Combating payments fraud in India's digital payments landscape

April 2025

pwc

Click to launch

Foreword

Dear readers,

I am delighted to present the latest edition of our newsletter to you.

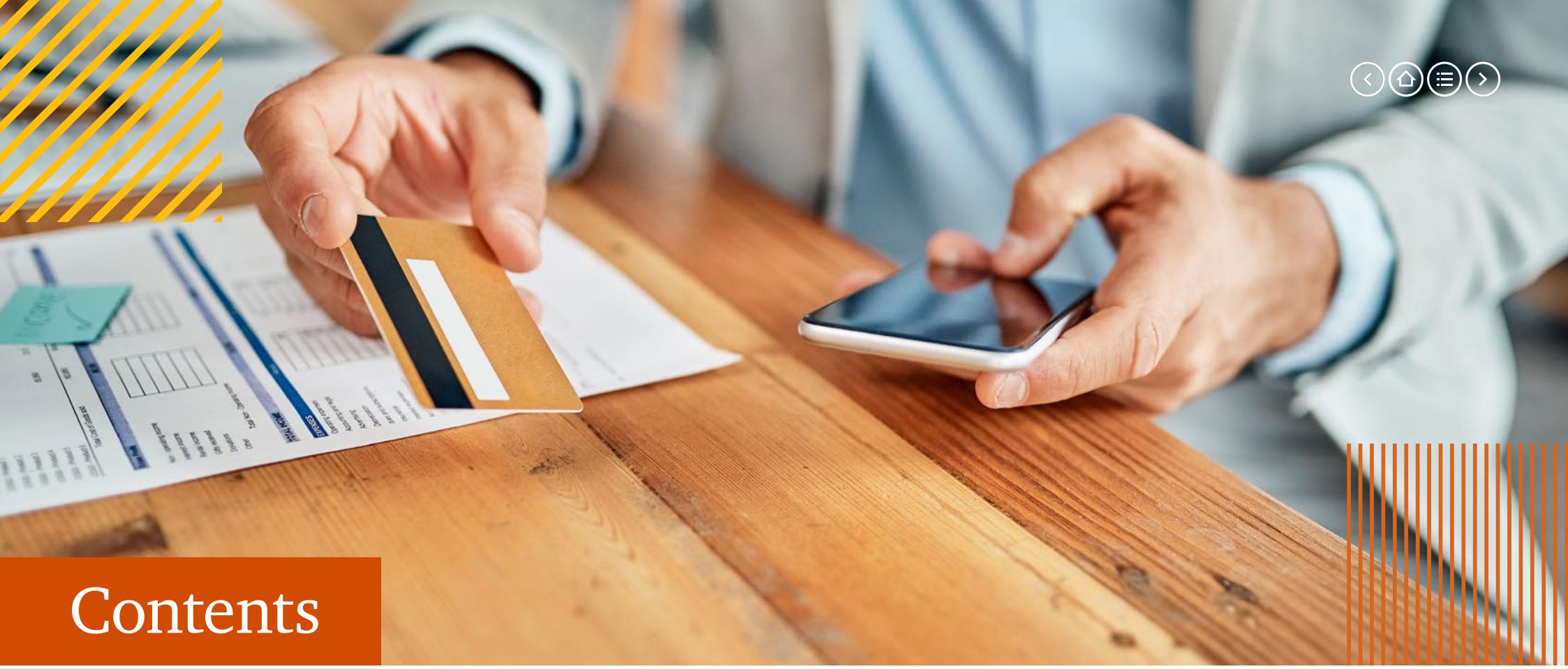
In this issue, we share our insights on payments fraud and the strategies for mitigation. We also delve into related areas, including advanced payments fraud tactics like social engineering and technical innovations, highlighting the urgent need for regulatory action and consumer education.

Additionally, we feature initiatives such as the Reserve Bank of India's proposed Digital Payments Intelligence Platform for real-time fraud prevention.

I hope you find this newsletter informative and insightful.

For further details or feedback, please write to:

