GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 3222
TO BE ANSWERED ON 23.03.2022

INCREASE IN DIGITAL PAYMENTS

3222 SHRI ACHYUTANANDA SAMANTA:

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

(a) whether digital payments in the country have been rising year after year, mainly after the pandemic since more people have been forced to transact digitally and if so, the details thereof;
(b) whether this has led to a possibility of increased security breaches and possibility of individuals being scammed;
(c) if so, the details thereof?
(d) whether the Government is taking enough steps to educate and protect citizens, especially the elder or lesser educated sections of society; and
(e)if so, the details thereof and if not, the reasons therefor?

ANSWER

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

(a): Yes, Sir. Digital Payments transactions have been steadily increasing over last few years, as a part of Government of India's strategy to digitise the financial sector and economy. Over the past four years, digital payment transactions have grown multifold from 3,134 crore in FY 2018-19 to 5,554 crore in FY 2020-21. During current financial year ie FY 2021-22, the total number of 7422 crore digital transactions have been reported till 28th February, 2022. Bharat Interface for Money-Unified Payments Interface (BHIM-UPI) has emerged as the preferred payment mode of the citizens and has achieved a record of 452.75 crore digital payment transactions with the value of Rs 8.27 lakh crore till 28th February 2022. Covid-19 pandemic has established that digital payments enable access to healthcare as well through contactless payment modes like BHIM-UPI QR code in consonance with the "new normal" of social distancing.

(b) and (c): No, Sir. Reserve Bank of India (RBI), in exercise of the powers conferred by the Banking Regulation Act, 1949, the Reserve Bank of India Act, 1934 and Payment and Settlement Systems Act, 2007, has issued the Master directions, namely, Reserve Bank of India (Digital Payment Security Controls) directions, 2021 to the Regulated entities (REs) including Scheduled Commercial Banks, Small Finance Banks, Payment Banks and Credit Card issuing NBFC (Non Banking Financial Company. Further, digital payments are enabled through multi-factor authentication. The key objectives of multi-factor authentication are to protect the confidentiality of payment data as well as enhance confidence in digital payment by combating various cyber-attack mechanisms, like, phishing, keylogging, spyware/ malware and other internet-based frauds targeted at

REs and their customers. A strong grievance redressal mechanism has been set up by the Government and RBI to address the grievances related to cyber financial frauds of the individuals, in a time bound manner.

Further, the Government of India as well as RBI have undertaken several steps to ensure safety and security of digital payments. The steps taken by the Government are placed at **Annexure-I** and the steps taken by RBI are placed at **Annexure-II.**

(d) and (e): Government in coordination with ecosystem partners are taking various initiatives for awareness of citizens for secure payment practices. Some of the steps taken are given below:

1. Initiatives of Ministry of Electronics & Information Technology

a. Pradhan MantriGramin Digital SakshartaAbhiyan (PMGDISHA):Ministry of Electronics & IT **(**MeitY) has undertaken "Pradhan MantriGramin Digital SakshartaAbhiyan (PMGDISHA)" to usher in digital literacy in rural India by covering 6 crore rural households (one person per household) by 31.03.2023.

b. MeitY advised all Banks and Payment Service Providers to undertake awareness campaigns for promotion of secure payment practices and generate information security awareness. Materials are disseminated through portals - "www.infosecawareness.in", "www.cyberswachhtakendra.gov.in".

2. Awareness initiatives by RBI:

- RBI conducted Financial Literacy Week (FLW) between February 14-18, 2022 with the theme "Go Digital, Go Secure" for creating awareness about (a) Convenience of digital transactions; (b) Security of digital transactions; and (c) Protection of customers.
- RBI has advised Banks to conduct special camps through their Financial Literacy Centres (FLCs) and tailored camps for different target groups on banking, investment products suitable for post- retirement life, estate planning tools, bank operations for old/sick/incapacitated persons, awareness on Ponzi schemes and scams etc, amongst others.
- Rural branches of banks are directed by RBI to conduct one camp per month covering all the messages that are part of Financial Awareness Messages (FAME) booklet, which includes messages on consumer protection i.e. Mis-selling, Sachet portal, Grievance Redressal mechanism etc.
- Centre for Financial Literacy (CFLs) have been set up at the block level to disseminate messages pertaining to Special facilities for the elderly and disabled customer, as prescribed by RBI, doorstep Banking Services for Senior Citizens and Differently Abled Persons and Awareness about digital banking.

2. **Awareness initiatives by NPCI:**

Training programmes are conducted by National Payments Corporation of India (NPCI), for creating awareness about financial literacy and digital payments in rural areas. NPCI has recently undertook a one-week campaign from 1st February 2022, for creating awareness about secure payment practices, for the prevention of BHIM-UPI related frauds.

****

Annexure-I

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

i. Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats and counter measures 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 sectors participated.

viii. CERT-In conducts regular training programmes for network / system administrators and Chief Information Security Officers (CISOs) of Government and critical sector organisations

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 programmes and free tools to remove the same for citizens and organisations.

****

Annexure-II

Steps taken by Reserve Bank of India (RBI):

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

i. 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, about transactions effected without the Additional Factor of Authentication (AFA), the issuer bank shall reimburse the loss to the customer further without demur.

ii. The mandate for additional authentication / validation shall apply to all transactions using cards issued in India.

iii. 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.

iv. 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.

v. 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 and card present (international) transactions and contactless transactions.

vi. All new cards issued - debit and credit, domestic and international - by banks shall be EMV Chip and PIN based cards.

vii. 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.

viii. Prepaid Payment Instruments (PPIs) 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.

ix. 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.

x. 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.

****