GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION No. 629
TO BE ANSWERED ON: 01.12.2021

DIGITAL PAYMENT

629: SHRI SUMEDHANAND SARASWATI :

Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:

(a) whether the number of digital payments have increased substantially after promoting the same in the country and if so, the details thereof along with the number of digital payments conducted during each of the last three years, State-wise;
(b) whether the Government has undertaken any comparative study with regards to other countries in terms of digital payments and if so, the details of such countries along with the outcomes of the study thereof; and
(c) whether the Government has taken adequate steps for safety and security of various digital platforms at present in the country and if so, the details thereof?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY (SHRI RAJEEV CHANDRASEKHAR)

(a): Yes, Sir. Digital Payments transactions have been steadily increasing since last few years. Over the past four years digital payment transactions have grown multifold from 1004 Cr in FY 2016-17 to 5554 Cr in FY 2020-21. State/UT-wise transaction details are not maintained. The total number of digital payments undertaken in the country during the last three years and current year is as under:

Financial Year (FY)	**Total number of Digital Transactions (In Crore)**
FY 2018-19	3134
FY 2019-20	4572
FY 2020-21	5554
FY 2021-22(till mid November)*	4683

* Data for October & November, 2021 is provisional

(b): The Reserve Bank of India (RBI) has released a report on “Benchmarking India’s Payment Systems”, which provides a comparative position of the payment system ecosystem in India relative to comparable payment systems and usage trends in other major countries

(URL:https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/BIPS04062019CE3C72E9873244ED8BAAE9C8FC5955A8.PDF.

The study found that India has a strong regulatory system and robust large value and retail payment systems that have contributed to the rapid growth in the volume of transactions in these payment systems. There has been a substantial growth in e-payments by Government and also in digital infrastructure in terms of mobile networks. The report emphasises the need to undertake further efforts to bring down the volume of paper clearing and increase acceptance infrastructure to enhance digital payments in India.

(c): The Government has undertaken several steps to ensure safety and security of various digital platforms. The following are the details:

Steps taken by CERT-In (Indian Computer Emergency Response Team):

i. Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis to ensure safe usage of digital technologies. CERT-In has issued 68 advisories for organisations and users for data security and mitigating fraudulent activities.

ii. CERT-In works in coordination with service providers, regulators and Law Enforcement Agencies (LEAs) to track and disable phishing websites and facilitate investigation of fraudulent activities.

iii. Security tips have been published for users to secure their Desktops, mobile/smart phones and preventing phishing attacks.

iv. All authorised entities/ banks issuing PPIs in the country have been advised by CERT-In through Reserve Bank of India to carry out special audit by empanelled auditors of CERT-In on a priority basis and to take immediate steps thereafter to comply with the findings of the audit report and ensure implementation of security best practices.

v. Government has issued guidelines for Chief Information Security Officers (CISOs) regarding their key roles and responsibilities for securing applications / infrastructure and compliance.

vi. CERT-In has empanelled 96 security auditing organisations to support and audit implementation of Information Security Best Practices.

vii. Cyber security mock drills are conducted regularly to enable assessment of cyber security posture and preparedness of organisations in Government and critical sectors. 61 such drills have so far been conducted by CERT-In, wherein 600 organisations from different States and sectorsparticipated.

viii. CERT-In conducts regular training programmes for network / system administrators and Chief Information Security Officers (CISOs) of Government and critical sector organisations regarding securing the IT infrastructure and mitigating cyber attacks. 15 and 17 training programmes were conducted covering 708 and 4801 participants during the year 2020 and 2021 (till October 2021) respectively.

ix. CERT-In has set up the National Cyber Coordination Centre (NCCC) to generate necessary situational awareness of existing and potential cyber security threats. Phase-I of NCCC is operational.

x. CERT-In operates the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre). The centre provides detection of malicious programs and free tools to remove the same for citizens and organisations.

xi. CERT-In provides the requisite leadership for the Computer Security Incident Response Team-Finance Sector (CSIRT-Fin) operations under its umbrella for responding to, containment and mitigation of cyber security incidents reported from the financial sector.

xii. CSIRT-Fin, CERT-In, National Institute of Securities Markets (NISM) and Centre for Development of Advanced Computing (CDAC) conducting a self-paced 60 hour certification program on "Cyber Security Foundation Course" for professionals in financial sector.

xiii. Ministry of Electronics & Information Technology (MeitY) conducts programmes to generate information security awareness. Specific books, videos and online materials are developed for children, parents and general users about information security which are disseminated through portals like "www.infosecawareness.in", and "www.cyberswachhtakendra.gov.in".

Steps taken by RBI (Reserve Bank of India):

Reserve Bank of India (RBI) has taken various steps to enhance security of digital payment transactions (including card transactions) and reduce frauds. These also include various benefits (in terms of increased safety of transaction, efficiency in grievance redressal mechanism, etc.) being provided to customers. Following are the broad measures taken by RBI:

a. It is mandatory to put in place a system of providing for additional authentication / validation based on information not visible on the cards for all on-line card not present transactions. In case of customer complaint regarding issues, if any, arising out of transactions effected without the Additional Factor of Authentication (AFA), the issuer bank shall reimburse the loss to the customer further without demur.
b. The mandate for additional authentication / validation shall apply to all transactions using cards issued in India
c. Card networks have been advised to ensure mandatory PIN authentication for all transactions performed using credit, debit and prepaid cards – magnetic stripe or EMV Chip and PIN based.
d. Banks have been advised to put a system in place of online alerts for all types of transactions irrespective of the amount, involving usage of cards at various channels
e. At the time of issue / re-issue, all cards (physical and virtual) shall be enabled for use only at contact based points of usage [viz. ATMs and PoS devices] within India. Issuers shall provide cardholders a facility for enabling card not present (domestic and international) transactions, card present (international) transactions and contactless transactions.
f. All new cards issued – debit and credit, domestic and international – by banks shall be EMV Chip and PIN based cards

g. Instructions have been issued to limit the liability of customers in case of unauthorised electronic payment transactions resulting in debit to PPIs issued by banks and authorised non-banks.
h. PPI (Pre Paid Instruments) shall establish a mechanism for monitoring, handling and follow-up of cyber security incidents and cyber security breaches. The same shall be reported immediately to DPSS, Central Office, RBI, Mumbai. It shall also be reported to CERT-IN as per the details notified by CERT-IN.
i. Banks have been advised to put in place appropriate risk mitigation measures like transaction limit, transaction velocity limit, fraud checks and others depending on the bank's own risk perception, unless otherwise mandated by the RBI.
j. All mobile banking transactions involving debit to the account shall be permitted only by validation through a two-factor authentication (2FA). One of the factors of authentication shall be mPIN or any higher standard.

****