vivek.belgavi@pwc.com or **mihir.gandhi@pwc.com**



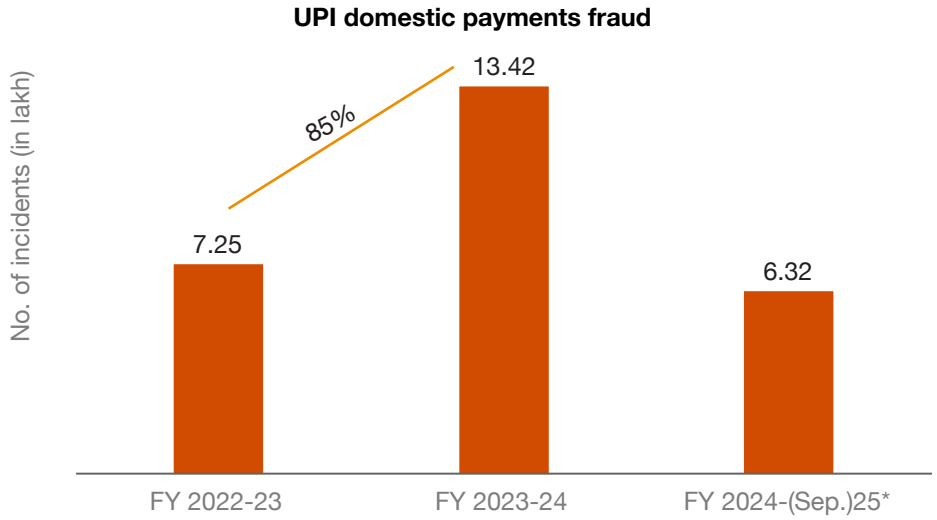
Contents

01 Introduction

In today's growing digital landscape, the security of financial assets should be prioritised above all else in order to ensure robust protection and reduce fraud.

As per the Economic Survey 2023-24, India accounts for 46% of all digital payments in the world. Of this, 80% is contributed by Unified Payments Interface (UPI), which is over 13,116 crore transactions in FY 23-24, and this is expected to grow to 43,900 crore by FY 28-29.[1] During FY 23-24, India witnessed over 15,900 crore digital transactions occurring nationwide.

Surge in UPI fraud cases



Source: Government of India, Department of Financial Services

The volume of UPI transactions surged from 92 crore in 2017-18 to 13,116 crore in 2023-24, growing at an average annual rate of 129%. Meanwhile, the total value of these transactions jumped from INR 1 lakh crore to INR 200 lakh crore over the same period, with an annual growth rate of 138%.[2]

However, this growth was accompanied by a rise in frauds as well. In 2022-23, UPI fraud losses amounted to INR 573 crore, making up 0.4% of the total transaction value. This increased to INR 1,087 crore in 2023-24, which is 0.5% of the transaction value. By September 2024, fraud value was INR 485 crore, which is 0.4% of the transaction value for that period, and has the potential to reach INR 970 crore by the end of the year if the trend continues.[3]

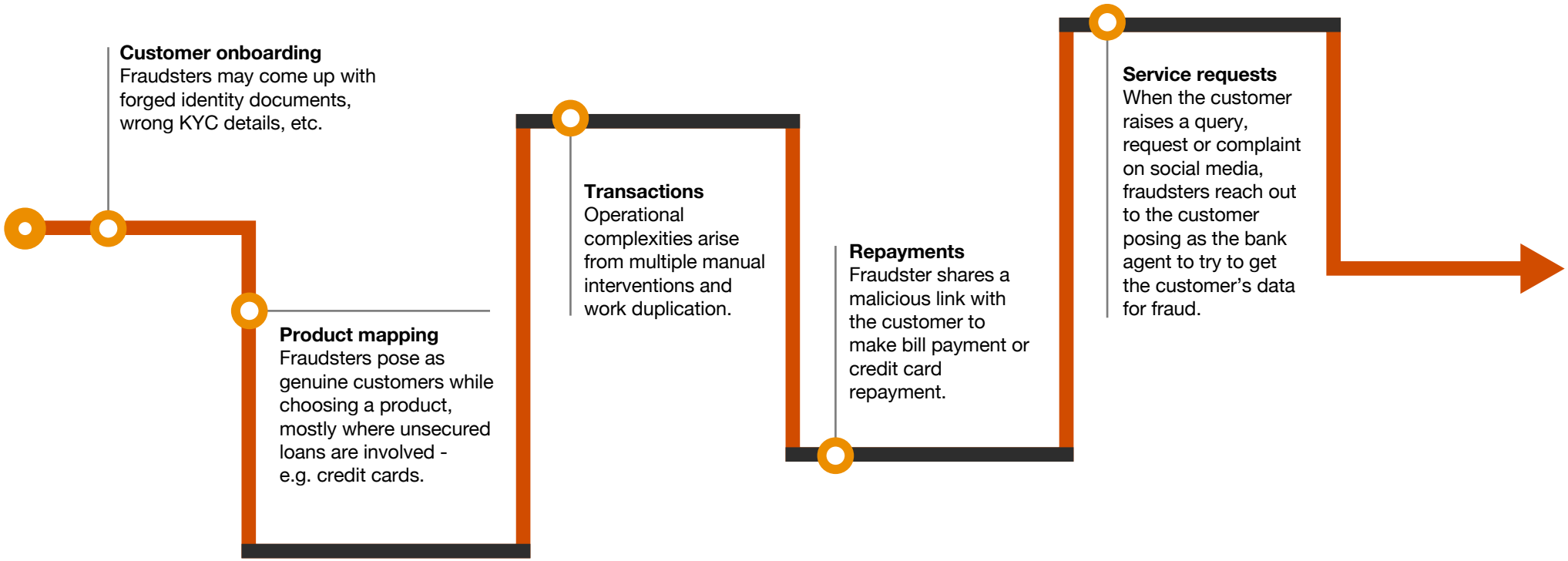
These percentages, though small, mask a ballooning threat as transaction volumes explode, spotlighting the urgent need to tackle sophisticated fraud tactics in a digital-first world.

