GOVERNMENT OF INDIA
FINANCE
LOK SABHA

STARRED QUESTION NO:350
ANSWERED ON:15.12.2006
BANK FRAUDS
Kaushal Shri Raghuvir Singh;Singh Shri Uday

Will the Minister of FINANCE be pleased to state:

(a)whether the government is aware of the organized gangs involved in cheating by cloning international credit cards;

(b) if so, the bank-wise details thereof;

(a) whether the Government has detected the technique being used in stealing data;

(b) if so, the details thereof;

(c) whether the increasing use of electronic channels for payments has posed a new security problem for banks;

(d) if so, whether any technique has been developed in this regard to control such crimes; and

(e) if so, the details thereof ?

Answer

MINISTER OF THE STATE IN THE MINISTRY OF FINANCE MINISTER (P.CHIDAMBARAM)

(a) to (e): A statement is laid on the Table of the House.

Statement referred to in reply to Part (a) to (g) of Lok Sabha Starred Question No.350 for 15.12.2006 by Shri Raghuveer Singh Koshal and Shri Uday Singh regarding Use of Electronic Channels in Banks.

(a) & (b) The Fraud Monitoring Cell of Reserve Bank of India (RBI) receives report on all frauds/cheating detected at Commercial Banks and Financial Institutions. RBI has reported that they have no information regarding organized gangs involved in cheating by cloning International credit cards.

(c) & (d) Cloning i.e. skimming and duplicating credit cards is a technique being used in stealing data and making counterfeit cards. Skimming is defined as the transfer of magnetic stripe data from a genuine credit card to the magnetic stripe of a counterfeit plastic card. A few instances of skimming of credit cards for unauthorised uses by unscrupulous elements have been reported to RBI by banks.

(e), (f) & (g) Banks need to put in place appropriate system to mitigate the risk arising out of electronic channels for payments. RBI has issued a circular to Banks on 26.6.2006 advising them to take preventive measures to combat skimming related frauds. These measures, inter-alia, include :-

Customers should protect their ATM Personal Identification Number (PIN), periodically verify the transaction history to ensure its correctness, immediate inform to the bank if the ATM/Credit card is lost or stolen, etc.

Banks should conduct regular inspection of ATM machines and ensure that cash is loaded in the machines in the presence of bank officials, conduct random checks for identifying any signs of tampering of fixtures attached to ATMs, investigate customer complaints quickly to determine if ATM was misused, evaluate the latest security features like anti-skimming features offered by ATM vendors and implement the important features based on the perceived risks, etc.