GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION No. 3983
TO BE ANSWERED ON: 18.03.2020

FRAUDULENT USAGE OF CREDIT / DEBIT CARD

3983 DR. SUJAY RADHAKRISHNA VIKHE PATIL: SHRI UNMESH BHAIYYASAHEB PATIL: DR. SHRIKANT EKNATH SHINDE: SHRI HEMANT SRIRAM PATIL: SHRI DHAIRYASHEEL SAMBHAJIRAO MANE:

Will the Minister of Electronics and Information Technology be pleased to state:

(a) the number of reported case of fraudulent usage of debit/credit cards of people by pilferage of their passwords/OTP/pin code during the last three years, State/UT-wise;
(b) the steps taken by the Government in this regard; and
(c) the steps taken/to be taken by the Government to create awareness as well as further strengthen the security system to ensure maximum internet security to the people?

ANSWER
MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI SANJAY DHOTRE)

(a): As per the information received from Reserve Bank of India, the number of cases reported of fraudulent usage of debit/credit cards of people across various states and UTs have been mentioned in Annexure-I.
(b) and (c): Government of India has taken several steps, that are mentioned in Annexure-II to create awareness and strengthen cyber security. Further, steps taken by Reserve Bank of India (RBI) for digital payments security and awareness are mentioned in Annexure-III.

Annexure-I

State-wise data on frauds reported by SCBs and FIs on the category ''Card/Internet - ATM/Debit Cards, Credit Cards and Internet Banking' for the last 3 Financial Years and period up to the quarter ended December 2019 of current Financial Year based on Reporting (Rs. in cr.)

	2016-17		2017-18		2018-19		2019-20	
Name of State	**No. of frauds**	**Amt. involved**	**No. of frauds**	**Amt. involved**	**No. of frauds**	**Amt. involved**	**No. of frauds**	**Amt. involved**
Andaman & Nicobar Islands					10	0.12	20	0.09
Andhra Pradesh	31	0.64	72	0.27	181	0.36	465	1.85
Arunachal Pradesh			11	0.12	1	0.01	6	0.05
Assam	3	0.11	218	2.03	87	0.85	423	2.58
Bihar	4	0.07	50	0.24	151	0.61	260	1.02
Chandigarh	7	0.19	90	0.27	111	0.37	146	66.67
Chhattisgarh	1	0.01	46	0.22	106	0.41	164	0.57
Dadra & Nagar Haveli			10	0.01	16	0.02	21	0.03
Daman & Diu							20	0.04
Goa			18	0.08	114	0.57	176	0.44
Gujarat	16	0.53	563	9.41	1135	2.23	1788	4.79
Haryana	238	8.28	8444	24.05	8983	21.20	5083	17.52
Himachal Pradesh	1	0.02	26	0.16	47	0.17	125	0.58
Jammu & Kashmir	1	0.09	53	0.38	27	0.07	71	0.20
Jharkhand	9	0.12	40	0.15	109	0.61	155	0.53
Karnataka	221	9.16	1573	10.59	1886	5.17	2845	17.57
Kerala	9	0.46	120	0.64	212	1.46	745	3.75
Madhya Pradesh	4	0.10	104	0.83	212	0.62	515	1.72
Maharashtra	379	12.10	15629	43.44	21673	42.35	21897	44.99
Manipur			1	0.00	8	0.07	5	0.02
Meghalaya			8	0.03	12	0.05	20	0.13
Mizoram					5	0.01	8	0.06

Nagaland			9	0.04	3	0.02	9	0.07
New Delhi	156	3.44	1697	13.37	4191	15.76	5499	15.37
Odisha	1	0.06	51	0.35	115	0.53	456	2.55
Overseas	7	0.22	27	0.16	27	0.29	12	0.09
Puducherry	2	0.05	9	0.04	6	0.05	12	0.05
Punjab	3	0.27	214	0.99	288	0.92	501	2.14
Rajasthan	10	0.16	132	1.18	374	1.47	755	9.17
Sikkim			2	0.01	4	0.00	15	0.06
Tamil Nadu	208	4.39	3855	50.36	5497	24.06	5258	17.03
Telangana			586	4.30	974	2.61	1284	2.75
Tripura			6	0.04	9	0.03	25	0.10
Uttar Pradesh	37	1.04	763	3.16	5109	7.80	2130	10.57
Uttarakhand			119	0.57	128	0.53	141	0.44
Uttaranchal	5	0.13						
West Bengal	19	0.67	245	1.50	493	17.99	951	2.86
Grand Total	1372	42.29	34791	168.99	52304	149.42	52006	228.44

Notes: It may be noted that fraud cases below Rs. 1 lakh were not required to be reported to RBI prior to April 1, 2017.

