Intergovernmental Group of Experts on

Consumer Protection Law and Policy, 9th session

Room XII, Palais des Nations, Geneva

6-8 July 2026

Consumer Protection in Digital Financial Services: Lessons from India's Digital Payment Ecosystem for Global Policy Frameworks

Contribution

Voluntary Organisation in Interest of Consumer Education, India (VOICE)

UNCTAD INTERGOVERNMENTAL GROUP OF EXPERTS ON CONSUMER PROTECTION LAW AND POLICY

9TH SESSION | JULY 6–8, 2026 | GENEVA, SWITZERLAND
WRITTEN CONTRIBUTION

Consumer Protection in Digital Financial Services:
Lessons from India's Digital Payment Ecosystem for Global Policy Frameworks

Submitted by: Voluntary Organisation in Interest of Consumer Education, India (VOICE)
A Consumer Rights Organisation, India
May 2026

Authors
Rinki Sharma, Prof.K.V. Bhanu Murthy, Prof.Sri Ram Khanna
VOICE (India)

About VOICE

VOICE (Voluntary Organisation in Interest of Consumer Education) is a 43-year-old consumer rights organisation credited with initiating the consumer movement in India. Since its founding, VOICE has worked to protect, educate and empower consumers across all dimensions of their economic and social lives.

Core Work Areas

- Consumer Law, Rights and Advocacy -Consumer guidance, grievance handling, mediation and policy submissions.
- Consumer Awareness and Education - Consumer Voice publication, video lectures, public campaigns.
- Consumer Research and Product Testing -evidence-based research informing policy and consumer guidance.
- Regulatory Engagement - formal submissions to government bodies and regulatory authorities on consumer protection frameworks.

Leadership and Institutional Credibility

VOICE's leadership draws from senior academics, retired bureaucrats, lawyers and social activists, bringing institutional depth, cross-sector credibility and decades of ground-level consumer advocacy experience to every initiative the organisation undertakes.

The New Age Consumer Framework

In recent years, VOICE has embraced a modern strategic framework - 'The New Age Consumer' - developed by Prof. K.V. Bhanu Murthy, which aligns the organisation's work with the realities of India's digital age. This framework recognises that the nature of consumer problems has fundamentally changed: from physical marketplace grievances to

digital payment security, data privacy, algorithmic manipulation, platform accountability and the protection of consumers who are digitally challenged.[1]

The framework identifies nine new dimensions of consumer concern in the digital environment - from payment system security and data theft to the use of optimisation algorithms that pit sophisticated business decision-making against the ordinary consumer's heuristic methods.[2]

A Distinctive Contribution: Extending the Consumer Definition

A distinctive contribution of VOICE's evolving framework is the extension of the traditional consumer definition to include micro and mini entrepreneurs and the self-employed. These actors, street vendors, home-based workers, gig economy participants and women's Self-Help Group members consume digital financial services and face economic, educational and social vulnerabilities comparable to individual retail consumers, yet fall outside both retail consumer protection frameworks and formal business regulation.[3]

This written contribution draws on VOICE's 43 years of consumer advocacy experience, its ground-level work with micro-entrepreneurs and women's SHGs, its formal regulatory submissions to the Reserve Bank of India in 2026, and the academic framework developed by Prof. K.V. Bhanu Murthy in his note 'A New Perspective on VOICE: Dealing with the New Age Consumer.'[4]

Executive Summary

India presents a unique and instructive case study for global consumer protection in digital financial services. Through the deliberate architecture of its digital public infrastructure — Aadhaar-based biometric identity, the Unified Payments Interface (UPI), and bank-account-to-mobile-number linkage — India has enabled large-scale digital financial participation by ordinary citizens at a speed and scale unmatched by most UNCTAD member countries. This democratisation of digital finance, while transformative, has created new and rapidly evolving consumer protection challenges. Digital fraud cases grew from 2.6 lakh in 2021 to 28 lakh in 2025, a 10-fold increase in cases and 40-fold increase in fraud value in just four years.

This paper makes four distinctive contributions to the IGE's 9th Session theme of Safe Products and Confident Consumers in the Digital Marketplace:

---

[1] Bhanu Murthy, K.V. 'A New Perspective on VOICE: Dealing with the New Age Consumer.' Academic note prepared for VOICE. Delhi Technological University. 2025.

