GOVERNMENT OF INDIA
MINISTRY OF FINANCE
DEPARTMENT OF FINANCIAL SERVICES

RAJYA SABHA
STARRED QUESTION NO. *120
ANSWERED ON TUESDAY, 10 FEBRUARY 2026/21 MAGHA 14, 1947 (SAKA)

DIGITAL PAYMENTS AND SYSTEMIC RISK

*120. SHRI G.C. CHANDRASHEKHAR:

Will the Minister of FINANCE be pleased to state:

a. whether Government has analysed systemic concentration, operational risks and fraud exposure in digital payment platforms amid rising transaction volumes; and
b. the regulatory safeguards introduced to ensure resilience, competition and consumer protection?

ANSWER

THE MINISTER OF FINANCE
(SMT. NIRMALA SITHARAMAN)

(a) and (b): A statement is laid on the Table of the House.

*****

STATEMENT REFERRED TO IN REPLY TO PART (a) AND (b) OF RAJYA SABHA STARRED QUESTION NO. 120 FOR 10 FEBRUARY, 2026, REGARDING "DIGITAL PAYMENTS AND SYSTEMIC RISK" TABLED BY SHRI G.C. CHANDRASHEKHAR, HON'BLE MEMBER OF PARLIAMENT

(a): The digital payment transactions in the country have grown exponentially from 2,071 crore in FY 2017-18 to 22,831 crore in FY 2024-25, registering a compound annual growth rate (CAGR) of 41%. These transactions have been facilitated through various modes/platforms such as Unified Payments Interface (UPI), card networks (Credit Card/Debit Card), internet banking, Real Time Gross Settlement (RTGS), Immediate Payment Service (IMPS), Aadhaar Enabled Payment System (AePS) etc. The Government, Reserve Bank of India (RBI) and National Payments Corporation of India (NPCI) have been regularly reviewing the growth of digital payments and the risks associated with the digital payment platforms. From the review, it has been noted that, of the total digital payment transactions in FY 2024-25, UPI constitutes around 81% of the transaction volume. The UPI platform is based on an open and interoperable protocol which is enterprise agnostic, allowing all the ecosystem players to participate equally. Presently, the UPI platform connects 685 banks and 40 non-banks as Third-Party App Providers (TPAPs). However, the majority of the transactions are made through a few TPAPs, as preferred by the end users/customers.

NPCI has informed that they have noted some of the operational risks such as peak-hour congestion, API failures, member-side downtime, etc., and appropriate advisories have been issued to the banks and TPAPs from time to time. Banks and TPAPs have also been advised to conduct regular compliance and system checks to ensure continuity of services to the end users. Further, with the increase in digital payments, the incidence of frauds has also gone up in the recent years. However, NPCI has implemented several measures including device binding, two-factor authentication, transaction limits, real-time Al-based fraud risk monitoring, enhanced API-level information sharing, and in-app safety alerts.

(b): The Government, RBI and NPCI have been taking up regulatory and supervisory measures to ensure operational resilience, fraud prevention and consumer protection. These inter alia, include the following:

- RBI has issued the Cyber Security Framework for Banks (2016) and for Urban Cooperative Banks (2018); the Master Direction on IT Governance, Risk, Controls and Assurance Practices (2023); the Master Direction on Outsourcing of IT Services (2023), the Guidelines on Storage of Payment System Data (2018); the Master Directions on Digital Payments Security Controls (2021) and the Master Directions on Fraud Risk Management (July 2024).
- RBI has also issued advisories on money mule activities in November 2024 and launched MuleHunter.AI in December 2024 to identify and monitor suspected money mule accounts.
- Banks and financial institutions have strengthened their fraud-risk frameworks by deploying advanced automated monitoring tools, including Enterprise Fraud Risk Management Systems (eFRMS), scenario-based transaction analysis, and AI/ML-driven anomaly detection, supported by enhanced due diligence processes and structured staff training programmes.
- In order to facilitate citizens to report cyber frauds, including financial frauds, the Ministry of Home Affairs has launched the National Cyber Crime Reporting Portal "www.cybercrime.gov.in" as well as National cybercrime helpline number "1930". The Department of Telecommunications has launched

the Digital Intelligence Platform (DIP) and the ‘Chakshu’ portal to report suspected mobile numbers associated with cyber frauds.

- RBI and Banks have been taking up awareness campaigns through short SMS, radio campaign, publicity on prevention of cybercrime. Further, RBI has been conducting electronic-banking awareness and training (e-BAAT) programmes which focuses on awareness about frauds and risk mitigation.
- NPCI has also undertaken digital payment safety awareness programs, including UPI security campaigns, appointment of Safety Brand Ambassadors and offline training in 48 villages across six states (West Bengal, Odisha, Bihar, Punjab, Haryana and Assam).

*****