GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION No. 1778
TO BE ANSWERED ON 21.09.2020

DIGITAL PAYMENTS

1778: SHRI B.B.PATIL:

Will the Minister of Electronics and Information Technology be pleased to state:

(a) whether the number of digital payments in the country has increased significantly due to Covid-19 and if so, the details thereof;
(b) the number of digital payments made during each of the last three years and the current year, State/UT-wise;
(c) whether the Government has conducted any comparative study with regard to digital payments in other countries;
(d) if so, the details and the outcome thereof;
(e) whether appropriate steps have been taken by the Government for security and safety of various platforms for digital transactions in the country; and
(f) if so, the details thereof and if not, the reasons therefor?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI SANJAY DHOTRE)

(a): Yes, Sir. In the wake of COVID-19 pandemic, digital payments have increased as people are adopting more digital payments as these are easy, convenient and safe and enable a contactless mode of payment. That there was an overall dip in digital payments in April & May 2020 as compared to March 2020 due to imposition of lockdown as a measure the contain the spread of the pandemic. Thereafter digital payments have witnessed an increase with unlock since June 2020. The volume of monthly digital payment transactions in the year 2020 are mentioned in the table below:

Month	**Volume of Digital Transactions(In Crore).**
January'2020	435.88
February'2020	410.73
March'2020	414.90
April'2020	306.47
May'2020	329.22
June'2020	412.14

July'2020*	396.48
August'2020*	400.82

*Final data for July and August 2020 has not yet been published by RBI

(b): 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 2017-18	2071
FY 2018-19	3134
FY 2019-20	4572
FY 2020-21(till August)*	1634.92

* Final data for July and August 2020 has not yet been published by RBI

(c) and (d): 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 (ref. URL: https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=47222 for Press Release dated 04.06.2019 by RBI and aforesaid report).

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, however, notes that India is required to take further efforts to bring down the volume of paper clearing and increase acceptance infrastructure to enhance digital payments.

(e) and (f): The government has undertaken the following measures to enhance the cyber security posture of digital payment systems in the country:

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

i. CERT-In issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis to ensure safe usage of digital technologies. Regarding securing digital payments, 37 advisories have been issued for users and institutions.

ii. 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.

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

iv. All the Government websites and applications are required to be audited with respect to cyber security prior to their hosting. The auditing of the websites and applications are required to be conducted on a regular basis after hosting also.

v. Government has empanelled 90 security auditing organizations to support and audit implementation of Information Security Best Practices.

vi. Government has formulated Crisis Management Plan for countering cyber attacks and cyber terrorism for implementation by all Ministries/ Departments of Central Government, State Governments and their organizations and critical sectors.

vii. Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors. 49 such drills have so far been conducted by CERT-In where 434 organizations from different States and sectors, such as, Finance, Defence, Power, Telecom, Transport, Energy, Space, IT/ITeS, etc participated. Out of these drills, 11 drills were conducted in coordination with the Reserve Bank of India and The Institute for Development and Research in Banking Technology for financial sector organizations.

viii. CERT-In conducts regular training programmes for network / system administrators and Chief Information Security Officers (CISOs) of Government and critical sector organizations regarding securing the IT infrastructure and mitigating cyber attacks.

ix. The Government has launched the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre). The centre is providing detection of malicious programmes and free tools to remove the same.

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

Steps taken by RBI (Reserve Bank of India):

xi. RBI has set up a Cyber Security and IT Examination (CSITE) Cell within its Department of Supervision in 2015. A comprehensive circular on Cyber Security Framework in Banks issued on June 2, 2016 covers best practices pertaining to various aspects of cyber security.

xii. RBI has also set up a Cyber Crisis Management Group to address any major incidents reported including suggesting ways to respond. RBI also conducts cyber security preparedness testing among banks on the basis of hypothetical scenarios with the help of CERT-In. RBI carries out IT Examination of banks separately from the regular financial examination of the banks since 2015 to assess their cyber resilience evaluate the processes implemented by banks for security checks like VA/PT etc. and their follow up action.

xiii. In October 2018, RBI prescribed a set of baseline cyber security controls for Urban cooperative banks (UCBs). To further strengthen the cyber security resilience of the UCBs, a comprehensive cyber security framework was issued on December 31, 2019.

xiv. RBI has also issued circular on Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions dated July 17,2017.

xv. In total, since March 2020, RBI issued more than 18 advisories/alerts to the supervised entities on various cyber threats and best practices to be adopted. Some of them were issued in close coordination with CERT-In.

Steps taken by NPCI (National Payments Corporation of India):

xvi. NPCI has put in place a mechanism through its Board-level Risk Management Committee (RMC) and it monitors and reviews risk management and cyber security of the Company on a regular basis.

xvii. NPCI has adopted a layered approach of Prevent, Detect & Respond towards addressing Cyber Threats. The cyber security risk management extends all 3 layers with various teams undertaking activities tasked according to the state of the risk encountered.

xviii. As part of its Software Development Lifecycle, security assessments for NPCI's infrastructure are carried out regularly to identify and fix vulnerabilities. Deviations from processes are also tracked separately. In addition, it is required that security coding practices and data privacy measures are in line with the compliance standards to ensure maximum security of various in-house applications developed by NPCI.

xix. NPCI conducts periodic Phishing simulation exercises on its employees to ascertain their ability to identify such attacks and not fall prey to such attacks. NPCI has recently on-boarded a Central Threat Intelligence platform and have started sharing the information on Cyber threats and relevant IOC's to the member banks that participate in NPCI's digital ecosystem.

****