Easebuzz | India FinTech Forum

Fintech Policy Advocacy

TRUST & TECH

DIALOGUES

Building Resilience Against Financial Crimes in Digital Payments – A Shared Responsibility

www.indiafintech.com

www.easebuzz.in

Table of Contents

Editorial Team

Nipa Dutta
CEO, India Fintech Forum

Parimal Kumar Shivendu
Group Head, Easebuzz

Trust and Tech Roundtable | Key Insights

I. Scale of the Problem: Global and Indian Context

- In 2023, approximately **$3.1 trillion** in illicit funds flowed through the global financial system; about **16%** of these were fraud-related transactions.
- Globally, 1 in 5 people has been a victim of some form of financial fraud. The situation is even more alarming among older people—**60%** of individuals above the age of 60 have experienced fraud at some level.
- In India, with its explosive growth, rapid innovation, and an ageing population with higher wealth and financial independence, the challenge is magnified.
- In 2022, 60% of complaints recorded on government portals were related to financial crimes.
- Reported financial crime losses were around **₹2,000 crore** in 2022, which doubled to nearly **₹5,000** crore in 2023.
- According to the IBM Security Report 2023, the average cost of a data breach in India rose to **₹17.9 crore**, marking a **28% increase** since 2020.

The Digital Payments Landscape

- India's digital payments ecosystem has grown remarkably in the last five years. Transaction volumes increased nearly fourfold—from **4,371 crore** in 2020–21 to 16,443 crore in 2023–24, reflecting a CAGR of about **49%.**
- This surge has been primarily driven by UPI, which has become the backbone of digital payments.
- However, UPI-related frauds have also surged—cases increased by **85%** in FY24, from **7.25 lakh** in FY23 to **13.4 lakh.**
- The total value of UPI frauds more than doubled in the same period, rising from **₹573** crore to **₹1,087 crore.**

Other Fraud Trends

- Card and internet-related frauds accounted for 87% of all cases in April–September 2023–24, and 71% in April–September 2024–25 for banks.
- Fraudsters have targeted all groups, including experienced bankers, technology CXOs, and senior government officials. However, the most vulnerable have been elderly and retired individuals, who are often exploited due to their trust, accumulated wealth, isolation, and declining cognitive health.

II. Enhancing Public Awareness and Education

Despite mandatory communications from banks and widespread media efforts (e.g., WhatsApp groups), awareness campaigns are having a limited impact.

The bigger challenge lies in the lack of knowledge about remedial actions after a fraud occurs. Victims are often unaware of their rights vis-à-vis financial institutions and the extent of bank/company liability. As a result, valuable time is lost before reporting, which allows the fraud to escalate and become more difficult to trace.

Remedial Measures:

- **Large-Scale & Ongoing Programs:** There is an urgent need to implement continuous public awareness campaigns to educate citizens about:
  - **New and Evolving Fraud Types:** Proactively share information on the latest scams and digital threats.
  - **Prevention Methods:** Provide clear, actionable steps individuals can take to protect themselves.
- **Targeted Education:**
  - **Business Leaders & Professionals:** Equip them with knowledge of financial crimes and responsible practices to prevent organisational vulnerabilities.
  - **Vulnerable Groups (e.g., elderly, less educated):** Develop interactive programs tailored to their needs, addressing their unique susceptibilities.
  - **Incentivise Participation:** Encourage citizens to undergo training by offering small incentives.

- **Empowering Victims with Recourse Information:**
  - **Increase Awareness of Recourse Mechanisms:** Clearly communicate avenues such as the Banking Ombudsman and RBI guidelines on limited liability.
  - **Streamline Reporting Processes:** Simplify how victims can report fraud and help them understand their rights regarding fund recovery.
- **Innovative Funding & Outreach:**
  - **Leverage CSR Initiatives:** Encourage corporates to fund consumer education programs as part of their Corporate Social Responsibility (CSR).
  - **Utilise Popular Media:** Create relatable content—through films, short videos, and digital campaigns—that both incentivises reporting and provides practical guidance.

III. Utilising Fire to Fight Fire

Fraudsters are rapidly advancing their social engineering methods by leveraging emerging technologies, particularly Artificial Intelligence (AI).

- **AI-assisted attacks** such as phishing, vishing, smishing, and whaling use fraudulent emails/websites, voice impersonation, SMS fraud, and scams targeting senior officials.
- **Generative AI** is now creating hyper-realistic impersonations, including deepfakes, synthetic identities, and fabricated data.
- **AI-powered cybercrime tools** are enabling the development of next-generation malware, Man-in-the-Middle (MiM) attacks, self-propagating fraud engines, and polymorphic hacking software—making fraudulent activities nearly undetectable by conventional methods.
- In India, the rapid adoption of UPI has led to new forms of scams beyond traditional account hacking or OTP-based fraud. A notable example is "digital arrest", where entire syndicates target victims after collecting personal or business information from social media and other surroundings.