[2] Bhanu Murthy, K.V. 'A New Perspective on VOICE: Dealing with the New Age Consumer.' The framework identifies nine new dimensions of consumer concern in the digital environment, including payment system security, data theft, algorithmic exploitation, data privacy and protection of digitally challenged consumers. Delhi Technological University. 2025.

[3] Bhanu Murthy, K.V. 'A New Perspective on VOICE: Dealing with the New Age Consumer.' The framework advocates for inclusion of micro and mini entrepreneurs and the self-employed within the ambit of consumer protection. Delhi Technological University. 2025.

First, it explains India's unique digital stack as an essential global context for UNCTAD member countries building or scaling digital payment infrastructure.

Second, it presents India's emerging regulatory framework features, including cooling-off periods, liability allocation, kill switch, trusted person authentication and alert standards, as replicable models for global adoption.

Third, it presents ground-level evidence from our formal policy advocacy submissions to the Reserve Bank of India, identifying critical consumer protection gaps with direct global relevance.

Fourth, it extends the traditional definition of consumer to include micro and mini businesses and the self-employed, particularly women's Self-Help Groups, as an under protected segment in developing economies.

1. India's Digital Stack: The Global Context

1.1 A Unique Global Architecture

India's digital payment revolution is built on a deliberate public infrastructure architecture that distinguishes it from any other economy in the world. Three interconnected systems form the foundation:

Aadhaar, a biometric digital identity system covering over 1.3 billion citizens, enables identity verification without physical documentation.

UPI (Unified Payments Interface) is the world's largest real-time payment system, processing over 13 billion transactions per month, enabling instant account-to-account transfers via mobile phone.

Bank-account-to-mobile-number linkage -enabling any citizen with a mobile phone and a bank account to send and receive money instantly, without a physical card, branch visit, or internet banking setup.

Digital transaction volumes in India have increased 38-fold over the past decade, with a compound annual growth rate of approximately 53% by volume and 13% by value. Most UNCTAD member countries do not yet have comparable infrastructure, making India's experience both instructive and cautionary for nations at earlier stages of digital payment development.

1.2 India's Emerging Regulatory Response Framework: Replicable Models for Global Adoption

India's **Reserve Bank of India (RBI)** is developing one of the world's most comprehensive digital fraud protection frameworks for a large-scale real-time payment system. Through our formal submissions to RBI, we have engaged directly with this framework and identified six

features that are directly replicable by UNCTAD member countries, building or strengthening their own consumer protection systems for digital payments.

These six features are detailed in Section 2 of this paper.

1.3 The Consumer Protection Gap

The speed of digital adoption has outpaced consumer protection frameworks. The dominant fraud typology is the Authorised Push Payment (APP) fraud, where consumers themselves initiate fraudulent transactions under social engineering, coercion, or impersonation.

The term 'authorised' here requires careful unpacking - it does not mean the consumer willingly or knowingly participated in fraud. Rather, it describes the technical fact that the consumer themselves initiated and authenticated the transaction, as opposed to a fraudster accessing the account without the consumer's knowledge.

In APP fraud, the consumer is deceived into making the payment themselves. A fraudster, posing as a bank official, a government officer, a family member in distress, or a legitimate business, creates a scenario of urgency, fear or trust that compels the consumer to transfer money. Common tactics include:

In APP fraud, the consumer is deceived into making the payment themselves. A fraudster — posing as a bank official, a government officer, a family member in distress, or a legitimate business creates a scenario of urgency, fear or trust that compels the consumer to transfer money. Common tactics include:

- Impersonation fraud - the fraudster claims to be from the consumer's bank, stating their account has been compromised, and they must immediately transfer funds to a 'safe account.'
- KYC fraud - the consumer is told their UPI or Aadhaar-linked account will be deactivated unless they complete an urgent 'verification' by sending a test payment.
- Investment fraud - the consumer is shown fabricated evidence of high returns and transfers money to what they believe is a legitimate investment platform.
- Emergency fraud - the fraudster impersonates a family member claiming to be in a medical or legal emergency requiring immediate funds.
- Deepfake fraud - increasingly, AI-generated voice or video clones of trusted individuals are used to make the deception convincing and impossible to detect.

