Digital Forensics Challenges in UPI Fraud, QR Scam and Online Payment Theft— A Review

Bharadwaj M[1*], Rajarajeshwari BN[2]
[1,2]Asst. Professor Department of Digital Forensics, School of Sciences, Malla Reddy University, Hyderabad, Telangana, India.

*bharadwaj861@gmail.com

Abstract:

The rapid adoption of digital payments particularly India's Unified payments Interface (UPI) QR- based acceptance, and mobile wallets has produced dramatic convenience gains and equally rapid growth in fraud. This review synthesizes recent literature, incident reports and forensic practice to (1) characterize the main attack vectors used in UPI/QR/Online payment theft, (2) identify digital forensic challenges that impede investigation and prosecution, and (3) propose technical, procedural and policy recommendations to strengthen evidence collection, attribution and remediation. Key challenges include ephemeral evidence, encrypted and proprietary ecosystems, cross-jurisdictional/ multi-actor money-mules, weak endpoint hygiene, and gaps in logging and KYC. Recommended mitigations span better log retention and standardization, improvised endpoints and UX for fraud detection, stronger legal mandates for evidences preservation, and adoption of machine assisted triage and explainable ML for transaction level forensics. Major claims are supported by recent government, academic and industry reports.

Key Words: Authentication, encryption, endpoint security, evidence collection, fraud detection, KYC (Know your customer), Log retention, money mules.

1. Introduction

Digital payment volumes have exploded globally and in India in particular. UPI and QR-based payments now from a major share of retail transactions, prompting and QR based payments now form a major share of retail transactions, prompting parallel growth in fraud incidents and losses. Public sources and academic studies show rising numbers of UPI linked fraud reports and significant use of QR codes as phishing vectors and transaction diversion mechanisms These trends create an urgent need for forensic readiness and updated investigative technique [1].

This review focuses on forensic challenges arising from three overlapping phenomena: (a) UPI fraud (social engineering, unauthorized confirmations, SIM swap/ malware enabling payments), (b) QR scams (malicious/ replaced QR targets and dynamic QR manipulation) and (c) online payment theft (e-wallet compromise, credential reuse, card not present fraud).

D. R. Reddy et al. (eds.), *Proceedings of the First International Conference on Advances in Forensics and Cyber Technologies (ICFACT 2025)*, Advances in Computer Science Research 127,
https://doi.org/10.2991/978-94-6239-610-4_27

We synthesize recent literature, technical analyses and policy statements to identify shared and distinct forensic problems, current best practices, and research gaps [2].

2. Background & Attack Vectors

2.1 UPI ecosystem and common fraud techniques

UPI is an instant, app-centric payments rail; it relies on device bound app approvals, PINs and rapid settlement. Attackers exploit social engineering (caller-authenticity spoofing, fake customer-care), money-mule networks, malicious apps, and account takeover via SIM – swap or malware to initiate fraudulent UPI flows. Government and industry data document rising case counts and monetary loss concentrations in recent years [3].

2.2 QR code scams

QR codes are used at POS and online for convenient checkout. Threats include pasted/ replaced QR stickers that point to attacker accounts, dynamic QR manipulation, QR in phishing emails or images, and malicious QR generators that encode crafted payloads (URLs leading to phishing pages or apps). Research shows QR based phishing is a growing vector because scanners hide the destination, and users rarely verify URLs [4].

2.3 Online Payment theft beyond UPI/QR

This includes card not present fraud, credential stuffing against wallet accounts, SIM swap enabling OTP interception, and social engineering that convinces victims to approve transactions. Attackers use layering (mule accounts, rapid cashouts) to launder funds. Forensics must therefore trace split flows across multiple services and intermediaries [5]

3. Forensic lifecycle – Where the Problems Appear

Digital forensics for payment fraud covers: incident detection evidence preservation evidence collection analysis (linking transactions to actors/devices) attribution reporting/prosecution. At each stage, UPI/QR/online payment systems introduce unique friction [5]**.**

- Detection and triage: Real time transaction volumes are massive; many suspicious signals are subtle. Banks/PSPs may flag behaviour but noisy alerts make triage hard [7].
- Preservation: Settlement and reconciliation systems may over write logs or retain them for short legally defined periods, endpoints (user phones) are frequently factory-reset or over written soon after compromise [8].
- Acquisition: Much of the relevant data app logs, push notifications, device telemetry, network flows are proprietary and distributed across PSPs, UPI switches, app developers and telecoms. Obtaining coordinated snapshots requires legal processes and cooperation [9].
- Analysis: Mapping a transaction to a person is complicated by intermediaries, anonymized wallets, SIM swap forged KYC and money mule layering. Chain of custody for digital evidence is challenging when multiple organisations hold fragments [10].
- Attribution & prosecution: Technical evidence (IP, device IDs) can be spoofed or proxied through VPNs, botnets, or mule accounts, legal thresholds for proving intent and knowledge are high [11].

