GOVERNMENT OF INDIA
MINISTRY OF FINANCE
LOK SABHA
UNSTARRED QUESTION NO-2945
ANSWERED ON- 21/03/2022

INCREASE IN BANKING FRAUDS

2945. SHRI T.R. BAALU

Will the Minister of FINANCE be pleased to state:-

(a) whether the Government concurs with the view that banking frauds will increase in spite of the many innovations that are being adopted by various banks in capturing the maximum share of business through them;

(b) if so, the details of the remedial steps taken/being taken by the Government keeping in view the fact that the frauds may crop up from different corners of the world either through fake accounts or fake bills which the banks may not be aware of until a certain point of time; and

(c) if not, the reasons therefor?

ANSWER

THE MINISTER OF STATE IN THE MINISTRY OF FINANCE

(DR. BHAGWAT KARAD)

(a) to (c): The Reserve Bank of India (RBI) has issued Master Directions on Frauds in 2016, and Government has instituted wide-ranging structural and procedural reforms to check frauds in banks. Such systematic and comprehensive checking for frauds, including of the legacy stock of non-performing assets (NPAs), led to unearthing of frauds perpetrated over the years. The improved detection and reporting accompanied with the comprehensive steps taken to check frauds have resulted in sharp decline in the occurrence of such frauds, from Rs. 61,229 crore in the financial year 2016-17 to Rs. 11,583 crore in the financial year 2020-21, and to Rs. 648 crore during the first nine months of the current financial year.

Comprehensive steps that have been taken to prevent frauds in banks, include, inter-alia, the following:

(1) An online searchable database of frauds reported by banks, in the form of Central Fraud Registry, has been set up to enable timely identification, control and mitigation of fraud risk and also to carry out due diligence during the credit sanction process.

(2) RBI has issued Master Directions on Frauds, which requires banks, to report frauds beyond a threshold amount to the police, monitoring and follow-up of cases by a special committee, quarterly placement of information before Audit Committees of bank Boards, and annual review of frauds by banks. These reviews cover, inter alia, preventive measures, fraud detection systems, systemic lacunae, remedial action, monitoring of progress of investigation and recovery, and staff accountability.

(3) For management of fraud risk and for early detection of loan frauds, prompt reporting to RBI and investigative agencies, and timely initiation of staff accountability proceedings,
RBI has issued a framework for dealing with loan frauds and red flagged accounts (RFA), requiring banks to classify potential fraud accounts as RFAs based on observation or evaluation of early warning signals noticed.

(4) RBI has issued a circular to all banks in February 2018 to implement security and operational controls, such as straight-through process between the bank’s core banking solution or accounting system and the SWIFT messaging system, enable time-based restrictions in SWIFT, review logs at regular intervals, undertake reconciliation, etc. in a time-bound manner.

(5) RBI has instructed banks to report deficient third-party services (such as legal search reports, property valuers’ reports, etc.) and collusion of these service providers with fraudsters to the Indian Banks’ Association, which maintains a caution list of such service providers.

(6) Issuance by the Government in 2015 of “Framework for timely detection, reporting, investigation etc. relating to large value bank frauds” to PSBs for dealing with suspected frauds involving sum of money in excess of Rs. 50 crore.

(7) A National Cyber Crime Reporting Portal has been launched by the Ministry of Home Affairs to enable public to report incidents pertaining to all types of cybercrimes, and a toll-free number has also been operationalised to get assistance in lodging online complaints.

(8) For immediate reporting of financial frauds and to stop siphoning-off of funds by the fraudsters, Financial Cyber Fraud Reporting and Management System module has been made operational by the Indian Cyber Crime Coordination Centre, working under the Ministry of Home Affairs.

(9) The Indian Computer Emergency Response Team (CERT-IN) under the Ministry of Electronics and Information Technology issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis to ensure safe usage of digital technologies, and is working in coordination with service providers, regulators and LEAs to track and disable phishing websites and facilitate investigation of fraudulent activities.

(10) Public sector banks (PSBs) have been advised to strictly ensure rotational transfer of officials/employees.

(11) Institution of comprehensive, automated Early Warning Systems (EWS) in PSBs, with ~80 EWS triggers and use of third-party data for time-bound remedial actions.

****