In every case, the consumer presses the button. The consumer enters the PIN. The consumer completes the transaction. This is why it is technically 'authorised' — the payment system has no way of knowing that the consumer acted under deception rather than genuine intent.

This is precisely why APP fraud is so devastating and so difficult to address through traditional fraud frameworks. The consumer has not been hacked. Their account has not been breached. They have been psychologically manipulated into doing exactly what the fraudster needed them to do. The instantaneous settlement that makes UPI powerful

money moving in seconds, also means that by the time the consumer realises they have been deceived, the funds have already left the banking ecosystem entirely.

Digital fraud cases grew from 2.6 lakh (2021) to 28 lakh (2025), with fraud value rising from Rs. 551 crores to Rs. 22,931 crores a crisis that demands a comprehensive global policy response.

As Prof. K.V. Bhanu Murthy's New Age Consumer framework identifies, information asymmetry in the digital environment has two critical effects: adverse selection, where consumers are led to make wrong choices due to information gaps and moral hazard, where sellers pass risk to consumers who know less. APP fraud is the most acute manifestation of this asymmetry in India's high-velocity digital payment ecosystem.[5]

1.4 Our Advocacy Position

VOICE's formal submissions to RBI and this UNCTAD contribution are grounded in two clear consumer rights positions:

First — on APP fraud liability:

Social engineering that results in APP fraud must be recognised as a distinct fraud category in consumer protection frameworks. A consumer who acts under deception, fear or manufactured urgency has not genuinely 'authorised' a transaction in any meaningful legal or ethical sense. The burden of proof must shift to institutions to demonstrate that adequate, genuine and distinct warnings were provided before any consumer liability can be established.

Second — on extending consumer protection:

VOICE advocates for the inclusion of micro and mini entrepreneurs who are self-employed in the ambit of consumer protection, because they also consume digital financial services and are economically, educationally and socially vulnerable. Street vendors, home-based workers, gig economy participants and members of women's Self-Help Groups use personal digital payment accounts for business transactions exposing them to the full range of APP fraud risks with neither the protections available to retail consumers nor the resources available to formal businesses. This gap in consumer protection frameworks must be explicitly addressed in both national and international guidelines, including the UNCTAD Guidelines for Consumer Protection.

2. India's Emerging Regulatory Framework: Replicable Models for Global Adoption

India's Reserve Bank of India (RBI)is developing one of the world's most comprehensive digital fraud protection frameworks for a large-scale real-time payment system. Through our formal submissions to RBI, we have engaged directly with this framework and identified six

[5] Bhanu Murthy, K.V. 'A New Perspective on VOICE: Dealing with the New Age Consumer.' The framework analyses information asymmetry effects in digital environments: adverse selection (consumers led to wrong choices due to information gaps) and moral hazard (sellers passing risk to less-informed consumers). Delhi Technological University. 2025.

features that are directly replicable by UNCTAD member countries, building or strengthening their own consumer protection systems for digital payments.

2.1 Cooling-Off Period — A Model for Disrupting Social Engineering

What RBI Proposes:

A mandatory 1-hour lag for transactions above Rs. 10,000 to new beneficiaries, with the consumer retaining the right to cancel during this window.

Our Advocacy Position:

We support this strongly and recommend extending to 2-4 hours for high-value transactions. The one-hour window aligns with the 'golden hour' principle in fraud risk management.

Global Relevance for UNCTAD Member States:

The entire machinery of phone-based payment fraud is built on one weapon - speed. A cooling-off period is a direct attack on this mechanism.

UK allows banks to delay suspicious outbound payments by up to 72 hours. Singapore requires a 12-hour pause on high-risk account actions. India's 1-hour model is calibrated for high-volume real-time payment systems.

Any nation building instant payment infrastructure should adopt this as a baseline consumer protection requirement from day one.

Threshold of Rs. 10,000 captures approximately 98.5% of total fraud value while keeping everyday small transactions frictionless.

2.2 Customer Liability Framework — Shared Responsibility Model

What RBI Proposes:

Clear allocation of liability between the consumer, bank, and payment operator based on where the failure occurred. The framework distinguishes between unauthorised transactions (the bank's fault), transactions involving third-party breach, and consumer negligence.

