# GOVERNMENT OF INDIA
# FINANCE
# LOK SABHA

UNSTARRED QUESTION NO:121
ANSWERED ON:22.02.2013
CYBER FRAUDS IN BANKS
Semmalai Shri S. ;Singh Shri Ganesh;Thamaraiselvan Shri R.

**Will the Minister of FINANCE be pleased to state:**

(a) whether the number of incidents of cyber frauds particularly of withdrawing money by cloning of credit and debit cards including net banking are continuously increasing in the country ;

(b) if so, the details thereof and the number of such complaints sent by the public / private sector banks to the Reserve Bank of India (RBI) during the last three years and the current year, year-wise and the amount involved in it and loss suffered by banks as a result thereof, bank-wise;

(c) the details of the amount of public /private sector banks which has turned into non-performing assets due to said frauds during the said period; and

(d) the steps taken /proposed to be taken by the Government to bring cyber safety and check frauds in online transactions ?

## Answer

MINISTER OF STATE IN THE MINISTRY OF FINANCE (SHRI NAMO NARAIN MEENA)

(a) & (b) :- The details furnished by Reserve Bank of India (RBI) in respect of Scheduled Commercial Banks pertaining to frauds relating to ATMs/Debit Cards/ Internet Banking and Credit Cards is as under :

(Rs. In lakhs)

| Sl.No. | Calendar Year | Total cases reported | Amount involved |
|---|---|---|---|
| 1. | 2010 | 15018 | 4048.94 |
| 2. | 2011 | 9588 | 3672.19 |
| 3. | 2012 | 8322 | 5266.95 |

#Bank wise details of Cyber Frauds for the last 3 years is at Annex − 1.

(c) :- RBI has informed that it does not have data on Cyber Frauds in Public Sector Bank that have turned into non− performing assets.

(d) :- The measures initiated by RBI to strengthen security arrangements are as under:-

(i) RBI acts as per the Master Circular RBI.DBS.FrMC.BC.No.1/23.04.001/2012-13 dated July 02, 2012 on "Frauds − Classification and reporting" containing all the details/aspects relating to frauds. The same is also available on the website of RBI i.e. www.rbi.org.in. On receipt of fraud reports from banks, various aspects related to the frauds are examined and concerned banks are advised to report the case to CBI/ Police/ SFIO, examine staff accountability, complete proceedings against the erring staff expeditiously, take steps to recover the amount involved in the fraud, claim insurance wherever applicable and streamline the system as also procedures so that frauds do not recur.

(ii) RBI has issued two circulars viz; (i) 'Security arrangements for ATMs of bank' dated February 22, 2006 and (ii) 'Skimming of ATM/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 preventive measures include educating customers through cautionary messages posted in the web-site of card issuing banks, informing customers not to reveal PIN in response to requests received through e-mails, to periodically

verify the transaction history, immediate reporting to the bank, if any unauthorized transaction is observed, and inform the bank if the card is lost or stolen.

(iii) On the basis of suggestions of a Working Group set up by RBI in 2010, RBI has issued guidelines which are fundamentally expected to enhance safety, security, efficiency in banking processes leading to benefits for banks and their customers. The implementation progress are required to be reviewed and report submitted to the Board on quarterly basis.

(iv) RBI vide its Master Circular dated 1.7.2011, on "Credit Card Operation of Banks" advised banks to set up internal control systems to combat frauds and to take pro-active fraud control and enforcement measures and to ensure that credit card operations were run on sound, prudent and profitable lines as also fulfill 'Know Your Customer' requirement, assess credit risk of customers, specify terms and conditions in clear and simple language, ensure prompt dispatch of bills, maintain customer confidentiality etc.

(v) All Commercial Banks have also been cautioned by RBI vide letter dated. 16.02.2006 on phishing attacks which contained details of the modus-operandi on such attacks and minimum set of preventive/detective measures to tackle phishing attacks.

(vi) Besides above, public is advised through press releases/notifications regarding not to reveal account details, do not fall prey to fictitious offers of fund transfer, remittance towards participation in lottery, money circulation schemes, and other fictitious offers of cheap funds etc.