GOVERNMENT OF INDIA
FINANCE
LOK SABHA

UNSTARRED QUESTION NO:3302
ANSWERED ON:12.12.2014
BANKING FRAUDS
Dhotre Shri Sanjay Shamrao;Kodikunnil Shri Suresh;Mahtab Shri Bhartruhari;Thakur Shri Anurag Singh

Will the Minister of FINANCE be pleased to state:

(a) whether India ranks high in the list of online banking frauds affected by cyber criminals;

(b) if so, the details thereof along with the number of credit/debit/ATM cards, electronic money transfer complaints reported in the country including the amount involvedtherein, during the last three years and the current year, bank and State/UT-wise;

(c) whether the Government has taken any action against the erring bank officials engaged in such cases and if so, the details thereof during the said period, bank-wise;

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

(e) whether any mechanism is available with the Banks to detect fraud cases instated of reporting such cases by their customers; and

(f) if so, the details thereof and if not, the reasons therefor along with the reaction of the Government thereto and the corrective steps taken/being taken by the Government to protect the customers from these frauds and check such incidents in future?

Answer

MINISTER OF STATE IN THE MINISTRY OF FINANCE (SHRI JAYANT SINHA)

(a) & (b) : The details of fraud cases reported by banks to the Reserve Bank of India (RBI) pertaining to the Credit / Debit /ATM cards, electronic money transfer related cases reported in the countryincluding the amount involved therein, during the last three years and the current year, bank wise data given in Annex. As reported by RBI, State/UT-wisedata is not maintained by RBI.

(c) : In all cases of fraud, the bank undertakes an investigation and takes action including fixing of the staff accountability as per the applicable disciplinary rules.

(d), (e) & (f) : RBI has taken the following measures to prevent such frauds:

(i) The Reserve Bank has been sensitizing banks and general public against the fictitious offers of cheap funds/lottery winnings etc from abroad sent by fraudsters. Various advisories were issued by the Bank cautioning the members of public against responding in any manner to offers of money from abroad.

(ii) A working Group on "Information Security, Electronic Banking, Technology, Risk Management and Tracking of Cyber Frauds" set up by RBI in April, 2010 had inter alia suggested that chip based cards may be used as an alternative to magnetic strip cards based as a measure to counter the risks of skimming of ATM Cards. Based on the various recommendations of the Working Group, suitable guidelines were issued by RBI vide circular dated April 19, 2011 advising the Banks to frame / create / fine-tune/modify their IT policies and implement procedures and technologies based on new developments and emerging concerns.

(iii) The various guidelines issued so far by the RBI (in chronological order) related to security of card and electronic payment transactions are as follows:

(A) CARD NOT PRESENT TRANSACTION (CNP)

Additional factor of authentication for use of cards issued by banks in India for all online transactions (February 18, 2009)

Additional factor of authentication for use of cards issued by banks in India and acquired by banks in India. Mandate of AFA applicable only in this case where there is no foreign exchange outflow (October 25, 2010)

Additional factor of authentication for use of cards issued by banks in India for all IVR transactions (December 31,2010)

Additional factor of authentication for use of cards issued by banks in India for all Mail order Telephone Order transactions (MOTO) /Standing Instructions (August 04, 2011)

Transactions using cards issued by banks in India towards online purchase of goods and services provided within the country, to be

acquired only through a bank in India and the transaction should necessarily settle only in Indian currency (August 22, 2014)

(B) CARD PRESENT TRANSACTIONS (CP)

PIN validation for every successive transactions at ATM (October 18, 2010)

Working Group recommendation (September 22, 2011) − to enhance the security of card acceptance infrastructure, and undertake necessary actions to ensure readiness of infrastructure for migration to EMV Chip and PIN cards

Guidelines on security of card payments and electronic payments (February 28, 2013)

I. All new debit and credit cards to be issued only for domestic usage unless international use is specifically sought by the customer. Such cards enabling international usage will have to be essentially EMV Chip and Pin enabled.

II. Issuing banks should convert all existing MagStripe cards to EMV Chip card for all customers who have used their cards internationally at least once (for/through e- commerce /ATM/POS)

III. All the active Magstripe international cards issued by banks should have threshold limit for international usage. The threshold should be determined by the banks based on the risk profile of the customer and accepted by the customer. Till such time this process is completed an omnibus threshold limit (say, not exceeding USD 500) as determined by each bank may be put in place for all debit cards and all credit cards that have not been used for international transactions in the past.

All new card present infrastructures has to be enabled for both EMV chip and PIN and Aadhaar (biometric validation) acceptance (November 26, 2013; these instructions have been put on hold awaiting the feedback from the industry through Indian Banks Association)

(C) GENERAL MEASURES

Online alerts for all types of card transaction irrespective of the channels and the amount (March 29, 2011)

(D) Securing electronic payment transactions (February 28, 2013):

Customer induced options may be provided for fixing a cap on the value / mode of transactions/beneficiaries. In the event of customer wanting to exceed the cap, an additional authorization may be insisted upon.

Limit on the number of beneficiaries that may be added in a day per account could be considered.

A system of alert may be introduced when a beneficiary is added.

Banks may put in place mechanism for velocity check on the number of transactions effected per day/ per beneficiary and any suspicious operations should be subjected to alert within the bank and to the customer.

Introduction of additional factor of authentication (preferably dynamic in nature) for such payment transactions should be considered.

Banks may consider implementation of digital signature for large value payments for all customers, to start with for RTGS transactions.

Capturing of Internet Protocol (IP) address as an additional validation check should be considered.

(iv) RBI had also issued a caution circular DBS CO IS Audit BC No. 3/31.02.03/2005-06 dated February 16, 2006 to all commercial banks on "Phishing Attacks"(i.e. creating fake website of banks and collecting customer details such as user ID, password etc. and thereby fraudulently withdrawing money from the customer's account using fake credit card). The circular contained details of the modus operandi on such attacks and minimum set of preventive/detective measures to tackle phishing attacks.