GOVERNMENT OF INDIA
MINISTRY OF FINANCE
DEPARTMENT OF FINANCIAL SERVICES

RAJYA SABHA
UNSTARRED QUESTION NO. 1794
ANSWERED ON – 2/8/2022
DATA SECURITY OF CUSTOMERS IN BANKING AND INSURANCE COMPANIES

1794 # **SHRI RAM NATH THAKUR**:

Will the Minister of FINANCE be pleased to state:

(a) whether it is a fact that many of the personal and account details of the customers are being passed on to others by banks and insurance companies;

(b) whether it is also a fact that RBI has failed to take strict action against banks in case of breaches of data;

(c) the details of cases related to breach of data during the last five years; and

(d) the details of action taken by RBI in such cases during the last five years?

ANSWER

THE MINISTER OF STATE FOR FINANCE
(DR. BHAGWAT KARAD)

(a): As per Reserve Bank of India (RBI) Master Direction on Know Your Customer regarding sharing of information, bank shall maintain secrecy regarding the customer information, and same shall be treated as confidential and details shall not be divulged for any purpose without the express permission of the customer. Public Sector Banks have informed that personal and account details of the customers are not being passed on to others except when it is required to be provided under the provisions of law. Further, the Insurance Regulatory and Development Authority of India has informed that no instance with regard to passing of personal and account details of the customers to others by insurance companies, has come to its notice.

(b) to (d): RBI has apprised that total number of successful data breach attacks reported by banks is 248 (Public Sector Banks-41, Private Sector Banks-205 and Foreign Banks-2) during the period June-2018 to March-2022 and most of the data breaches pertain to card number leakage, theft of business/non-business information etc.

With regard to action taken by RBI in cases of data breaches, RBI has informed that it has issued guidelines on Cyber Security Framework for Scheduled Commercial Banks (SCBs), whereby banks are required to implement cyber/IT controls, among other things, for prevention of data leakage from its systems. Banks have also been directed to strengthen IT risk governance framework which mandates active role by their Chief Information Security Officer besides an active involvement of the Board / IT committee of the Board in ensuring compliance with the required standards.

Further, RBI has informed that non-compliance due to non/inadequate implementation of required controls are also assessed during IT examination conducted by RBI. Calibrated action against banks is adopted for ensuring adherence by them to extant regulatory instructions/ guidelines and resolution of related supervisory concerns. The degree of action taken for ensuring compliance depends on the severity and frequency of the non-compliance and also the specific nature of instructions which have not been complied. The supervisory process and supervisory actions, including enforcement actions taken against outlier banks includes, inter alia, the following –

(i) Bringing the matter to the notice of the concerned bank, including management of the bank for initiating corrective measures within definite time lines.
(ii) Advising management/Board to examine and initiate actions against erring staff/senior officers, as required in a given time frame.
(iii) Letter of displeasure to the management, to be placed before the Board.
(iv) Enforcement action in the form of imposition of monetary penalty and/or restriction on business activities.

*****