GOVERNMENT OF INDIA
MINISTRY OF FINANCE
DEPARTMENT OF EXPENDITURE

LOK SABHA
STARRED QUESTION NO.124

ANSWERED ON FRIDAY, 4TH MARCH, 2016, 14TH PHALGUNA, 1937 (SAKA)

PROTECTION OF PERSONAL INFORMATION

*124. SHRI SULTAN AHMED

Will the Minister of FINANCE be pleased to state:

a) whether the Government has received complaints against the service providers for leaking personal information of customers to the Business Process Outsourcing (BPOs) during last three years and current year and if so, the details thereof;

b) whether the Government has formulated any code for the protection of personal information by service providers and if so, the details thereof; and

c) other measures taken/proposed to be taken by the Government to protect personal information of consumers?

ANSWER
MINISTER OF FINANCE
(SHRI ARUN JAITLEY)

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

STATEMENT REFERRED TO IN REPLY TO PARTS (A) TO (C) OF LOK SABHA STARRED QUESTION NO.124 BY SHRI SULTAN AHMED TO BE ANSWERED ON 4TH MARCH, 2016 REGARDING "PROTECTION OF PERSONAL INFORMATION"

(a): Ministry of Finance has not received any complaint against service providers for leaking personal information of customers to Business Process Outsourcing (BPOs) during last three years and current year.

(b) & (c): Measures for protection of personal information by Service Providers have been provided under **Information Technology Act, 2000** administered by the Ministry of Communications & Information Technology, Department of Electronics and Information Technology, and **Indian Telegraph Act, 1885** administered by the Department of Telecommunications, Ministry of Communications & Information Technology under which Agreement is signed with Telecom Services Providers which inter-alia contains mandate to protect the interest of stakeholders/customers and privacy of the individual, **Prevention of Money Laundering Act, 2002** administered by the Department of Financial Services under which every information maintained, furnished or verified, save as otherwise provided under any law for the time being in force, shall be kept confidential and **the instructions** issued by Pension Fund Regulatory and Development Authority which under the Risk Management Principles provides for ensuring that every insurer shall take appropriate steps to require that third party service providers protect confidential information of both the insurer and its clients from intentional or inadvertent disclosure to unauthorized persons etc. A copy of the relevant extracts is annexed.

Customers have options to register complaints under the above acts with the Police authorities, Consumer Forums, Banking and Judicial authorities etc., who may invoke the above provisions for protection from leaking of personal information of customers to the Business Process Outsourcing(BPOs) or any other entity, unauthorisedly.

RELEVANT EXTRACTS REFERRED IN THE STATEMENT IN REPLY TO PARTS (B) TO (C) OF LOK SABHA STARRED QUESTION NO.124 BY SHRI SULTAN AHMED TO BE ANSWERED ON 4TH MARCH, 2016 REGARDING "PROTECTION OF PERSONAL INFORMATION"

Information Technology Act, 2000

Section 43, Section 43A and Section 72A of the Information Technology Act, 2000 provides comprehensive legal framework for privacy and Security of data in digital form. Sections 43 and 43A of the Act provides for compensation to be paid to the victim in case of unauthorized access of information and leakage of sensitive personal information respectively. Section 43A also mandates that body corporate, who collect personal data or information must provide privacy policy for handling of or dealing in personal information including sensitive personal data or information on their websites. Section 72A provides for punishment for disclosure of information in breach of the lawful contract.

Indian Telegraph Act, 1885

Terms and Conditions for the unified licences.

"37.2 Subject to terms and conditions of the license, the Licensee shall take all necessary steps to safeguard the privacy and confidentiality of any information about a third party and its business to whom it provides the Service and from whom it has acquired such information by virtue of the Service provided and shall use its best endeavors to secure that:-

a) No person acting on behalf of the Licensee or the Licensee divulges or uses any such information except as may be necessary in the course of providing such Service to the Third Party; and

b) No such person seeks such information other than is necessary for the purpose of providing Service to the Third Party.

Provided the above para shall not apply where:

a) The information relates to a specific party and that party has consented in writing to such information being divulged or used, and such information is divulged or used in accordance with the terms of that consent; or

b) The information is already open to the public and otherwise known.

37.3 The Licensee shall take necessary steps to ensure that the Licensee and any person(s) acting on its behalf observe confidentiality of customer information.

39.4 The LICENSEE shall ensure protection of privacy of communication and ensure that unauthorized interception of messages does not take place.

