GOVERNMENT OF INDIA
MINISTRY OF FINANCE
DEPARTMENT OF FINANCIAL SERVICES

LOK SABHA

UNSTARRED QUESTION NO.536

TO BE ANSWERED ON THE 18th November, 2016/ Kartika 27, 1938 (SAKA)

Internet/Online Banking Frauds

QUESTION

536. SHRI RAMESH BIDHURI:
SHRI JANAK RAM:
SHRIMATI RAMA DEVI:
DR. SWAMI SAKSHIJI MAHARAJ:

Will the Minister of FINANCE be pleased to state:

(a) whether there has been a rise in the cases of withdrawal of money in a fraudulent manner through internet / online banking in the recent years and if so, the details thereof during each of the last three years and current year;

(b) the number of complaints received / reported in the country including the amount involved therein, during the last three years and the current year, bank and State / UT-wise;

(c) whether the Government has conducted any study/inquiry to ascertain the nature of these frauds, if so, the details thereof;

(d) whether there is any mechanism available with the Banks to detect such frauds; and

(e) if so, the details thereof and the corrective steps taken/being taken by the Government to protect the customers from the said frauds in future?

ANSWER

The Minister of State in the Ministry of Finance

(SHRI SANTOSH KUMAR GANGWAR)

(a) to (e): Data on frauds related to ATM / Credit / Debit cards & Net banking related frauds reported by the banks during last three years and current year, as informed by RBI is given below.

Area of operation	April 2013-March 2014		April 2014- March 2015		April 2015- March 2016		April 2016-June 2016	
	No. of Cases	Amount (Rs. in crore)	No. of Cases	Amount (Rs. in crore)	No. of Cases	Amount (Rs. in crore)	No. of Cases	Amount (Rs. in crore)
Credit Cards	7890	55	10382	42	9849	46	1927	7
ATM/Debit Cards	1307	8	2498	14	6585	31	1328	6
Internet Banking	303	15	203	24	34	2	18	1

The measure initiated by RBI to prevent such frauds is given below:

RBI has issued circular on 'Skimming of ATM/Debit/Credit Cards', dated June 26, 2006, advising banks to take various preventive measures to combat frauds relating to skimming or duplicating of credit cards. The banks, inter alia, were also advised to inform to customers not to reveal PIN in response to requests received through e-mail, to periodically verify the transaction history to ensure its correctness and if any unauthorized transaction observed it should be immediately reported to the bank and inform the bank if the card is lost or stolen.

(ii) In January 2016, Central Fraud Registry (CFR) has been operationised as searchable online central data base for use by the banks for frauds above Rs. 1 lakh. This data base is helpful to the banks not only during credit decisions but also to know about fraud in other areas of the banking including cyber frauds, ATM/debit/ credit card and internet banking.

(iii) Caution advices are also issued as and when necessary for preventing and controlling the frauds.

(iv) On September 28, 2016, RBI has reiterated its instruction on funds transfer requirement received through email/fax messages September 28, 2016. Banks were advised to strengthen the mechanism put in place by them in this regards and also to adhere to it strictly, including contacting the customer over phone at his registered phone number to ensure genuineness of request of the customer.

(v) RBI vide their letter dated 02.06.2016 advised that Banks should immediately put in place a 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, duly approved by their Board by September 30, 2016. Testing for vulnerabilities at reasonable intervals of time is very important. The IT architecture should be designed in such a manner that it takes care of facilitating the security measures to be in place at all times. It is essential that unauthorized access to networks and databases is not allowed. Confidentiality of customer information should not be compromised at any situation. Banks should take necessary preventive and corrective measures in addressing various types of cyber threats such as denial of service, distributed denial of services (DDoS), ransom-ware / crypto ware, destructive malware, etc. Banks shall report all unusual cyber security incidents to RBI within 2 - 6 hours of detection.

****