GOVERNMENT OF INDIA
MINISTRY OF HOME AFFAIRS

RAJYA SABHA
STARRED QUESTION NO. 105

TO BE ANSWERED ON THE 31ST JULY, 2024/ SRAVANA 9, 1946 (SAKA)

BIOMETRIC CLONING FOR FINANCIAL FRAUD

*105 SHRI B. PARTHASARADHI REDDY:

Will the Minister of HOME AFFAIRS be pleased to state:

(a) whether Government has taken cognizance of the rising financial fraud being committed through biometric cloning;

(b) if so, the details of the cases registered under biometric cloning;

(c) whether Government has taken stringent measures to address the issue of fake biometrics for financial fraud; and

(d) if so, the details thereof and if not, the reasons therefor?

ANSWER

MINISTER OF STATE IN THE MINISTRY OF HOME AFFAIRS
(SHRI BANDI SANJAY KUMAR)

(a) to (d): A statement is laid on the Table of the House.

R.S.S.Q.NO. *105 FOR 31.07.2024

STATEMENT IN REPLY TO PARTS (a) to (d) OF THE RAJYA SABHA STARRED QUESTION NO. *105 TO BE ANSWERED ON 31.07.2024.

'Police' and 'Public Order' are State subjects as per the Seventh Schedule of the Constitution of India. The States/UTs are primarily responsible for the prevention, detection, investigation and prosecution of crimes including cyber fraud through their Law Enforcement Agencies (LEAs). The Central Government supplements the initiatives of the States/UTs through advisories and financial assistance under various schemes for capacity building of their LEAs.

The National Crime Records Bureau (NCRB) compiles and publishes the statistical data on crimes in its publication "Crime in India". The latest published report is for the year 2022. Specific data regarding cases registered under biometric cloning is not maintained separately by NCRB. However, so far, around 29,000 incidents under Aadhar Enabled Payment System (AePS) frauds have been reported on National Cyber Crime Reporting Portal by citizens.

To strengthen the mechanism to deal with cyber crimes in a comprehensive and coordinated manner, the Central Government has taken steps which, inter-alia, include the following:

i. The Ministry of Home Affairs has set up the 'Indian Cyber Crime Coordination Centre' (I4C) as an attached office to deal with all types of cyber crime in the country, in a coordinated and comprehensive manner.

ii. The 'National Cyber Crime Reporting Portal (NCRP)' (https://cybercrime.gov.in) has been launched, as a part of the I4C, to enable public to report incidents pertaining to all types of cyber crimes, with special focus on cyber crimes against women and children. Cyber crime incidents reported on this portal, their conversion into FIRs and subsequent action thereon are handled by the State/UT Law Enforcement Agencies concerned as per the provisions of the law.

iii. I4C in coordination with National Payment Corporation of India (NPCI), Unique Identification Authority of India (UIDAI) and LEAs have taken various measures which, inter-alia include reporting against Business Corporate agents by Banks on NCRP, strengthening of KYC while onboarding of Business Corporate agents by Banks, introduction of biometric authentication for each transaction by the Business Corporate agents, integration of AePS

fraud management of NPCI with NCRP and action on incidents on AePS Frauds to curb AePS (Aadhar Enabled Payment System) Frauds.

iv. NPCI has implemented various measures to enhance the security of Aadhar Enabled Payment System (AePS) transactions which inter-alia include setting of cumulative AePS Limits for Cash withdrawal and Bhim Adhaar Pay to a maximum of Rs 50,000 per month, advisory to AePS member banks to disable AePS for specific categories of accounts and to provide multiple options to the customers to enable/disable AePS debit transactions.

v. Seven Joint Cyber Coordination Teams (JCCTs) have been constituted for Mewat, Jamtara, Ahmedabad, Hyderabad, Chandigarh, Vishakhapatnam, and Guwahati under I4C covering the whole country based upon cyber crime hotspots/ areas having multi jurisdictional issues by on boarding States/UTs to enhance the coordination framework among the Law Enforcement Agencies of the States/UTs. Seven workshops were organized for JCCTs at Hyderabad, Ahmedabad, Guwahati, Vishakhapatnam, Lucknow, Ranchi and Chandigarh in 2023.

vi. The 'Citizen Financial Cyber Fraud Reporting and Management System', under I4C, has been launched for immediate reporting of financial frauds and to stop siphoning off funds by the fraudsters. So far, financial amount of more than Rs. 2400 Crore has been saved in more than 7.6 lakh complaints. A toll-free Helpline number '1930' has been operationalized to provide assistance in lodging online cyber complaints.

vii. Till date more than 5.8 lakhs SIM cards and 1,08,000 IMEIs as reported by Police authorities have been blocked by Government of India.

viii. To spread awareness on cyber crime, the Central Government has taken steps which, inter-alia, include; dissemination of messages through SMS, I4C social media account i.e. X (formerly Twitter) (@CyberDost), Facebook(CyberDostI4C), Instagram (cyberDostI4C), Telegram(cyberdosti4c), Radio campaign, engaged MyGov for publicity in multiple mediums, organizing Cyber Safety and Security Awareness weeks in association with States/UTs, publishing of Handbook for Adolescents/Students, etc. The States/UTs have also been requested to carry out publicity to create mass awareness.

****