GOVT. OF INDIA
MINISTRY OF FINANCE
DEPARTMENT OF FINANCIAL SERVICES

LOK SABHA
UNSTARRED QUESTION No 2787

TO BE ANSWERED ON THE 03RD AUGUST, 2018 (FRIDAY) / SHRAVANA 12, 1940(SAKA)

"Data Breach at Banks"

QUESTION

2787. SHRI K. PARASURAMAN:

Will the Minister of FINANCE be pleased to state:

(a) whether the data breach at 19 Indian banks has led to more than 32 lakh debit cards being blocked or recalled and if so, the details thereof;

(b) the action taken by the Government in this regard;

(c) whether the Government is having any roadmap to check such incidents in future; and

(d) if so, the details thereof?

ANSWER

(MINISTER OF STATE IN THE MINISTRY OF FINANCE)
(SHRI SHIV PRATAP SHUKLA)

(a) & (b): It had come to the Reserve Bank of India's (RBI) notice on September 8, 2016 that details of certain cards issued by a few banks had been possibly compromised at Automated Teller Machines (ATMs) linked to the ATM Switch of one of the service providers. Further, RBI had issued a press release on "ATM/Debit Card Data breach" dated October 24, 2016 in this regard (text of press release is attached as Annexure).
(c) & (d): RBI reviews the cyber security developments and threats on an ongoing basis and necessary measures are taken to strengthen the cyber resilience of banks.
In order to focus more attention on IT related matters, RBI had set up a Cyber Security and IT Examination (CSITE) Cell within its Department of Banking Supervision in 2015.
A comprehensive circular on Cyber Security Framework in Banks issued by RBI on June 2, 2016 covers best practices pertaining to various aspects of cyber security.
Banks were advised by RBI to implement various security control measures in a phased manner with specific timelines to enhance the security of the ATM Infrastructure.

*****

Annexure referred to in statement of reply to PQ No. 2787 for reply on 03.08.2018 on Data Breach at Banks

ATM/Debit Card Data Breach

The Reserve Bank of India convened a meeting today with senior officials from select banks, National Payment Corporation of India and card network operators to review the steps taken by various agencies to contain the adverse fall out of certain card details alleged to have been compromised.

It had come to the Reserve Bank's notice on September 8, 2016 that details of certain cards issued by a few banks had been possibly compromised at Automated Teller Machines (ATMs) linked to the ATM Switch of one of the service providers. The issue is currently being investigated by an approved forensic auditor, under PCI-DSS framework.

The number of cards misused, as per currently available information, is small. As a matter of abundant precaution, however, card network operators concerned were earlier advised to share the details of cards used during the period of such exposure. Based on this, banks have been taking necessary remedial action to avoid any potential abuse of such cards in future by unscrupulous elements and to protect the interest of their customers. Banks have taken measures including advising the customers to change PIN, blocking payments at international locations, reducing the withdrawal limits, monitoring unusual patterns, replacing the cards and re-crediting the accounts of cardholders for amounts wrongly debited.

The Reserve Bank has urged the cardholding bank customers that it is a good practice to change the PIN and passwords periodically and not to share them with anyone for any reason. It has also cautioned that banks do not ask for card or account details from their customers. Customers may, therefore, exercise caution and not reveal such information to any person on phone or email.

The Reserve Bank has already instructed banks on June 2, 2016 to put in place cyber security framework. Banks have once again been advised to review the existing cyber security arrangements. The Reserve Bank has emphasised an early implementation of this framework so that (i) possibility of such incidents happening in future is minimised and (ii) in the event of such incidents, containment measures are taken immediately.

******