Our Advocacy Position:

We support the shared responsibility model but urge that 'consumer negligence' be defined narrowly and specifically, with the burden of proof on the bank to demonstrate that adequate, distinct consumer warnings were issued before shifting liability.

Global Relevance for UNCTAD Member States:

Most developing nations have no formal liability allocation framework for digital payment fraud. Consumers bear 100% of losses by default.

India's tiered liability model, distinguishing between bank negligence, third-party breach, and consumer negligence, is a template that any nation designing consumer protection law for digital payments can adopt.

The framework's recognition that social engineering does not automatically constitute consumer negligence is a landmark consumer protection principle with global significance.

2.3 Loss Compensation Mechanism - A Starting Point for Developing Nations

What RBI Proposes:

Bona fide fraud victims are compensated up to Rs. 25,000 currently, with a lifetime restriction.

Our Advocacy Position:

We recommend replacing the lifetime restriction with a rolling 3-year reset. A consumer victimised by a SIM swap attack in 2026 should not be permanently barred from protection against a deepfake fraud in 2030. These are different crimes using different technologies.

Global Relevance for UNCTAD Member States:

India is establishing the first formal compensation mechanism for APP fraud in a large developing economy, a model other nation can build upon.

The rolling reset principle is universally applicable: any compensation framework designed before the era of deepfakes, AI voice cloning, and SIM swaps needs to be future-proofed with reset mechanisms rather than lifetime caps.

Nations designing digital fraud compensation funds should build in automatic review cycles tied to the evolution of fraud technology.

2.4 Kill Switch - Consumer-Controlled Emergency Protection

What RBI Proposes:

A single consumer-controlled facility to instantly disable all digital payment transactions from an account. operable via mobile banking or a bank branch. Kill switch activation overrides all other configurations.

Our Advocacy Position:

We strongly support the kill switch and recommend that reactivation be possible through both digital channels (with enhanced biometric verification) and physical branch visits — ensuring accessibility for rural and elderly consumers who may not have reliable digital access.

Global Relevance for UNCTAD Member States:

The kill switch converts the consumer from a passive fraud victim to an active protector of their own financial safety, a fundamental shift in the consumer-bank power dynamic.

Singapore's implementation validates this model. India's implementation at the UPI scale — with 13 billion monthly transactions will be the largest real-world test of consumer-controlled digital payment protection.

Any nation deploying mobile-first payment systems should build kill switch functionality into the baseline infrastructure design, not as an afterthought.

2.5 Trusted Person Authentication — Protecting Vulnerable Consumers

What RBI Proposes:

Mandatory trusted person authentication for transactions above Rs. 50,000 for citizens aged 70+ and differently-abled consumers. The trusted person acts as an additional authentication layer, not a decision maker.

Our Advocacy Position:
We support this framework and recommend lowering the age threshold to 65+, given evidence that fraud victimisation peaks in the 55-70 age group. We also recommend making the threshold Rs. 25,000 for this vulnerable segment, since even smaller fraud amounts can be catastrophic for consumers on fixed pensions.
Global Relevance for UNCTAD Member States:
India is developing the first formal regulatory framework that explicitly recognises elderly and differently-abled consumers as a protected category requiring enhanced protection in digital payment systems.
Nations with ageing populations entering digital finance — a near-universal trend — can adopt this framework directly.
The trusted person model is replicable even in nations without sophisticated digital infrastructure, requiring only phone-based authentication as a minimum.

2.6 Alert Standards — Defining Adequate Consumer Warning

What RBI Proposes:
Specific warnings are required from banks before consumer liability can be established for failing to heed fraud warnings.

Our Advocacy Position:
We recommend that 'specific warnings' be legally defined as distinct, non-routine, and intrusive alerts, colour-coded haptic pop-ups within banking applications, or mandatory IVR confirmation calls rather than standard SMS messages that are indistinguishable from promotional content. A warning buried in marketing noise is not a warning; it is compliance theatre.

Global Relevance for UNCTAD Member States:
Alert fatigue is a universal phenomenon in all digital banking markets not unique to India. Any nation that allows banks to shift liability based on 'standard warnings' creates a systematic injustice for consumers.

India's framework, if amended as we recommend, would establish minimum standards for what constitutes adequate consumer warning, applicable globally.

UNCTAD should consider adopting alert quality standards as part of its Guidelines for Consumer Protection.