A range of fraudulent activities have been observed, including the widespread increase in UPI-related frauds and the tricky schemes employed by fraudsters to deceive victims with false promises of financial gain.

1 https://www.indiabudget.gov.in/economicsurvey/doc/echapter.pdf
2 https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2057013
3 https://sansad.in/getFile/loksabhaquestions/annex/183/AU211_sk53e3.pdf?source=pqals

01 Introduction

The following flowchart illustrates how payments fraud can occur at any stage of the digital transaction lifecycle, highlighting key vulnerable points.



Credit card frauds, QR code scams, e-commerce account takeover, biller scams, courier scams, web skimming are some of the many common frauds. Fraudsters have introduced several new methods to pull off payments fraud, and notably, are targeting the youth who are generally perceived to be the most informed and vigilant group of citizens.

01 Introduction

Control over payments fraud – is it still that far?

Combating payments fraud is an ongoing global challenge – one that is met with ever-evolving tactics by fraudsters. While complete eradication may be a distant goal, significant strides are being made worldwide to mitigate payments fraud risks, using a combination of advanced technology, regulations, and customer education and awareness.

As payments fraud risks continue to evolve on a global scale, various nations have implemented innovative strategies to enhance financial security. Below are some key payments fraud prevention measures and frameworks being adopted worldwide:

In the US, the delayed but rapid rollout of EMV chip technology since 2015 has dramatically shifted fraud from in-person card cloning to online channels, cutting counterfeit card losses by over 75% at equipped merchants.[4]

Example 1: Account verification services (AVS) were introduced, which flag mismatched billing addresses during online purchases.

Example 2: Positive pay was launched, where businesses match issued checks against bank records to block fakes, to tackle evolving threats.

The UK has made notable advancements in payments fraud prevention through practical, innovative measures.

Example 1: Introduction of real-time transaction monitoring systems that flag suspicious activities – such as unusually large transfers to new accounts – allowing them to pause payments and contact customers within minutes to verify legitimacy

Example 2: Confirmation of payee services where payers verify if the recipient's name matches the account details, has reduced Authorized Push Payment (APP) fraud (wherein victims are tricked into sending money to fraudsters) by catching discrepancies early.

As online transactions increase, the US encounters significant fraud challenges in the digital payments sector.

The UK has seen a sharp rise in Authorised Push Payment (APP) fraud, prompting swift action to protect its digital payment users.

Singapore, a hub for digital innovation, is grappling with sophisticated fraud tactics such as behavioural manipulation scams targeting its advanced payment systems.

Singapore has adopted a comprehensive, multi-layered approach to payments fraud prevention, integrating digital intelligence, behavioural analysis and fund tracking systems.

Example 1: Integration of digital analysis, behavioural analysis and fund tracking systems in their financial systems

Example 2: Introduction of Protection from Scams Bill to empower law enforcement to freeze the accounts of victims, preventing further financial losses[5]

Despite these advancements, human elements – trust, awareness and vulnerabilities – continue to pose a significant challenge. While technological innovations and regulatory measures contribute to strengthening the financial ecosystem, the complete eradication of payments fraud remains an elusive goal. The aim is not to eliminate payments fraud but to cultivate a resilient financial system in which payments fraud risks are minimised, and consumers can transact with greater confidence.

4 https://www.darkreading.com/cyber-risk/fraud-drops-76-for-merchants-using-emv-says-visa
5 https://www.mha.gov.sg/mediaroom/press-releases/introduction-of-the-protection-from-scams-bill/

02 Facets of payments fraud

India's rapid shift to digital payments, driven by the widespread adoption of UPI, has turned the country into a prime target for payments fraud. As millions embrace cashless transactions for everything from daily purchases to bill payments, fraudsters have seized the opportunity to exploit vulnerabilities in this growing ecosystem.

Here are some of the key tactics fraudsters use to target India's digital payments consumers:

1. Refund fraud

Refund fraud targets UPI users by exploiting the ease of peer-to-peer transfers. Fraudsters contact victims, claiming they've accidentally sent money to the user's UPI account and need it returned. They often use fake transaction screenshots or impersonate real entities like shopkeepers to build trust, pressuring the victim to send the alleged amount to a different UPI ID. This tactic takes advantage of India's high volume of UPI transactions, where users may not double-check claims before transferring funds, leading to significant losses.

2. AI-driven impersonation

Advancements in technology, particularly AI, have enabled fraudsters to impersonate trusted entities with alarming precision in India's digital payments space. Using AI-generated voice calls or deepfake videos, they pose as bank officials or customer service agents, convincing users to divulge sensitive details such as OTPs or to authorise UPI payments under the guise of securing their accounts. This tech-driven approach exploits the growing reliance on digital banking in India, posing a sophisticated threat to unsuspecting users.