Remedial Measures:

1. Technology for Fraud Detection and Prevention

- **Collaborative Defence:** Share data across providers through interoperable data lakes to better track fraud patterns.
- **Synthetic Data with AI:** Deploy AI-enabled synthetic data to minimise false positives and eliminate biases.
- **Mule Account Detection:** Identify and block mule accounts used for parking illicit funds.
- **AI-Powered Threat Intelligence:** Continuously track and analyse fraud trends for real-time anomaly detection and pattern recognition.
- **Dynamic Transaction Firewalls:** Alert users of potential fraudulent activity before a payment is committed—moving away from the current post-transaction analysis approach.

2. Digital IDs & Secure Authentication

- **Beyond OTPs:** Develop and adopt stronger Multi-Factor Authentication (MFA) methods to reduce reliance on vulnerable OTPs.
- **Biometric & Behavioural Analytics:** Use advanced methods such as keystroke dynamics and user behaviour analysis to detect Remote Access Trojans (RATs).
- **Geo-Pattern Analysis:** Monitor IP-based activity to detect syndicated crimes linked to specific regions.

3. Enhanced Customer Protection

- **Product Company Accountability:** Payment product companies should take responsibility for fraud prevention, offering built-in consumer protection (e.g., seller protection, chargeback mechanisms).
- **Location-Based Restrictions:** Implement checks to restrict payments originating from high-risk locations or IP addresses.
- **Data-Driven Models:** Use diverse data sources—such as device details, card history, and transaction patterns—to build robust fraud detection systems.
- **Friction in Payment Products:** Introduce interactive transaction processes that add risk-monitoring controls while engaging the customer.

4. Blockchain for Data Security

- **Blockchain Applications:** Explore blockchain and distributed ledger technology (DLT) to ensure secure, immutable storage and authentication of personal and financial data.

IV. Strengthening Regulatory & Law Enforcement Frameworks

India's digital payments ecosystem has grown rapidly, but financial fraud—driven by gaps in KYC processes, telecom negligence, weak Accountability within financial institutions, and fragmented enforcement—poses a serious threat to consumer trust and systemic stability. Existing identity verification mechanisms are outdated and vulnerable, while coordination among banks, telecom operators, law enforcement agencies, and regulators remains inefficient. This often results in delayed responses and inadequate redressal for victims.

Underreporting of fraud, driven by low awareness, stigma, or lack of confidence in institutional response, further conceals the accurate scale of the problem. Weak implementation of data privacy safeguards compounds the issue by enabling the misuse of personal information. Unless addressed through modernisation, stronger Accountability, legal reforms, better inter-agency coordination, and incentives for reporting, these challenges risk undermining the progress India has made in building a robust, inclusive, and trusted digital financial ecosystem.

Remedial Measures:

1. Modernise KYC Processes

- **Adopt Technology-Driven KYC:** Replace outdated, document-heavy procedures with digital, consent-based identity verification that balances ease of use with fraud prevention.
- **Leverage the Account Aggregator (AA) Framework:** Expand adoption of the AA ecosystem to enable secure, consent-driven sharing of financial data.

2. Increase Accountability

- **Telecom Accountability:** Enforce liability on telecom operators for negligence leading to fraud, including SIM-swap scams.
- **Financial Institution Accountability:** Impose strict penalties on banks that open accounts with weak KYC compliance or fail to act swiftly on reported fraud.

3. Judicial & Enforcement Reforms

- **Streamline Reporting & Investigation:** Simplify fraud reporting for victims and ensure faster, coordinated investigations.
- **Law Enforcement Training:** Provide continuous training to police and cybercrime units on digital forensics, financial crime patterns, and investigative best practices.
- **Strengthen Legal Frameworks:** Reclassify serious cybercrimes as non-bailable offences and expedite judicial processes to act as a deterrent.
- **Improve Inter-Agency Coordination:** Enhance collaboration between police, banks, regulators (RBI, NPCI), and the Indian Cybercrime Coordination Centre (I4C).

4. Incentivise Reporting

- **Financial & Non-Financial Incentives:** Guarantee quick interim relief (e.g., reversal of funds within 24 hours of bank-reported fraud) while investigations continue.
- **Address Underreporting:** Reduce stigma and build confidence in redressal systems to encourage victims to report incidents.
- **Fraud Transparency in Marketing:** Mandate disclosure of fraud-prevention measures in financial product promotions.

5. Strengthen Data Privacy Protections

- **Practical Implementation of the DPDP Act:** Ensure strict compliance with the Digital Personal Data Protection Act (DPDP) to safeguard personal data.
- **Promote Consent Architecture:** Operationalise consent-driven data-sharing frameworks such as those within India Stack.

V. Fostering a Collaborative Ecosystem

The increasing sophistication and scale of financial fraud underscore systemic vulnerabilities that demand a collective response. Public awareness of evolving fraud techniques remains low, while fragmented compliance practices often prioritise box-ticking over principle-driven prevention. Fraud prevention cannot be the sole responsibility of regulators; it must be embraced as a shared mandate by banks, fintechs, telecom operators, hardware providers, customers, and law enforcement agencies alike.