2.7 Summary: India's Framework Features vs Global Standards
The following table summarises India's emerging framework features and their international comparators, providing UNCTAD member states with a reference model for adoption:

Framework Feature	India (RBI Proposal)	Our Recommendation	International Comparator
Cooling-Off Period	1 hour for transactions above Rs. 10,000 to new payees	2-4 hours; 24-hour waiting for new whitelist additions	UK: 72 hrs | Singapore: 12 hrs | Sweden: Variable

Liability Allocation	Tiered liability — bank, third party, consumer based on fault	Narrow definition of consumer negligence; burden of proof on bank	EU PSD2 | UK PSR 2024
Loss Compensation	Rs. 25,000 with lifetime restriction	Rolling 3-year reset replacing lifetime cap	No direct comparator — India leading
Kill Switch	Single facility to disable all digital payments	Digital + physical reactivation options for rural/elderly access	Singapore EASF | Australia digital padlock
Trusted Person Auth	Mandatory for 70+ and PwD above Rs. 50,000	Extend to 65+; lower threshold to Rs. 25,000	Ireland trusted contact | USA trusted contact
Alert Standards	Specific warnings required before liability shifts	Distinct intrusive alerts (haptic/IVR) — not standard SMS	No global standard yet — India can lead

3. Consumer Protection Gaps: Evidence from Our Policy Advocacy

Our organisation submitted formal comments to the Reserve Bank of India in April and May 2026 on two significant regulatory frameworks: the Draft Directions on Limiting Customer Liability in Digital Fraud and the Discussion Paper on Safeguards in Digital Payments. Our submissions identified four critical consumer protection gaps with direct global relevance.

3.1 Social Engineering and the 'Authorised Transaction' Fiction

India's regulatory draft classifies a transaction as 'authorised' even when the consumer was tricked into sending money to a scammer. Our position is clear: a consumer who acts under deception, fear, or manufactured urgency has not genuinely authorised a transaction. Social engineering must be recognised as a distinct fraud category not absorbed into the 'authorised payment' definition. This principle is universally applicable to any digital payment system.

3.2 Alert Fatigue — Unjust Liability Shift to Consumers

Banks send consumers dozens of SMS messages per week — transaction alerts, promotional offers, loan reminders. When a fraud warning arrives in this format, under active psychological pressure from a fraudster, consumers cannot reasonably be expected to parse the difference. The standard SMS warning does not constitute a 'specific, directed and clear warning' sufficient to shift 100% liability to the consumer.

3.3 Five-Day Reporting Window — Systematically Excluding the Vulnerable

A fixed 5-day reporting window from the date of fraud occurrence systematically excludes senior citizens, rural populations, and low-connectivity consumers who may not discover the fraud within this period. The reporting window must be triggered from the 'Date of Discovery' when the consumer first receives confirmation of the transaction not the date of occurrence.

3.4 Compensation Cap — Technologically Obsolete

A Rs. 25,000 lifetime compensation cap designed before the era of deepfakes and AI voice cloning is already obsolete. Fraud tactics evolve rapidly — a consumer victimised by a SIM swap in 2026 should not be permanently barred from protection against a deepfake fraud in 2030. We recommend a rolling 3-year reset mechanism that keeps the safety net relevant as technology evolves.

4. Consumer Risks Embedded in Fintech Product Design

Consumer protection in digital financial services cannot be limited to fraud prevention. The design of fintech products itself creates systematic consumer risks through heuristic exploitation, shrouded attributes, data opacity, and the erosion of financial literacy. These are not accidental design choices — they are deliberate applications of behavioural economics in the service of profit rather than consumer welfare.[6]

- **Heuristic Exploitation:** Pre-selected defaults, artificial urgency, and friction-based dark patterns systematically drive consumers toward choices serving business interests over their own welfare.

- **Shrouded Attributes:** Hidden fees, flat-rate rather than effective annual rate disclosure, and credence goods systematically exploit the information asymmetry between fintech companies and consumers.

- **Data Rights Erosion:** Consumer transaction data is claimed by platforms; opaque third-party sharing proceeds without meaningful consent or control.

- **Financial Literacy Decline:** Automation reduces understanding; robo-advisors create dependency; chatbot dead-ends leave consumers without meaningful recourse when problems arise.