Building a secure digital payments ecosystem

It is important to understand and address the various complex drivers of payments fraud for creating a secure digital payments ecosystem. Social engineering, technical advancements, low financial awareness and liberal legal restrictions collectively contribute to the persistence and evolution of payments fraud. Therefore, each of these factors requires targeted strategies for effective mitigation.

Educating consumers about common payments fraud tactics and improving financial literacy are crucial steps in empowering individuals to protect themselves. Additionally, leveraging advanced technologies such as AI and ML can enhance payments fraud detection and prevention, allowing for real-time analysis of transactional data to identify suspicious activities. At the same time, strengthening legal frameworks and mechanisms is imperative to deter fraudulent activities and to ensure that trust in digital payment systems is maintained.

An all-encompassing approach that combines education, technology, law enforcement and policy development is necessary to safeguard consumers and businesses alike. By addressing these vulnerabilities and fostering collaboration across the payments ecosystem, we can build a resilient and trustworthy digital economy that minimises payments fraud risks and enhances financial inclusion.

03 Key stakeholder actions

Navigating the payments ecosystem

Although it may be difficult to navigate through the payments ecosystem, by breaking it down and learning about the responsibilities of each major participant, we can see a clearer picture. A brief overview of the primary players and their specific roles in mitigating payments fraud is presented below.

1. Regulatory bodies (RBI, FIU and NPCI): Architecting financial resilience

In the digital age, financial security is not about building walls, but creating intelligent, adaptive systems. This philosophy is evident in the current regulatory approach, which emphasises flexibility, innovation and measures to safeguard financial systems against evolving threats.[6]

Digital payment security controls for non-bank payments system operators: A comprehensive overview[7]

The Master Directions on Cyber Resilience and Digital Payment Security Controls for non-bank Payment System Operators represent a significant shift in India's approach to digital payments security, moving from traditional compliance to proactive prevention. Below are some key highlights:

Mandatory AI-driven fraud detection: The act requires financial institutions to implement advanced ML systems that can:

- Analyse transaction patterns in real time.
- Identify potential fraud with 99.6% accuracy.
- Adapt to emerging fraud techniques automatically.

Comprehensive data protection protocols: An approach that spans beyond traditional data protection:

- End-to-end encryption for all digital transactions
- Strict guidelines for data handling and storage
- Mandatory quarterly security audits for all financial institutions

Enhanced penalty structures: A deterrent mechanism that ensures institutional accountability:

- Substantial financial penalties for security breaches
- Potential suspension of operational licences for repeated violations
- Personal accountability for top management in case of systemic failures

Impact: The regulations have already demonstrated remarkable effectiveness, with a reduction in reported financial cyber incidents within six months of implementation.[8]

2. Card networks: The technological frontiers

The role of card networks has evolved significantly. They are no longer mere facilitators of transactions but have become key players in digital security. This transformation signifies their role in creating robust, intelligent systems that protect against fraud and ensure secure transactions.[9]

Quantum encryption: The next frontier

A significant advancement has been observed wherein card networks have initiated the first large-scale pilot of quantum-resistant encryption:

- Developed in collaboration with leading quantum computing researchers
- Capable of protecting against potential future quantum computing attacks
- First implementation covers high-value international transactions[10]

6 https://www.pwc.in/assets/pdfs/consulting/financial-services/fintech/payments-transformation/combating-fraud-in-the-era-of-digital-payments.pdf
7 https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12715
8 https://rbi.org.in/Scripts/PublicationVisionDocuments.aspx?Id=1159
9 https://ibsintelligence.com/ibsi-news/indias-fraud-risks-rise-but-genai-could-be-the-game-changer-study-shows/
10 https://www.finextra.com/blogposting/27840/digital-fortification-rbis-new-measures-and-the-future-of-fraud-prevention-in-india

03 Key stakeholder actions

3. Issuers and acquirers: Advanced risk management

Banking institutions: Redefining security paradigms

The role of risk management in banking has evolved significantly. It's no longer just about detecting fraud after it occurs but about predicting and preventing it before it happens. This proactive approach involves using advanced technologies like AI and ML to analyse patterns and identify potential threats early on.[11]

Hyper-personalised fraud detection

- ML models with unprecedented 99.8% accuracy
- Individual user behaviour profiling beyond traditional parameters
- Real-time risk scoring that considers:
  - transaction history
  - geolocation
  - device characteristics
  - behavioural biometrics

Biometric authentication evolution

- Covers high-value transactions
- Includes advanced techniques like:
  - typing pattern analysis
  - device interaction fingerprinting
  - voice and facial recognition technologies

4. Payment service providers (PSPs): Technology alchemists

Transforming digital transaction security

The concept of a zero-trust ecosystem is transforming digital security. In this model, every transaction is treated as a potential threat and must be verified before being trusted. This approach involves continuous verification, strict identity checks and the use of advanced security measures to ensure that every interaction is secure.[12]

Blockchain-enhanced security mechanisms

- Blockchain-enhanced security mechanisms have seen substantial global investments. Implementation of:
  - immutable transaction records
  - decentralised verification protocols
  - smart contract-based fraud prevention[13]

5. Merchants: From vulnerable to vigilant

Strategic defense in the digital marketplace

A significant transformation has taken place in merchant-level fraud prevention:

- ML models have substantially reduced fraud.
- Real-time transaction screening now operates with millisecond-level decision-making.
- Advanced geolocation and device fingerprinting technologies are being utilised.