However, the lack of structured collaboration platforms and industry consortia limits the sharing of best practices, technological innovations, and coordinated defence strategies.

Meanwhile, the talent pipeline for cybercrime investigation and fraud prevention remains underdeveloped, with few incentives for students and professionals to view this as a viable career path. Gaps also persist in bridging innovation and compliance, as compliance teams are often excluded from the early stages of product design, creating vulnerabilities at scale.

Furthermore, inadequate disclosure of fraud statistics by institutions obscures the true magnitude of the challenge, hindering informed policy interventions and leaving consumers unaware of which entities maintain stronger safeguards. Unless these challenges are addressed through coordinated education, collaboration, skill-building, principle-based compliance, and transparent reporting, India's financial ecosystem risks eroding the trust it has painstakingly built.

Remedial Measures:

Call for Action and Responsibility:

- Implement large-scale, ongoing public education programs to inform society about emerging fraud methods and prevention strategies.
- Focus on understanding the "intent" or "principle" behind regulatory guidelines to foster proactive compliance cultures.
- Recognise that fraud prevention is not solely the regulator's responsibility—every stakeholder in the financial ecosystem, including banks, payment processors, customers, and app providers, must play an active role.

Importance of Collaboration:

- Foster Partnerships: Encourage continuous collaboration among fintechs, traditional banks, regulatory bodies, law enforcement agencies, telecom operators, hardware OEMs, and all ecosystem stakeholders.
- Share Best Practices: Establish forums and platforms to share insights, innovative solutions, and success stories from both startups and established companies.

Collective Responsibility:

- Emphasise Shared Accountability: Reinforce that protecting the financial ecosystem is a collective responsibility, not just that of regulators.
- Promote Ethical Governance: Cultivate a culture of integrity and responsible practices across organisations to prevent internal vulnerabilities and misuse.

Skill Building:

- Enable students and professionals to pursue careers in combating financial and cybercrime.
- Make skill-building initiatives, including ethical hacking and fraud prevention, viable and lucrative career paths comparable to other law enforcement roles.

Bridging the Gap Between Innovation and Compliance:

- Integrate Compliance in Design: Involve compliance officers and legal teams from the initial product design phase to identify potential risks and build robust, secure systems.
- Support Innovative Solutions: Establish forums to promote and handhold disruptive fraud detection and prevention solutions developed by startups for adoption by regulators and larger industry players.

Measure and Disclose Fraud Data:

- Transparent Reporting: Encourage, and potentially mandate, financial institutions and platforms to report fraud statistics. This will provide a clearer picture of the problem's scale and highlight companies with robust security measures, similar to insurance claim ratios

Conclusion

Nip it in the bud:

As patterns of fraud evolve with advanced technologies, especially AI, organisations should:

- Simulate actions typically perpetrated by fraudsters using advanced AI.
- Create digital identities to detect behavioural and transactional anomalies.
- Implement a dynamic threat matrix to prevent fraud in real-time transactions rather than relying solely on historical data.
- Identify and prevent localised fraud using selective firewalls.
- Operate like a syndicate through collective data sharing, leveraging AI-powered analytical models and pattern recognition.

How to detect / where to report:

- Run targeted awareness campaigns, especially for vulnerable populations, with clear instructions on remediation. Use impactful channels such as films, field campaigns, and promotional activities.
- Ensure customers are well-informed about their data privacy rights and corporate liabilities.
- Encourage private-public collaboration to utilise CSR funds for impactful awareness and remediation campaigns.
- Train and equip law enforcement agencies (LEAs) and government bodies to support victims effectively.

Regulators to step in:

- Incentivise transparent reporting of fraud cases, encourage continuous improvement in fraud detection, and penalise non-disclosure or failure to implement committed controls.
- Mandate the inclusion of fraud metrics in reporting and product marketing.
- Introduce a dynamic Fraud Threat Matrix to be adopted globally by all companies.
- Encourage industry consortia to treat fraud resolution as an end-to-end process, similar to the organised syndicates committing the fraud.
- Similar to Investor Awareness Programs (IAP) for AMCs, banks and corporates should allocate a certain percentage of revenue for targeted fraud training across the value chain—covering financial institutions, product companies, telecom providers, and hardware/gadget OEMs.

Ecosystem involvement:

- Encourage the formation of consortia and forums involving all stakeholders to:
- Share data to block and mitigate entry points for syndicated fraud.
- Exchange best practices across the industry.
- Collaborate on solutions for everyday challenges in the value chain.
- Train the next generation in financial and cybercrime.
- Create spaces for open conversation, brainstorming, disruptive ideas, and product innovation.


TRUST & TECH
DIALOGUES
Buzzing भारत
Easebuzz
Celebrating
the entrepreneurial spirit of
भारत


Easebuzz
India FinTech Forum
TRUST & TECH
DIALOGUES
Building Resilience Against Financial Crimes in Digital Payments – A Shared Responsibility
Buzzing भारत
Celebrating
the entrepreneurial spirit of
भारत


IFTA 2025

Thank You

www.easebuzz.in | www.indiafintech.com