Remedies for digital payment frauds

KEEPING VIGIL. Static safeguards, targeting discrete acts of fraud, will only spur fraudsters to probe other vulnerabilities

GETTYIMAGES/ISTOCKPHOTO

BENI CHUGH
SARADA MAHESH

The recent rise in fraud in the financial ecosystem is a cause for concern. The RBI's 'Report on Trends and Progress of Banking in India', notes that the value of fraudulent activities in banking operations has risen from ₹11,261 crore in 2023-24 to ₹34,771 crore in 2024-25.

Apart from the obvious monetary losses, frauds cause a crisis of confidence and trust among customers that threatens the momentum of financial inclusion and the growth of the sector.

Considering these drastic and cascading effects of frauds, the RBI is deliberating important policy interventions to address frauds in digital payments.

First, the RBI's draft framework on limiting customer liability in digital transactions ("liability framework") recognises authorised push payments (APP) as a customer risk and proposes a redress mechanism for it. APPs comprise payment transactions that the customer may have authorised willingly but unintentionally.

This includes social engineering ploys where fraudsters manipulate customers to either share transaction credentials enabling the fraudster to transfer monetary sums to themselves or directly transfer monetary sums to the fraudster. The liability framework proposes a one-time compensation of up to ₹25,000 or 80 per cent of the transaction value for victims of low-value APP fraud.

Further, the compensation is conceived as a low-burden mechanism, a de facto guarantee to remedy bona fide APP losses of up to ₹50,000.

Interestingly, this compensation is dispensed by the financial system. Banks vet complaints, establish their veracity and the RBI offers the compensation. It may reduce the proclivity of the customers to approach the legal system to seek redress for low-value APP fraud, thus, shielding the legal system from becoming overwhelmed by low-value, high-volume complaints that are expensive to investigate.

The one-time compensation, though illustrative of the central bank's resolve to make good to victims, does not offer any enduring solution for the customer who gets defrauded repeatedly. Its low-effort nature also does not have the effect of disciplining the customer by accounting for their role in enabling the fraud, which is characteristic of a good remedial measure. In addition to providing a remedy for APP frauds, the RBI has also proposed preventative safeguards to curb APP fraud. The RBI's discussion paper titled 'Exploring safeguards in digital payments to curb frauds' suggests four such measures: a lag in fulfilment of transactions above ₹10,000; an additional authentication system of trusted persons for older customers; commensuration of credit to accounts based on a relationship of trust established with the bank; and a customer-led kill-switch for digital payments.

Chase system-level resilience instead of individual fraud categories. This requires diverse financial and non-financial actors such as telecom operators and e-commerce entities to work together

These safeguards underline the RBI's 'stop and think' approach, encouraging customers to pause and reconsider the riskiness of the transaction at hand.

However, the application of these interventions is anchored in static demographic categories of age, physical condition or the sophistication of the remitter. These indicators alone may not be useful for detecting fraud.

RECHARACTERISING THE ISSUE OF FRAUD

Conventionally, fraud has been characterised as a static issue where bad actors exploit the gaps in the system and/or use their comparative operational advantage to cheat people out of money. Typically, static systems do not learn from or react to changes in the environment in which they operate.

However, fraudsters are known to improvise in response to policy developments. If policies make it difficult for fraudsters to cheat 70-year-old citizens, they will focus on the 68-year-olds. Put simply, static preventative safeguards do not terminate frauds, they only incentivise the fraudster to identify other exploitable vulnerabilities. This ever-evolving nature of fraud offers four lessons for designing fraud prevention policies:

First, static rules will be gamed. Fraud prevention needs to be reimagined as a system of continuous recalibration instead of a system rooted in 'static' customer risk profiles. For instance, AI & ML tools can gauge the riskiness of a transaction by combining real-time, user-centric indicators such as recent account activity, device information and user behaviour patterns with aggregate patterns like emerging geographical hotspots, complaints and network traffic. Such assessments can detect fraud better than KYC-based risk profiles.

Second, chase system-level resilience instead of individual fraud categories. This requires diverse financial and non-financial actors such as telecom operators and e-commerce entities to continually work together to identify emerging frauds and close gaps in the system.

Third, defend at scale. This can be supported by building tools to continuously gather, harvest and share intelligence across the diverse stakeholders and using AI to build detective and predictive capabilities.

Finally, design adaptive policy interventions. Interventions should automatically recede from use when obsolete forms of fraud no longer pose active customer risk and vice versa.

RBI initiatives such as the Digital Payments Intelligence Platform, already embody some of these characteristics. It remains unclear where such initiatives sit alongside the remedial and preventative measures being discussed in the current policy proposals. Absent such clarity, it would appear that policies that seek to tackle discrete instances of fraud, such as the measures that have been just announced, may have limited effectiveness.

Chugh is Head - Future of Finance; Mahesh is Senior Research Associate, Dvara Research