11 https://pib.gov.in/PressReleasePage.aspx?PRID=2114874
12 https://www.thehindu.com/sci-tech/science/indian-cryptography-research-gears-up-to-face-the-quantum-challenge/article69115334.ece
13 Ibid.

03 Key stakeholder actions

6. Consumers: Empowered digital citizens

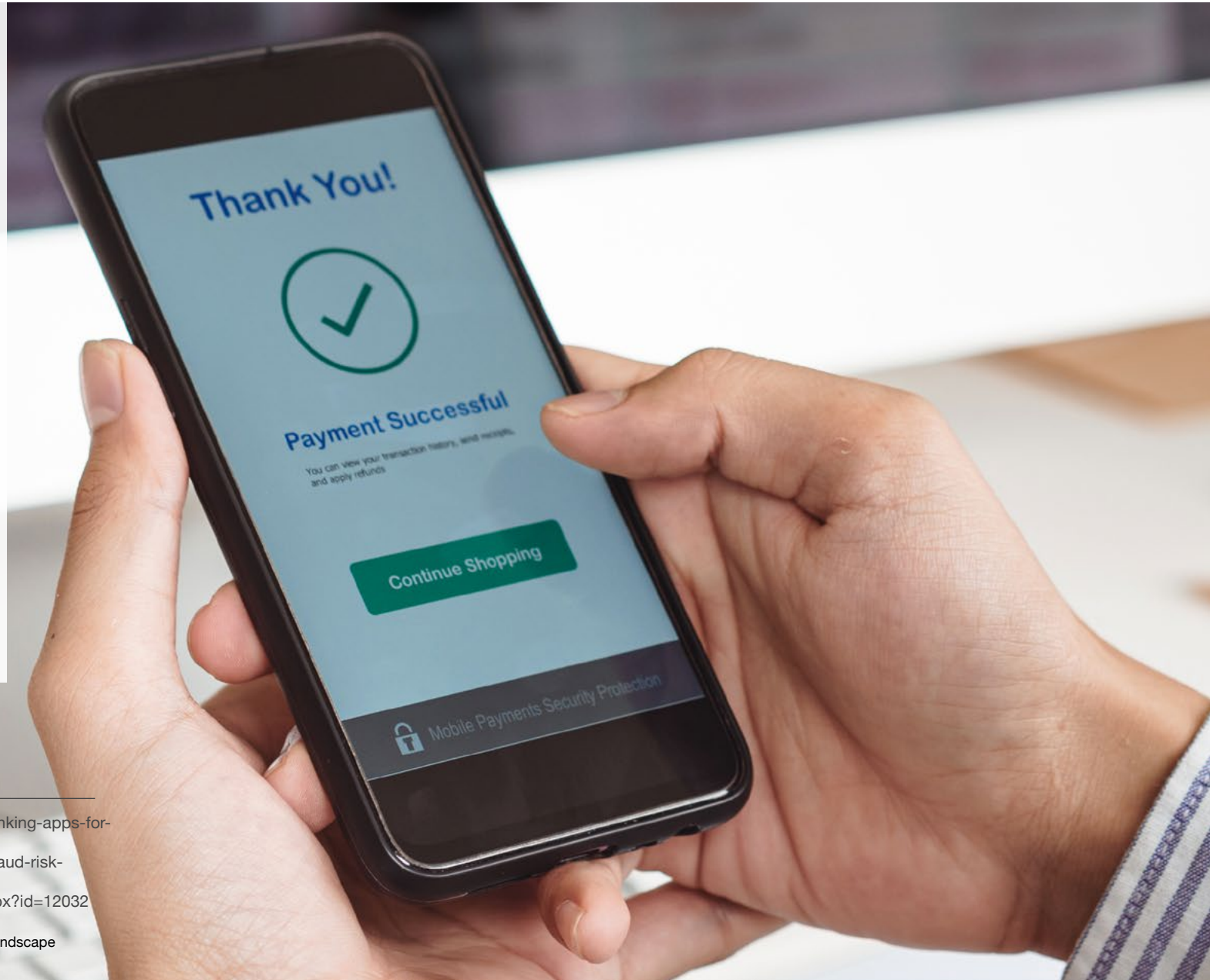
The most significant change is perhaps at the consumer level, which highlights the true democratisation of digital security:

- 78% of consumers now actively participate in fraud prevention[14]
- nationwide digital safety programmes providing free cybersecurity training
- advanced mobile banking security features that empower users[15]

Emerging technological frontiers

- Use of generative AI for fraud detection[16]
- Neuromorphic computing security
- Decentralised identity verification
- Predictive threat intelligence networks

The future of payments security is about creating adaptive, intelligent systems that anticipate, prevent and neutralise threats.