4. Specific Technical Challenges

4.1 Ephemerality & short retention windows

Payment rails and app backends sometimes retain detailed telemetry only for limited durations; banks routinely archive transactional logs and may not persist device level telemetry needed for forensic correlation. This leads to lost investigative leads if preservation requests are delayed [12].

4.2 Data fragmentation and provenance gaps

Relevant evidence is split, phone app logs, UPI switch records (NPCI), bank authorization logs, PSP internal fraud telemetry, telecom call/SMS records, and merchant POS camera feeds. Differences in timestamp formats, clock skew and missing correlation IDs complicate reconstruction of timeless and event causality [13].

4.3 Encrypted and proprietary data formats

Many mobile apps log in app specific binary formats or send telemetry encrypted end-to-end. Vendors may be unwilling or slow to decode and share due to privacy/competitive reasons or legal constraints. Additionally, end-to-end encryption prevents network capture from revealing payloads without device access [14].

4.4 Device and user privacy constraints

Regulatory privacy regimes and legitimate user rights limit the scope of data investigators can obtain without due process; balancing victim privacy against investigation needs is legally and ethically complex [15].

4.5 Social engineering's evidentiary thinness

When fraud succeeds via persuasion (victim enters PIN or approves a payment), technical artefacts proving coercion or deception are often lacking investigators must rely on transaction context, call/SMS metadata, and victim testimony. This makes legal proof of deception difficult [16].

4.6 Money mule networks and rapid cashouts

Criminal networks immediately withdraw or transfer funds across accounts and mini-wallets, often within hours, making recovery and forensic linkage harder. Layered transfers hinder tracing and increase demands on real time monitoring [17].

4.7 QR specific problems: invisibility of destination and dynamic content

Users scanning QR codes rarely see the underlying URL, many QR scanners do not display or warm about redirecting domains. Dynamic or codes (server-generated) can change targets between scan and settlement, and printed or stickers can be swapped or overlaid physically at merchant locations. These properties create gaps in forensic capture [18].

5. Methodologies & Tools for Investigation – Current Best Practices

5.1 Rapid Preservation/ Preservation orders

Investigators should issue immediate preservation requests to banks, PSPs, NPCI/UPI switch, app providers, and telecoms to freeze logs and transaction records, Template legal instruments and incident response playbooks reduce delay. Where legal frameworks allow, emergency preservation can secure volatile evidences [19].

5.2 Endpoint forensics and app log extraction

Forensic acquisition from Android/IOS devices 9app logs, notifications, keystore artifacts) is vital. Where possible, forensic images, secure app logs, and notification histories should be collected quickly by trained examiners to avoid tampering loss. Tools must handle encrypted app containers and parse proprietary formats [20].

5.3 Correlation across data silos using timeline reconstruction

Combine transaction logs (timestamps, UPI transaction IDs), app notifications, SMS logs, call records, merchant POS logs and CCTV to build a coherent timeline. Use normalized timestamps and correlation IDs to reconstruct the stepwise flow from social engineering to settlement [21].

5.4 Network and telemetry analysis

When devices access is possible, network captures (when available) and app telemetry can reveal redirection endpoints, C2 servers for malware, and payloads delivered via malicious QR destinations. Malware reverse engineering may be necessary for advanced attacks [22].

5.5 Intelligence on mule networks & clustering analytics

Graph analysis on transaction flows helps detect typical mule patterns: many small transfers to cluster accounts, rapid cascading withdrawals, or repeated use of specific gateway accounts. ML-assisted clustering can surface suspicious networks needing legal action [23].

5.6 User-centric evidence: Interviews and behavioural analysis

Victim interviews, combined with device inspection, help establish social engineering vectors. UX related evidence (screenshots, notification wording) can demonstrate deception. For prosecution, coupling testimonial evidence with technical logs strengthens cases [24].

