Government of India
Ministry of Finance
Department of Financial Services

LOK SABHA

Unstarred Question No. 2304
Answered on Monday, August 1, 2022/Sravana 10, 1944(Saka)

COOPERATIVE BANKS

2304. SHRI M.V.V. SATYANARAYANA:

Will the Minister of FINANCE be pleased to state:

(a) whether the Ministry has taken note of the significantly low share in deposits and advances in cooperative banks as compared to scheduled commercial banks;

(b) if so, whether the Ministry has considered a roadmap for improving dependability of cooperative banks;

(c) if so, the details thereof and if not, the reasons therefor;

(d) whether the Ministry has recorded the number of cyber frauds in cooperative banks in the past five years; and

(e) if so, the details thereof, State-wise and the steps being taken to minimize such instances?

Answer

THE MINISTER OF STATE IN THE MINISTRY OF FINANCE
(DR. BHAGWAT KARAD)

(a) to (c): The details of total deposits and advances of Rural Cooperative Banks (RCBs) [State Cooperative Banks (StCBs) + District Central Cooperative banks (DCCBs)], Urban Cooperative Banks (UCBs) and Scheduled Commercial Banks (SCBs) including Regional Rural Banks (RRBs) are as below:

(Amount in Rs. lakh crore)

Bank	Deposits	Loans and Advances
SCBs (including RRBs)	154.58	110.73
RCBs	6.05	5.17
UCBs	5.29	3.14

Source: RBI & NABARD; Data as on 31 March 2021

The size of deposits and advances of banks depends on various factors such as, geographical reach of the banks; size and robustness of the banking infrastructure, including IT platforms/systems; capital base; customer-profile, products offered & service delivery of the bank.

Some of the policy initiatives taken by Reserve Bank of India (RBI) for strengthening Cooperative banks are as under:

- The Banking Regulation Act, 1949 has been amended to provide additional powers to RBI for more effective regulation of co-operative banks. The major amendments pertain to areas such as management, audit, capital, reconstruction/amalgamation, etc. These amendments are expected to go a long way in strengthening the governance and regulation of co-operative banks.

- RBI issues instructions, circulars, guidelines and notifications to StCBs, DCCBs and UCBs under the provisions of the Banking Regulation Act, 1949 [As Applicable to Cooperative Societies (AACS)].
- Guidelines have been issued by RBI for StCBs /DCCBs and UCBs on various matters related to capital adequacy, income recognition and provisioning norms, investments, maintenance of deposits, branch expansion of StCBs/DCCBs and UCBs, customer service, etc.
- StCBs/DCCBs are being periodically inspected by NABARD under provisions of the Banking Regulation Act, 1949 to ensure that the banks are complying with the extant guidelines/instructions/norms.
- UCBs are being periodically inspected by RBI under provisions of the Banking Regulation Act, 1949 to ensure that the banks are complying with the extant guidelines/instructions/norms.

In order to strengthen the StCBs and DCCBs, NABARD enters into Memorandum of Understanding (MoU) with State Coop. Banks and State Governments for implementing state-specific Development Action Plans (DAPs). To review the performance under DAP, the quarterly meetings of high-powered forum under the nomenclature of "State Level Task Force (SLTF)" and "High Level Committee (HLC)" are conducted periodically. The forum has representatives from State Government, RBI, NABARD and StCB. To review and monitor the performance of DCCBs against DAPs, there is a district level forum called District Level Monitoring & Review Committee (DLMRC) with representations from State Government, RBI, NABARD, StCB, etc.

(d) & (e): The data related to Cyber Frauds in cooperative banks is maintained by NABARD for StCBs and DCCBs. For UCBs, the same is maintained by regional offices of RBI. As apprised by RBI and NABARD, a total of 429 cyber frauds have been reported by cooperative banks in past five years. As informed by RBI, the state-wise data of cyber frauds is not centrally maintained.

Steps taken by RBI and NABARD to minimize cybersecurity incidents and frauds are indicated in Annexure-I of this reply.

******

Annexure I as referred to in Part (d) & (e) of Answer to Lok Sabha Unstarred Question No.2304 for reply on 01.08.2022

Steps taken to mitigate cyber risks in respect of Cooperative Banks

A. Initiatives taken by RBI, inter-alia, include:

i. Setting up of a Cyber Security and IT Examination (CSITE) Cell within its Department of Supervision in 2015.
ii. Review of cyber security developments and threats on an ongoing basis and taking necessary measures to strengthen the cyber resilience of the banks, including the UCBs.
iii. Setting up a Cyber Crisis Management Group to address any major incidents reported, including suggesting ways to respond.
iv. Prescribing a set of baseline cyber security controls in October, 2018 for primary (Urban) cooperative banks (UCBs). To further strengthen the cyber security resilience of the UCBs, a comprehensive cyber security framework with graded approach was issued on December 31, 2019.
v. Carrying out IT Examination of select UCBs (based on digital depth of products/services offered; incidents reported, etc.), which is separate from the regular financial examination of the banks to assess their cyber resilience.
vi. Conducting cyber security preparedness testing on the basis of hypothetical scenarios with the help of CERT-In.
vii. Circular dated June 21, 2018 issued on "Control measures for ATMs – Timeline for compliance" advised banks to take various measures to strengthen security of ATMs.
viii. Guidelines dated December 31, 2019 issued on Cyber Security Controls for ATM Switch Application Service Providers (ASPs) for banks, including UCBs which are dependent upon third party ASPs for shared services for ATM Switch applications.

B. Steps taken by NABARD, inter-alia, include:

i. Compulsory reporting of all the Cyber Frauds or Incidents to Cyber Security and Information Technology Examination (CSITE) Cell at NABARD, Head Office by its Supervised Entities (SEs) within 6 hours after detection.
ii. Once the fraud information received, CSITE Cell reviews the fraud/incident, lapses in process or mis-configuration, and advises immediate corrective action to be initiated by the banks.
iii. Conducting regular training and awareness programs for its Supervised Entities through its training institutions on cyber security aspects.
iv. Guidelines dated February 06, 2020 issued to all its Supervised Entities for implementing Cyber Security Framework. All Supervised Entities have been also advised to report its cybersecurity implementation status to NABARD half yearly.
v. Issued letter to banks to conduct the audit by certified expert auditors. NABARD also inspect cybersecurity implementation in the banks during its onsite inspection.