14 https://media.chase.com/news/consumers-are-using-banking-apps-for-more-than-transactions-new-chase-study-finds
15 https://www.npci.org.in/who-we-are/risk-management/fraud-risk-management
16 https://www.rbi.org.in/scripts/BS_ViewMasDirections.aspx?id=12032

04 Initiatives to tackle payments fraud

The Reserve Bank of India (RBI) has taken various initiatives in the recent years to fight payments fraud.

Phasing out UPI collect requests (proposed in FY25):

NPCI, which manages and operates the UPI platform, has suggested phasing out of the 'collect request' feature to curb UPI frauds aimed at gullible customers who approve fraudulent requests from fraudsters posing as authorised merchants. These collect calls would be replaced with 'push transactions' wherein the customers will now scan the merchant QR code to complete the payment.

Beneficiary account number look-up (proposed in FY25):[17]

To enhance security, the RBI plans to introduce real-time payee name validation before fund transfers.

Users will receive instant feedback on whether the recipient's name matches the provided account details.

This initiative aligns with the newly enacted Digital Personal Data Protection Act, 2023, ensuring data protection during transactions.

Digital Payments Intelligence Platform (proposed in 2024):[18]

The RBI plans to establish a Digital Payments Intelligence Platform to combat payments fraud.

This platform will leverage advanced technologies, providing network-level intelligence and real-time data sharing across all payments systems.

A committee led by A.P. Hota, former MD and CEO of NPCI, is examining the feasibility of this digital infrastructure and will provide recommendations within two months.

Sanchar Saathi Scheme, 2023:[19]

In 2023, the Department of Telecommunications (DoT) rolled out the Sanchar Saathi Scheme, which plays an important role in enhancing the security of mobile phone users throughout India. This initiative is about giving people the tools they need to manage and protect their mobile connections.

While Sanchar Saathi doesn't directly deal with financial transactions like some of the RBI initiatives, it does play an important role in cutting down on telecom-related fraud. By improving how mobile devices are tracked and allowing users to report any unauthorised activity, the scheme helps spot and stop fraudulent actions. It also encourages cooperation between telecom companies and law enforcement, which means quicker action when fraud is suspected.

Even though its focus isn't directly on stopping payments fraud, the security improvements from Sanchar Saathi have had a positive ripple effect.

By tightening security around mobile devices, it helps keep fraudsters at bay, contributing to a safer environment for everyone using digital payments.

Digital Payment Security Controls, 2020:[20]

The Digital Payment Security Controls introduced by the RBI in 2020 comprise a thorough set of guidelines intended to bolster the security of digital payments systems in India. These measures are crafted to reduce risks linked to digital transactions, safeguard consumers and maintain the integrity and security of the payments ecosystem.

- Establishment of robust risk management framework
- Security control measures including authentication, transaction monitoring and data encryption
- Customer protection and incident reporting measures

17 https://bfsi.economictimes.indiatimes.com/news/financial-services/payee-name-lookup-whats-the-new-feature-rbi-plans-to-introduce-in-payment-systems/100659078
18 https://economictimes.indiatimes.com/industry/banking/finance/banking/rbis-proposed-digital-payments-intelligence-platform-will-mitigate-frauds-say-experts/articleshow/110801767.cms?from=mdr
19 https://sancharsaathi.gov.in/
20 https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12032

04 Initiatives to tackle payments fraud

Tokenisation Guidelines, 2019:[21]

The Tokensation Guidelines introduced by the RBI in 2019 aim to enhance the security of card transactions by substituting sensitive card information with a unique identification code called a 'token'. This method helps protect card details during digital transactions and lowers the risk of payments fraud.

- Only authorised networks (Visa, Mastercard, RuPay) can act as token service providers (TSPs).
- Token requestors such as mobile payment operators, merchants or digital wallets must be registered with the TSPs to offer tokenisation services.
- Tokens can be used to perform card transactions without exposing actual card details, thereby enhancing transaction security.

Internal Ombudsman Scheme, 2018:[22]

The Internal Ombudsman Scheme 2018, introduced by the RBI, aims to improve the efficiency of grievance redressal mechanisms within banks and ensure the fair resolution of customer complaints. This scheme requires certain banks to appoint an Internal Ombudsman to independently review and resolve complaints that have been partially or wholly rejected by the bank's internal grievance redressal system.