6. Legal, Regulatory & Organizational Gaps

- **Preservation mandates & retention periods:** Existing retention windows for various logs (telecom, PSPs) can be short or ambiguous, making timely evidence collection essential. Clear regulatory minimum retention (with secure access controls) would aid investigations [25].
- **Inter-agency coordination:** Multi-jurisdictional flows (across states or countries) require joint investigation files and standardized evidence exchange protocols. India's cybercrime cells and bank ombudsman processes show good examples but need scaling [26].
- **Standards for telemetry/ forensic readiness**: There is no universal forensic logging standard for PSP apps and switches; adopting minimal forensic telemetry standards (correlation IDs, non-repudiation metadata, time stamp synchronization) would improve post incident analysis [27].

7. Case Examples (Illustrative & Recent)

- **Large scale UPI fraud trend (2023-2024):** Government and parliamentary data showed sharp increases in reported UPI fraud cases and monetary losses in FY2023-24, highlighting growing scale and the need for systemic measures [28].
- **QR phishing research findings:** Usability and security research shows that QR code phishing is effective because scanners and users rarely surface the underlying URL; experiments and field studies documented successful redirection attacks. These studies highlight how forensic collection must include the scanned QR image and app logs showing the resolved URL [29].

8. Recommendations

Technical & Operational

- **Forensic-ready logging standards:** Mandate minimal logging schema for PSPs and merchant POS; unique correlation IDs per transaction, device/app identifiers (hashed), UTC timestamps with NTP sync, and record of notification delivery and user interaction events. (Helps timeline reconstruction) [30].

- **Longer, tired retention policies:** Regulatory minimum retention (e.g., 1 year for high granularity logs, longer for transactions) with secure access for investigators under due process [31].
- **Rapid preservation workflows:** Standardized emergency preservation orders and inter-provider escalation channels to freeze volatile telemetry immediately upon credible report [32].
- **Endpoint centric defences:** Encourage apps to store encrypted, tamper-evident transaction receipts on device and to implement clearer UX (showing destination account and domain before approval) to reduce social engineering success [33].
- **Cross-industry intelligence sharing:** Real time sharing of mule account indicators, scam templates and QR hashes across banks, PSPs and law enforcement through a trusted, privacy preserving platform [34].

Research & Tools

- **Explainable ML for Transaction triage:** Invest in ML that can flag suspicious flows but produce human-interpretable reasons to assist investigators and courts [35].
- **Automated QR provenance tools:** Tools that can analyse scanned QR images, resolve final destinations and compare to know malicious QR patterns, preserving the scanned image for forensic use [36].
- **Graph based tracing platforms:** Develop tooling to automatically combine transaction, telecom, and KYC graph data to identify mule patterns rapidly [37].

Legal/Policy

- Stronger anti-mule regulations and expedited freezing: Faster mechanisms to freeze suspected mule accounts and compel PSPs to block rapid cascading transfers pending investigations [38].
- Public awareness & UX nudges: National campaigns and mandatory in app warnings for risky flows (e.g., "This looks like an typical QR payment, verify merchant identity"). Evidences suggest UX nudges reduce success of social engineering [39].

9. Future Research Directions

- Formalizing legal technical interfaces for cross broader evidence preservation in payment rails.
- Forensic methods to de-obfuscate layered mule networks while preserving privacy.
- Human factors research on QR scanning behaviour to design scanner UI that provides effective, non-intrusive warnings.
- Explainable transaction risk ML tailored for court admissibility [40].

10. Recommendations

Strengthening forensic readiness is essential for investigating UPI fraud, QR scams, and online payment theft. Banks, PSPs and payment apps should adopt standardized forensic log formats with synchronized timestamps, device metadata, and transaction identifiers. Logs must be retained for at least 12-18 months, and a rapid evidence preservation mechanism should be established through 24/7 coordination channels between financial institutions and law enforcement agencies. Mobile apps should also generate secure, tamper evidence transaction records and QR scan histories to support endpoint forensics [41].

For QR based scams, security enhancements are needed at both system and user levels. Digitally signed QR codes and tamper resistant merchant stickers can prevent physical QR replacement. Apps should display the full destination UPI ID or URL before a payment is confirmed, reducing the success of phishing attacks. Forensic tools must be capable of reducing

the success of phishing attacks. Forensic tools must be capable of reconstructing QR metadata, tracking redirect chains, and matching codes with known malicious repositories to aid investigations [42].