5. Extending Consumer Protection to Micro Businesses and Women's SHGs

Traditional consumer protection frameworks focus on individual retail consumers. India's digital payment ecosystem has created a significant and under-protected category: micro and mini businesses, sole proprietors, self-employed individuals, and informal sector entrepreneurs who operate as businesses in practice yet use personal financial accounts. Women's Self-Help Groups (SHGs) represent a particularly important case. These groups operate as collective financial entities using personal member accounts. Digital financial inclusion of SHGs has outpaced digital safety literacy — groups that have transitioned to digital transactions often lack the knowledge to protect themselves against fraud, understand their rights, or access redressal mechanisms.

[6] Bhanu Murthy, K.V. 'A New Perspective on VOICE: Dealing with the New Age Consumer.' The framework identifies heuristic exploitation, shrouded attributes, data opacity and erosion of financial literacy as deliberate consumer risk mechanisms in fintech product design. Delhi Technological University. 2025.

We recommend that UNCTAD Guidelines for Consumer Protection explicitly recognise micro and mini businesses, sole proprietors, and self-employed individuals as a protected consumer category in digital financial services.

6. Policy Recommendations for UNCTAD Member States

6.1 For Nations Building Digital Payment Infrastructure

- Build consumer protection frameworks simultaneously with payment infrastructure, not retrofitted after adoption.

- Adopt India's six framework features cooling-off period, liability allocation, compensation mechanism, kill switch, trusted person authentication, and alert standards as a baseline consumer protection package.

- Adopt the 'Secure by Default' principle for all new digital payment accounts.
- Mandate digital literacy as a mandatory component of financial inclusion programs.

6.2 For Global Consumer Protection Standards

Recognise APP fraud and social engineering as a distinct category within international consumer protection frameworks, not a subcategory of 'authorised payment'.

• Adopt cooling-off periods for high-value transfers as an international standard for real-time payment systems.
• Replace static lifetime compensation caps with rolling reset mechanisms aligned with technology evolution cycles.
• Establish minimum alert quality standards, intrusive, distinct, and non-routine, before consumer liability can be imposed.
• Explicitly extend consumer protection to micro businesses, self-employed individuals, and women's SHGs in the UNCTAD Guidelines.

6.3 For Fintech Product Regulation

- Prohibit interface design that systematically exploits cognitive biases as an unfair commercial practice.
- Establish clear consumer data ownership: transaction data belongs to the consumer, not the platform.
- Mandate human-staffed complaint and dispute resolution in regional languages, not chatbot dead-ends.

7. Conclusion

India's digital payment revolution offers the world's most comprehensive real-world laboratory for understanding both the potential and the risks of large-scale digital financial inclusion. The six framework features India is developing — cooling-off periods, liability allocation, compensation mechanisms, kill switch, trusted person authentication, and alert standards represent a complete consumer protection package that UNCTAD member countries can adopt, adapt, and build upon.

The consumer protection challenges India faces today APP fraud, social engineering, alert fatigue, and compensation frameworks unfit for the AI era, are the challenges every digitising economy will face tomorrow. What India builds now matters for the world. *Safe consumers are confident consumers. Confident consumers are the foundation of a trustworthy digital economy for India, and for the world.*

References

Reserve Bank of India (2025). Discussion Paper: Exploring Safeguards in Digital Payments to Curb Frauds. Department of Payment and Settlement Systems.

VOICE (2026). Formal Comments on RBI Discussion Paper on Digital Payment Safeguards. April 2026.

VOICE 2026). Feedback on RBI Draft Directions on Limiting Customer Liability in Digital Fraud. April 2026.

National Cyber Crime Reporting Portal (NCRP), India. Annual Data on Digital Payment Fraud. 2021–2025.

Payment Services (Amendment) Regulations 2024, United Kingdom.

Monetary Authority of Singapore (2024). Enhanced Anti-Scam Framework and Shared Responsibility Framework.

Bhanu Murthy, K.V.(Former Dean, Faculty of Commerce and Business, Delhi School of Economics, Special Appointee, Professor, Delhi Technological University.
& Governing Council Member, Consumer VOICE, India Fintech and The Consumer
UNCTAD Guidelines for Consumer Protection (2016 Revision). United Nations.