Cyber Security Framework, 2016:[23]

The Cyber Security Framework for Banks comprises an extensive set of guidelines designed to enhance the cyber resilience of banks and financial institutions across India. This framework tackles the growing threats posed by cyberattacks to the banking sector and ensures that banks implement strong cybersecurity measures.

- Cybersecurity policy to be formulated
- Dedicated committee to oversee cyber security measures
- Vulnerability assessment and penetration testing

Cyber crisis management plan

- Third-party risk management

Indian Cyber Crime Coordination Centre (14C):[24]

The Cyber Crime Co-ordination Centre (I4C) has been set up by the Government of India with the aim of improving the collaborative efforts of various law enforcing agencies (LEAs) in the fight against cybercrime. This initiative aims to provide a cohesive framework for addressing digital threats comprehensively. A key function of the 14C is to arrest the fund flow by alerting the banks or wallet firms concerned so that the account can be instantly frozen. In line with recent developments, the RBI has announced that banks will use the 'bank.in' internet domain name, while non-bank financial institutions will use 'fin.in'. This measure aims to create a clear and secure digital identity for financial entities, facilitating easier and more secure communication in case of cybercrime.

Parallelly, the government has also launched the National Cyber Crime Reporting Portal that allows individuals to report cybercrimes directly. All cybercrime incidents that are reported through this portal are then automatically relayed to the respective LEAs of the concerned state or Union Territory for further intervention and satisfactory closure. These efforts collectively strengthen the national framework for combating cyber threats, ensuring that both preventive and responsive actions are effectively coordinated.

RBI Guidelines:[25]

The RBI mandates the deactivation or removal of out-of-contact numbers identified as fraudulent from the database by using the mobile number reconciliation (MNRL) process.

Customer care numbers must be enrolled and validated on the Sanchar Saathi portal to ensure authenticity.

21 https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=45954
22 https://www.rbi.org.in/CommonPerson/english/Scripts/PressReleases.aspx?Id=2709
23 https://www.rbi.org.in/scripts/notificationuser.aspx?id=10435
24 https://i4c.mha.gov.in/about.aspx
25 https://telecom.economictimes.indiatimes.com/news/policy/trai-directs-telcos-to-migrate-140-series-telemarketing-calls-to-dlt-platform-by-sept-30/112646616

04 Initiatives to tackle payments fraud

Distinct numbering series usage:

- 1600xx should be designated for service-related calls.
- 140xx must be used exclusively for promotional calls.

Debit accounts that have a negative balance will undergo increased scrutiny, particularly when associated mobile numbers are revoked.

The RBI has advised financial institutions to adopt the following measures to protect consumers:

- Financial institutions should conduct periodic reviews and remove inactive or unused sender IDs.
- Only verified URLs, callback numbers and short codes should be whitelisted to ensure authenticity.
- To prevent fraudulent activities, institutions are required to utilise pre-approved SMS templates for communications.
- Promotional content is not permitted in service-related messages.

TRAI Regulations:[26]

- All senders must register on the DLT platform before sending promotional SMS or calls.
- No entity can use random 10-digit mobile numbers for commercial communication.
- Failure to comply may result in blacklisting and telecom disconnection for up to two years.

26 https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2046872

05 Recommendations

As a part of our ongoing commitment to safeguard citizens from the growing threat of financial payments fraud, particularly mule accounts, we are continuously exploring innovative strategies.

Below are a few of these strategies that can be implemented to enhance the overall payments fraud prevention measures.

Biometric (voice/facial) authentication:

- To implement a system where customers must provide a voice sample during account setup – For high-value transactions or suspicious activities, the system could request a voice authentication. This will provide an additional layer of security since voice patterns are unique and difficult to replicate.
- For high-value UPI transactions, instead of sending an OTP via SMS, financial institutions can use a voice call with a voice-based OTP.
- Integrate facial recognition technology for transactions above a certain threshold, the user's face must be scanned through their device's camera before proceeding. This adds biometric security to UPI payments.

Dynamic UPI pin and QR codes with audio alerts:

To bolster UPI security, India can build on existing measures like OTPs for high-value transactions by introducing a system where the UPI PIN changes automatically after a set number of transactions or time. Additionally, adopting dynamic QR codes, generated uniquely for each transaction and expiring within minutes, can tackle fake QR code scams by ensuring each payment request is one-time and secure. These devices also provide instant audio alerts to confirm transactions and integrate seamlessly with UPI apps, adding an extra layer of verification for users. Together, these measures create a multi-layered defence, reducing the risk of fraud in India's fast-growing UPI ecosystem.

Usage of AI:

Use AI to analyse not just transaction patterns but also user behaviour on digital platforms, including mouse movements, typing speed and navigation patterns. Any deviation from the user's established behaviour could trigger a manual review or additional verification steps.

AI-driven mock phishing:

With customer consent, use AI to simulate phishing attempts on them in a controlled, ethical manner to test their vigilance. If they fall for the simulation, they receive immediate instruction on how to recognise and avoid real phishing attempts, turning potential vulnerabilities into learning opportunities.