Improved fraud detection and analytics are crucial for early risk identification. Real time ML models should monitor unusual transaction patterns, device changes, and rapid fund movement while remaining explainable for legal admissibility. A centralized mule-account intelligence system, supported by graph analytics, can help identify suspicious fund flows and freeze high-risk accounts quickly, limiting financial losses. [43]

From a regulatory perspective, stronger KYC verification, AI-based identity checks, and tighter account monitoring are necessary to reduce the creation of mule accounts. Faster freezing and reversal mechanisms for suspected fraudulent transactions must be formalized. Collaborative frameworks between banks, NPCI, CERT-In, and cybercrime units should streamline data sharing, ensure proper chain-of-custody, and accelerate investigations. [44]

Finally, enhancing user protection and awareness is critical since many frauds exploit human behaviour. In-app warnings, QR-scan risk alerts, and short cooldown timers for high-risk transactions can mitigate social-engineering attacks. Large-scale awareness programs, especially in rural areas, should educate users about fake customer-care scams, fraudulent QR codes, and secure payment practices. Ongoing research on user behaviour, secure identity, and standardized payment forensics will further strengthen the digital payment ecosystem. [45]

11.Conclusion

UPI, QR codes, and online payments have transformed commerce but introduced new, fast-moving fraud modalities. Forensics for these crimes is hampered by ephemeral evidence, fragmented ownership of logs, privacy constraints, and social engineering heavy attacks. Progress requires a coordinated mix of technical standards (forensic ready telemetry), operational readiness (rapid preservation), improved endpoint UX, ML assisted triage that is explainable, and legal/regulatory updates to mandate retention and inter provider cooperation. Implementing these will materially improve investigator's ability to reconstruct events, attribute responsibility, and recover funds there by restoring trust in digital payments.

References:

[1] R. K. Gupta and S. Sharma, "Digital Forensics in UPI Payment Ecosystems: Challenges and Opportunities," IEEE Access, vol. 10, pp. 112345–112359, 2022.

[2] A. Singh and P. Kumar, "Security Issues in Unified Payments Interface (UPI)," in Proc. Int. Conf. Cyber Security and Digital Forensics, 2021, pp. 88–94.

[3] National Payments Corporation of India (NPCI), "UPI Security Guidelines," NPCI Technical Report, 2023.

[4] CERT-In, "Advisory on QR Code Scams and Payment Fraud," Govt. of India Advisory CIAD-2024-0008, 2024.

[5] S. Dey and V. K. Jain, "Mobile Payment Forensics: A Survey of Challenges," Forensic Sci. Int.: Digital Investigation, vol. 41, 2022.

[6] P. Aggarwal, "QR Code Security: A Comprehensive Review," IEEE Security & Privacy, vol. 20, no. 2, pp. 45–56, 2022.

[7] S. K. Tripathi and M. K. Rai, "An Analysis of Fraudulent Digital Payments in India," J. Info. Security and Applications, vol. 72, p. 103402, 2022.

[8] A. Mishra, "Social Engineering in UPI-Based Transactions," in Proc. IEEE Int. Conf. Human-Centric Computing, 2021, pp. 174–181.

[9] M. Goyal et al., "AI-Based Fraud Detection in Real-Time Payment Systems," IEEE Trans. Emerg. Topics Comp., vol. 11, no. 1, pp. 89–102, 2023.

[10] K. A. Patel, "UPI Fraud: Digital Trails and Forensic Gaps," Indian J. Cyber Criminology, vol. 5, no. 1, pp. 55–68, 2023.

[11] Reserve Bank of India, "Trend and Progress of Banking in India," RBI Report, 2023.

[12] S. Chatterjee, "Forensic Investigation of Wallet-Based Payment Theft," Digital Investigation, vol. 39, p. 301248, 2021.

[13] A. K. Prasad, "Risk Scoring Models for Online Payment Transactions," IEEE Access, vol. 9, pp. 144221–144232, 2021.

[14] ISO/IEC 27043:2015, "Incident Investigation Principles and Processes."

[15] P. R. Menon and N. Kulkarni, "QR-Code–Based Phishing Attacks: Analysis and Mitigation," Computers & Security, vol. 124, p. 103029, 2023.

[16] R. Basu and S. Mukherjee, "Digital Evidence Preservation in Mobile Payments," in Proc. Int. Conf. Digital Forensics, 2022, pp. 211–219.

