GOVERNMENT OF INDIA
MINISTRY OF FINANCE
DEPARTMENT OF FINANCIAL SERVICES

RAJYA SABHA
UNSTARRED QUESTION NO. 1501
ANSWERED ON – 14/3/2023
Amendment of guidelines for online banking

1501. **Dr. Ashok Bajpai:**

Will the Minister of FINANCE be pleased to state:

(a) whether Government is planning to amend its guidelines with regard to online opening of the bank accounts for availing loans by using the IDs of other peoples keeping in view the surging of cyber crimes;

(b) if so, the details of initiatives taken;

(c) whether in view of the surging crime and phishing operations in the financial dealings with the banks which have made all available means unsuccessful and futile, Government has any plan to revisit and enhance punishment to treat such operations with highest severity to deter such crimes; and

(d) if so, the details thereof?

ANSWER

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

(a) to (d): The guidelines for online opening of the bank accounts are issued by Reserve Bank of India (RBI). Regulated Entities (REs) are required to undertake Customer Due Diligence (CDD) while opening a bank account as per RBI guideline. For online opening of a bank account Video based Customer Identification Process (V-CIP) as an alternate method for customer identification has been provided with facial recognition and customer due diligence by an authorised official of the Regulated Entities. The process involves undertaking secure, live and consent based audio-visual interaction with the customer to obtain identification information and to ascertain the veracity of the information furnished by the customer through independent verification of identity, PAN Card, Aadhar card and signature of customer, customer location and other details such as annual income, Occupation, purpose of account opening, etc.

Cyber crime cases are dealt under penal provisions under chapter 11- offence of the IT Act. Further, RBI has informed that it reviews the cyber security developments and threats on an ongoing basis and necessary measures are taken to strengthen the cyber resilience of banks. Comprehensive steps taken in order to strengthen security of digital transactions and to stop cybercrime include, *inter alia,* the following:

(i) Cyber Security and IT Examination (CSITE) cell has been established by RBI in 2015. A comprehensive circular on Cyber Security Framework was issued in June 2016. As per this circular, banks were advised to put in place a board-approved cyber-security policy elucidating the strategy containing an appropriate approach to combat cyber threats given the level of complexity of business and acceptable levels of risk.
(ii) Cyber Crisis Management Group has been established to address any major incident reported including suggesting ways to respond. RBI also conducts cyber security preparedness testing among banks.
(iii) RBI has issued Master Direction on Digital Payment Security Controls on 18.2.2021. As per this direction, banks have been advised to put in place necessary controls to protect the confidentiality and integrity of customer data, and processes associated with the digital product/services offered by them.
(iv) Ministry of Home Affairs has launched a National Cyber Crime Reporting Portal to enable public to report incidents pertaining to all types of cybercrimes.
(v) 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.
(vi) The Indian Cyber Crime Coordination Centre (I4C), working under the Ministry of Home Affairs has operationalised Financial Cyber Fraud Reporting and Management System module, for immediate reporting of financial frauds and to stop siphoning-off of funds by the fraudsters.

*****