Payments fraud prevention gamification:

Financial bodies can introduce a gamified learning platform within banking apps to educate customers on payments fraud prevention through interactive scenarios. Rewards could include small account credits or discounts on banking services, incentivising customers to learn and engage with security practices.

Central payments fraud prevention network:

- Collaboration between financial institutions where they can opt for a centralised database where PAN/Aadhaar sharing is performed. This will help financial institutions to check if any PAN/Aadhaar is flagged by other bodies before onboarding the customer.
- Collaborate with other financial institutions to create a decentralised network where payments fraud alerts are shared instantly and anonymously across institutions for real-time detection and prevention of fraud attempts.

05 Recommendations

Mule account prevention

Account relationship mapping:

Financial institutions can develop a system to map relationships between accounts. Mule accounts often have connections with many other accounts, serving as a middleman. By mapping these relationships, they can identify clusters of activity that might indicate mule operations.

Centralised mule monitoring system:

Implement a centralised mule monitoring system that tracks suspicious or anomalous transaction patterns across multiple financial institutions. This system would aggregate transaction data in real time, flagging potential mule accounts and enabling financial institutions to take swift action. By monitoring account activities such as rapid fund transfers or atypical withdrawal behaviour, the system can help detect money laundering and other fraudulent activities more efficiently across the financial ecosystem.

06 Conclusion

Digital payments promise financial inclusion – like enabling a farmer in rural India to receive government benefits via UPI – but the cost of unaddressed risks can result in financial fraud.

In 2023, India reported USD 1.7 billion[27] in UPI fraud, with most of it tied to social engineering, exposing gaps in awareness as adoption outpaces education.

Globally, fraud tactics evolved faster than traditional defenses, with the US seeing online fraud spike post-EMV and the UK racing to curb APP scams.

Businesses can counter this with AI-driven detection, flagging odd patterns in seconds and practical tools like the UK's Confirmation of Payee, which cut impersonation fraud by 17%.[28] Yet, technology alone isn't enough. Collaboration between banks, regulators, and consumers, shared fraud databases or joint awareness campaigns disrupts fraud networks more effectively than siloed efforts.

Empowering users with the know-how (e.g. spotting phishing) and options like multi-factor authentication build trust without slowing progress. A secure digital future hinges on blending sharp technology, real teamwork and informed users – not just chasing cashless goals.

27 https://sansad.in/getFile/loksabhaquestions/annex/183/AU211_sk53e3.pdf?source=pqals
28 https://www.openbankingexpo.com/insights/insight-confirmation-of-payee-a-crucial-tool-in-combating-app-fraud-in-the-uk/

Contact us

Vivek Belgavi
Partner and Leader, Financial Services Advisory
PwC India
vivek.belgavi@pwc.com

Mihir Gandhi
Partner and Leader, Payments Transformation and FinTech
PwC India
mihir.gandhi@pwc.com

Geetika Raheja
Partner, Payments Transformation and FinTech
PwC India
geetika.raheja@pwc.com

Zubin Tafti
Executive Director, Payments Transformation and FinTech
PwC India
zubin.tafti@pwc.com

Authors:
Mohit Singh, Rahul Chemburkar, Swatantra Singh, Kusal Hiten Shah

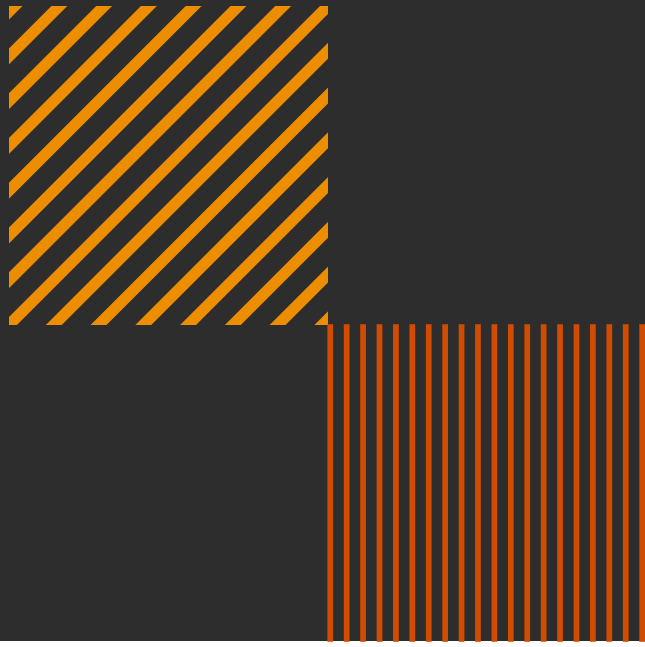
Editor:
Rashi Gupta

Design:
Harshpal Singh

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 149 countries with over 370,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.



pwc.in

Data Classification: DC0 (Public)

HS/April 2024 - M&C 45223