[17] S. Bose, "SIM Swap Attacks in Mobile Banking: A Forensic Study," IEEE Trans. Info. Forensics and Security, vol. 18, pp. 2305–2318, 2023.

[18] S. Gupta, "UPI Transaction Fraud: Investigative Challenges," Cyber Forensics Rev., vol. 7, no. 2, pp. 14–25, 2022.

[19] J. Park et al., "Graph-Based Detection of Money Mule Networks," IEEE Trans. Big Data, vol. 9, no. 4, pp. 1024–1034, 2023.

[20] C. Wong et al., "Machine Learning for Financial Fraud Detection," ACM Compute. Surveys, vol. 55, no. 7, pp. 1–38, 2023.

[21] Interpol, "Global Financial Fraud Assessment Report," Interpol Technical Report, 2023.

[22] Europol, "Mobile Payment Fraud Threat Landscape," Europol Study, 2022.

[23] R. Kumar and I. Banerjee, "Digital KYC Vulnerabilities in FinTech Systems," IEEE Trans. Engineering Management, vol. 70, no. 2, 2023.

[24] A. Joseph, "Cybercrime in Mobile Payments in India," Int. J. Adv. Comp. Sci., vol. 13, no. 4, pp. 78–86, 2022.

[25] K. S. Rao, "Forensic Readiness in Financial Institutions: A Framework," J. Info. Assurance and Security, vol. 18, no. 3, pp. 112–123, 2022.

[26] M. S. Ali, “Digital Wallet Fraud Trends and Investigations,” IEEE Consumer Electronics Mag., vol. 12, no. 3, pp. 11–20, 2023.

[27] Hyper Verge, “KYC Anomaly Detection Using AI,” Technical Whitepaper, 2023.

[28] F. Khan and S. U. Ahmed, “Review on Mobile App Telemetry and Forensics,” IEEE Access, vol. 11, pp. 55301–55318, 2023.

[29] C. Li et al., “Explainable AI for Fraud Detection,” IEEE Trans. Neural Networks, vol. 34, no. 1, pp. 35–50, 2023.

[30] B. Das, “Digital Payments and Cybersecurity Risks in India,” Economic & Political Weekly, vol. 58, no. 12, pp. 45–52, 2023.

[31] S. Rao, “Crime Patterns in QR Scams,” Cyber Crime Journal, vol. 6, no. 2, pp. 19–31, 2023.

[32] McAfee, “QR Code Scams Report,” McAfee Security Report, 2022.

[33] A. Nayak and G. S. Reddy, “Detection of QR Manipulation Attacks,” in Proc. IEEE Int. Conf. Cyber Défense, 2021, pp. 201–208.

[34] J. Mathur, “Digital Forensics of Android Payment Applications,” Mobile Security Journal, vol. 11, no. 3, pp. 88–95, 2022.

[35] J. Patel, “Online Payment Theft Using Social Engineering,” Forensic Research Int., vol. 4, pp. 145–156, 2022.

[36] Google, “Safety Recommendations for UPI Apps,” Google Security Whitepaper, 2023.

[37] A. Banerjee, “Mobile Device Forensics in Financial Crime Investigations,” IEEE Security & Privacy, vol. 18, no. 5, pp. 54–62, 2020.

[38] K. Chen et al., “Behavioural Biometrics for Payment Authentication,” IEEE Trans. Mobile Computing, vol. 21, no. 5, pp. 1623–1636, 2022.

[39] IBM, “Financial Fraud in Digital Payment Systems,” IBM Cybersecurity Report, 2023.

[40] Deloitte, “Digital Payments Fraud Study – India,” Deloitte Insights, 2023.

[41] Accenture, “Mobile Payment Security and Fraud Trends,” Accenture Research, 2022.

[42] PwC, “India Digital Trust Survey,” PwC Report, 2023.

[43] M. Rao and P. Narang, “Chain-of-Custody Challenges in Cyber Forensics,” Int. J. Digital Evidence, vol. 17, no. 1, pp. 44–52, 2023.

[44] A. K. Sharma, “Building a Secure Digital Payment Ecosystem,” Int. J. Info. Security, vol. 22, pp. 439–452, 2023.

[45] D. S. Babu and S. R. Jadhav, “A Review of Fraudulent Techniques in UPI and Mobile Payments,” IEEE Conf. InfoSec, 2024, pp. 120–129.