4. Digital Fraud in India- Economy

Recently the Reserve Bank of India (RBI) has proposed to compensate for losses arising from small-value fraudulent transactions

Background- RBI's Regulatory Mandate

The Reserve Bank of India (RBI), as India's monetary authority and banking regulator, operates under the RBI Act, 1934 and the Banking Regulation Act, 1949.

Beyond monetary policy, RBI performs-

1. Consumer protection oversight
2. Payment systems regulation
3. Supervisory control over banks and NBFCs
4. Cybersecurity risk governance

The latest proposal on compensation for small-value digital fraud reflects RBI's shift toward consumer-centric financial regulation.

Key Features of RBI's Proposed Compensation Framework

Compensation Cap- Customers may receive compensation up to ₹25,000 for small-value unauthorized transactions. Applicable even in cases where OTP was shared unintentionally, recognizing the evolving nature of digital deception.

Compensation Formula

Either ₹25,000 or 85% of the loss (whichever is applicable).

In certain models-

1. 70% borne by RBI
2. Remaining portion shared with the concerned bank

Funding Source

1. Compensation to be disbursed from the Deposit Education and Awareness Fund (DEAF).
2. DEAF is funded from unclaimed deposits and is intended for depositor protection and awareness.

Draft Guidelines for Public Consultation

RBI will release draft norms on-

1. Prevention of mis-selling of financial products
2. Fair loan recovery practices (curbing harassment and coercive recovery)
3. Limiting customer liability in unauthorized electronic banking transactions

Digital Payment Safety Enhancements

Discussion paper includes-

1. Delayed credit verification mechanism
2. Additional authentication layers for vulnerable users (elderly, rural customers)
3. Strengthening grievance redressal architecture

Objective

1. Enhance trust in digital payments
2. Promote accountability in banking institutions
3. Strengthen financial consumer protection

Present Status of Digital Fraud in India

Rising Cybersecurity Incidents

1. 10.29 lakh incidents in 2022
2. 22.68 lakh incidents in 2024

The increase reflects-

1. Greater digital penetration
2. Improved detection and reporting mechanisms
3. More sophisticated fraud techniques

Digital Payment Scale vs Fraud Rate

Despite high volumes of digital payments globally-

1. 1 fraudulent transaction per 1,01,242 transactions
2. ₹1.40 lost per ₹1 lakh transacted

This suggests-

1. Systemic robustness
2. Yet absolute loss figures remain significant due to transaction scale

Major Drivers of Digital Fraud

Rapid Digitisation

1. Over 86% of Indian household's internet-connected
2. Expansion under Digital India and UPI ecosystem
3. Increased attack surface for cybercriminals

Low Digital Literacy

1. Vulnerability to phishing, OTP scams
2. Lack of awareness of cyber hygiene

Weak Personal Security Practices

1. Sharing OTPs
2. Weak passwords
3. Downloading unverified applications

Organized Cybercrime Networks

1. Structured scam operations
2. Use of mule accounts
3. Exploitation of telecom loopholes

Identity Impersonation

Scammers posing as-

1. Bank officials
2. Government agents
3. Police authorities

Cross-Border Cyber Threats

1. Increasing foreign-origin cyber fraud
2. Jurisdictional challenges in enforcement

Ponzi & Investment Scams

1. Fake high-return digital platforms
2. Cryptocurrency and stock-trading fraud

Technological Exploitation

1. Clone websites
2. Fake mobile apps
3. Social engineering

Impacts of Digital Fraud

Economic Impact

1. Losses in tens of thousands of crores
2. Low recovery rate due to complex money trails

Banking System Impact

1. Increased compliance costs
2. Higher cybersecurity investments

Trust Deficit

1. Reduced public confidence in digital payments
2. Potential slowdown in digital financial inclusion

National Security Risk

Overlap with-

1. Data theft
2. Espionage
3. Terror financing

Social Impact

1. Elderly and rural users disproportionately affected
2. Psychological trauma and financial distress

Legal and Institutional Framework

Information Technology Act, 2000

1. Foundation of India's cyber law regime
2. Covers identity theft, impersonation, hacking
3. Empowers blocking of malicious platforms

IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

1. Accountability of social media intermediaries
2. Removal of unlawful content
3. Due diligence requirements

Digital Personal Data Protection Act, 2023

1. Mandates lawful processing of personal data
2. Data fiduciaries required to ensure security safeguards
3. Strengthens user consent framework

Key Institutions

Indian Computer Emergency Response Team (CERT-In)

1. Monitors cyber risks
2. Issues advisories
3. Conducts cybersecurity drills

National Critical Information Infrastructure Protection Centre (NCIIPC)- Protects critical sectors (banking, power, telecom)

Indian Cybercrime Coordination Centre (I4C)

1. Strengthens law enforcement coordination
2. Blocks fraudulent accounts
3. Provides technical assistance

National Cyber Exercises

1. Bharat National Cybersecurity Exercise 2025
2. STRATEX (Strategic Exercise)

These test inter-agency response preparedness.

Policy Significance of RBI's Intervention

Consumer-Centric Regulation

1. Recognizes asymmetric information between banks and consumers
2. Reduces victim-blaming in digital fraud

Risk Sharing Model- Shared liability among RBI and banks improves institutional accountability

Financial Stability Perspective- Protecting consumer trust prevents systemic digital payment slowdown

Behavioural Economics Dimension

1. Encourages customers to report fraud promptly
2. Reduces hesitation due to fear of total loss

Challenges in Implementation

1. Moral hazard risk (carelessness if compensation guaranteed)
2. Verification complexity in OTP-sharing cases
3. Administrative burden on banks
4. Ensuring quick grievance redressal

Way Forward

Strengthening Legal Framework

1. Stricter penalties for organized cybercrime
2. Fast-track cyber courts

AI & Machine Learning Integration

1. Real-time fraud detection
2. Behavioural anomaly tracking

Capacity Building

1. Specialized cyber police units
2. Judicial training in digital evidence

Public Awareness Campaigns

1. Regional language outreach
2. Targeted rural digital literacy programs

International Cooperation

1. Bilateral cybercrime treaties
2. Data-sharing agreements
3. Cross-border enforcement mechanisms

Conclusion

India's digital revolution has created both unprecedented inclusion and heightened cyber vulnerabilities. RBI's proposed compensation framework marks a progressive shift toward **shared liability and depositor protection**.

However, sustainable cyber resilience requires-

1. Strong regulation
2. Technological innovation
3. Institutional coordination
4. Citizen awareness

Only a coordinated, multi-stakeholder cybersecurity ecosystem can ensure that India's digital economy remains both inclusive and secure.

Source- https://indianexpress.com/article/business/digital-fraud-cases-rbi-plans-compensation-up-to-rs-25000-even-if-victim-shares-otp-10518253/