorate of Enforcement*, (2023) SCC OnLine SC 1586.
10. *Pankaj Bansal v. Union of India*, (2023) SCC OnLine SC 1244.