Annexure-II

Initiatives by the Government of India

i. The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis to ensure safe usage of digital technologies. Regarding securing digital payments, 35 advisories have been issued for users and institutions.

ii. All authorised entities/ banks issuing PPIs in the country have been advised by CERT-In through Reserve bank of India to carry out special audit by empanelled auditors of CERT-In on a priority basis and to take immediate steps thereafter to comply with the findings of the audit report and ensure implementation of security best practices.

iii. Government has issued guidelines for Chief Information Security Officers (CISOs) regarding their key roles and responsibilities for securing applications / infrastructure and compliance.

iv. Government has empanelled 90 security auditing organisations to support and audit implementation of Information Security Best Practices.

v. Government has formulated Crisis Management Plan for countering cyber attacks and cyber terrorism for implementation by all Ministries/ Departments of Central Government, State Governments and their organizations and critical sectors.

vi. Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organisations in Government and critical sectors. 44 such drills have so far been conducted by CERT-In where 265 organisations from different States and sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space, IT/ITeS, etc participated. Out of these drills, 9 drills were conducted in coordination with the Reserve Bank of India and The Institute for Development and Research in Banking Technology for financial sector organisations.

vii. CERT-In conducts regular training programmes for network / system administrators and Chief Information Security Officers (CISOs) of Government and critical sector organisations regarding securing the IT infrastructure and mitigating cyber attacks.

viii. Government has launched the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre). The centre is providing detection of malicious programs and free tools to remove the same.

ix. Under the Information Security Education and Awareness (ISEA) Project Phase-I (2005-2014), more than 44,000 candidates were trained in various formal/non-formal courses in Information Security through 40 institutions. Around 100 Government officials were trained as Master Trainers in the area of Information Security.

Annexure-III

Steps taken by RBI

1. Securing Card Transactions: (i) Banks have been advised to provide online alerts for all card transactions, vide, RBI circular dated March 29, 2011. **(ii)** RBI has also issued circulars dated September 22, 2011, February 28, 2013 and June 24, 2013 for securing electronic transactions advising banks to introduce additional security measures. **(iii)** RBI has directed banks to mandatorily put in place an Additional Factor of Authentication for all Card not present transaction w.e.f. 01.05.2013 failing which the issuer bank shall reimburse the loss to customer without demur. **(iv)** All authorised card payment networks are permitted to offer card tokenisation services to any token requestor, subject to certain conditions.

2. Securing Payments through Internet Banking / Electronic Payments: RBI has issued circular on 'Security and Risk Mitigation Measures for Electronic Payment Transactions' (DPSS.CO.PD No.1462 /02.14.003 /2012-13) dated February 28, 2013.

3. Prepaid Payment Instruments (PPIs): RBI has issued 'Master Direction on Issuance and Operation of PPIs' (MD on PPIs) (DPSS.CO. PD. No.1164/02.14.006/2017-18) dated October 11, 2017 (updated as on December 29, 2017). As per para 15.3 of MD on PPI issuers were instructed to put in place a framework to address the safety and security concerns, and for risk mitigation and fraud prevention.

4. Limiting Customer Liability on Unauthorized Electronic Banking Transactions: RBI has issued circular no. DBR.No. Leg.BC.78/09.07.005/2017-18 dated July 06, 2017 limiting the liability of customers on unauthorized electronic banking transactions.

5. Limiting Customer Liability in Unauthorized Electronic Banking Transactions in PPIs issued by Authorised Non-banks: RBI has issued circular no. DPSS.CO.PD.No.1417/02.14.006/2018-19 dated January 04, 2019 limiting the liability of customers in unauthorized electronic banking transactions in PPIs issued by Authorised Non-banks.

6. Enhancing Security of Card Transactions: RBI has issued circular no. DPSS.CO.PD No.1343/02.14.003/2019-20dated January 15, 2020on further enhancing security of card transactions.

7. Ombudsman Scheme for Digital Transactions: RBI has launched a scheme 'Ombudsman Scheme for Digital Transactions, 2019' on January 31, 2019 to provide for a mechanism of Ombudsman for redressal of complaints against deficiency in services related to digital transactions. The Scheme came into force on January 31, 2019. And the system participants defined under the scheme are to be complied with the provisions of the scheme. The scheme is available at the following path on RBI website: https://rbidocs.rbi.org.in/rdocs/Content/PDFs/OSDT31012019.pdf

8. For the purpose of creating awareness RBI is holding e-BAAT program at various locations wherein audience are sensitized about safe digital payments.Also, a campaign named "RBI Kehta Hai" is undertaken through print and electronic media to create awareness in this regard.

****