GOVERNMENT OF INDIA
MINISTRY OF FINANCE
DEPARTMENT OF FINANCIAL SERVICES

RAJYA SABHA
UNSTARRED QUESTION NO 2975
ANSWERED ON TUESDAY, 19 AUGUST, 2025/ 28 SRAVANA, 1947 (SAKA)

INCREASING FINANCIAL FRAUDS

2975 SMT. PRIYANKA CHATURVEDI:

Will the Minister of FINANCE be pleased to state:

(a) whether the Ministry is aware of the data released by the Ministry of Home Affairs regarding the ₹7,000 crore lost to online financial frauds in just the first five months of this year;

(b) if so, the measures taken by the Ministry to address the devastating loss caused by online financial fraud across the country;

(c) whether these scams originate internationally; and

(d) if so, whether Government considers collaborating with other countries to protect Indian citizens and penalise those responsible?

ANSWER

THE MINISTER OF STATE IN THE MINISTRY OF FINANCE

(SHRI PANKAJ CHAUDHARY)

(a) and (b) The Government has been constantly engaging with the financial sector regulators and other concerned stakeholders to strengthen the cyber security posture of the financial institutions. The Ministry of Home Affairs (MHA) has established the Indian Cyber Crime Coordination Centre (l4C) as an attached office to provide a framework and eco-system for Law Enforcement Agencies (LEAs) to deal with cybercrimes in a comprehensive and coordinated manner. The MHA has also launched the National Cyber Crime Reporting portal (https://cybercrime.gov.in) as well as a National Cybercrime Helpline Number ”1930 to enable the public to report all types of cyber crimes. Cyber crime incidents reported on this portal are routed automatically to the respective State/UT LEAs for further handling as per the provisions of law. Moreover, Department of Telecommunications (DoT) has launched Digital Intelligence Platform (DIP) and ‘Chakshu’ facility which enables citizens to report suspected fraud communication received over call, SMS or WhatsApp.

In order to reinforce the security of digital transactions, various initiatives have been taken by Reserve Bank of India (RBI) and National Payments Corporation of India (NPCI) from time to time. RBI has issued Master Directions on Digital Payment Security Controls in February, 2021 to combat web and mobile app threats. These guidelines mandate the banks to implement a common minimum standards of security controls for various payment channels like internet, mobile banking, card payment etc. RBI has also launched an Artificial Intelligence (AI) based tool 'MuleHunter' for identification of money mule and advised the banks and financial institutions for its uses.

(c) and (d) Available information indicates that some of these scam operations are carried out by transnational criminal networks operating from areas of South East Asia, including Cambodia and Laos. Government of India is working with its Mission offices in South East Asia to address the problem. Further, the matter has been raised in regional and multilateral platforms with the objective of building a political consensus and taking steps for a coordinated action to counter scam operations. Government is also working with State Governments for taking action against fraudulent recruiting agents. Regular advisories have been issued for cautioning Indian nationals against accepting unverified overseas job offers, emphasising the need for them to verify employer credentials through Indian Missions abroad. Safe and legal migration channels have been strengthened through the eMigrate platform. For those already trapped in such scam centres, sustained efforts are being made for their repatriation.

******