39.23(xix) In order to maintain the privacy of voice and data, monitoring shall be in accordance with rules in this regard under Indian Telegraph Act, 1885".

Prevention of Money Laundering Act, 2002

The Section 12(2) of the Prevention of Money Laundering Act, 2002 states that every information maintained, furnished or verified, save as otherwise provided under any law for the time being in force, shall be kept confidential.

Reserve Bank of India, Department of Banking Regulation(DBR) has issued Master Directions dated February 25, 2016 on Know Your Customer(KYC) to RBI's regulated entities, wherein they have been advised that information collected from customers for the purpose of opening of account shall be treated as confidential and details thereof shall not be divulged for the purpose of cross selling, or for any other purpose without the express permission of the customer.

In terms of circular reference DBOD No.BP 40/21.04.158/2006-07 dated November, 2006 on 'Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by banks' **Para 5.6 - Confidentiality and Security**, states as under:

i. Public confidence and customer trust in the bank is a prerequisite for the stability and reputation of the bank. Hence the bank should seek to ensure the preservation and protection of the security and confidentiality of customer information in the custody or possession of the service provider.

ii. Access to customer information by staff of the service provider should be on 'need to know' basis i.e., limited to those areas where the information is required in order to perform the outsourced function.

iii. The bank should ensure that the service provider is able to isolate and clearly identify the bank's customer information, documents, records and assets to protect the confidentiality of the information. In instances, where service provider acts as an outsourcing agent for multiple banks, care should be taken to build strong safeguards so that there is no comingling of information / documents, records and assets.

iv. The bank should review and monitor the security practices and control processes of the service provider on a regular basis and require the service provider to disclose security breaches.

v. The bank should immediately notify RBI in the event of any breach of security and leakage of confidential customer related information. In these eventualities, the bank would be liable to its customers for any damage.

DBR's Master circular on "Credit Card, Debit Card and Rupee Denominated Co-branded Pre-paid Card Operations of Banks and Credit Card issuing NBFCs" (Ref: DBR.No.FSD.BC.18/24.01.009/2015-16) dated July 1, 2015 has prescribed the following guidelines to protect the personal information of the consumers of financial products:

i. Para I 7.4 of the above circular states that Banks may ensure that they engage telemarketers who comply with directions/regulations on the subject issued by the Telecom Regulatory Authority of India (TRAI) from time to time while adhering to guidelines issued on "Unsolicited Commercial Communications – National Customer Preference Register (NCPR)".

ii. Para I 9.1 of the above circular states that Credit Card issuing bank/NBFC should not reveal any information relating to customers obtained at the time of opening the account or issuing the credit card to any other person or organization without obtaining their specific consent, as regards the purpose/s for which the information will be used and the organizations with whom the information will be shared. The application form for credit card must explicitly provide for consent the same. Further, in case where the customers gives his consent for the bank sharing the information with other agencies, banks should explicitly state and explain clearly to the customer the full meaning/ implications of the disclosure clause. The information being sought from customers should not be of such nature as will violate the provisions of the laws relating to secrecy in the transactions. Banks/NBFCs would be solely responsible for the correctness or otherwise of the data provided for the purpose.

iii. Para 9.2 of the above circular states that disclosure to the DSAs/recovery agents should also be limited to the extent that will enable them to discharge their duties. Personal information provided by the card holder but not required for recovery purposes should not be released by the card issuing bank/NBFC. The card issuing bank/NBFCs should ensure that the DSAs/DMAs do not transfer or misuse any customer information during marketing of credit card products.

iv. Para II 16 of the above circular states that the Debit Card issuing bank should not reveal any information relating to customers obtained at the time of opening the account or issuing the card and the co-branding non-banking entity should not be permitted to access any details of customer's accounts that may violate bank's secrecy obligations. Banks, which were granted specific approvals for issue of co-branded debit cards in the past, were advised to ensure that the co-branding arrangement is in conformity with the instructions mentioned above. In case, the co-branding arrangement is between two banks, the card issuing bank may ensure compliance with the above conditions.

Guidelines on Outsourcing of Activities by Insurance Companies vide circular ref. IRDA/Life/CIR/GLD/013/02/2011 dated 1st February 2011

Risk Management Principles: While outsourcing activities every insurer shall abide by criteria laid down in the following principles:

9.11 The insurer shall take appropriate steps to require that third party service providers protect confidential information of both the insurer and its clients from intentional or inadvertent disclosure to unauthorized persons.

(c) Other measures taken/proposed to be taken by the Government to protect the personal information of consumers?

******