

GOVT. OF INDIA
MINISTRY OF FINANCE
DEPARTMENT OF FINANCIAL SERVICES

LOK SABHA

UNSTARRED QUESTION No. 3552

TO BE ANSWERED ON THE MARCH 16, 2020/PHALGUNA 26, 1941 (SAKA)

“Cyber Attack on Banking Network”

QUESTION

3552. SHRI HEMANT SRIRAM PATIL: SHRI UNMESH BHAIYYASAHEB PATIL: DR. SUJAY RADHAKRISHNA VIKHE PATIL: SHRI DHAIRYASHEEL SAMBHAJIRAO MANE: DR. SHRIKANT EKNATH SHINDE:

Will the Minister of FINANCE be pleased to state:

- (a) the number of cases of cyber attacks on banking and other cashless networks that have been reported in the country during each of the last three years, State/UT-wise;
- (b) the steps taken/being taken by the Government to check cyber crimes, hacking of transactions involving credit cards and to organise campaigns for building and regaining confidence of citizens; and
- (c) whether the Government has proposed sufficient/ additional budgetary provisions to provide technological support to curb cyber crimes, if so, the details thereof and if not, the reasons therefor?

ANSWER

(MINISTER OF STATE IN THE MINISTRY OF FINANCE)
(SHRI ANURAG SINGH THAKUR)

(a) The State-wise data on frauds reported by Scheduled Commercial Banks and Select Financial Institutions under the category 'Card/Internet - ATM/Debit card, Credit Card and Internet Banking Frauds' for the last three financial years and period ended December 2019 of the current financial year based on date of reporting, where the amount involved is Rupees 1.00 lakh or above is enclosed as Annexure-I.

The State-wise data on frauds reported by Scheduled Commercial Banks and Select Financial Institutions under the category 'Card/Internet - ATM/Debit card, Credit Card and Internet Banking Frauds' for the last two financial years and period ended December 2019 of the current financial year based on date of reporting, where the amount Involved is less than Rupees 1.00 lakh is enclosed as Annexure-II.

(b) & (c) In order to strengthen the security of digital transactions, Reserve Bank of India (RBI) reviews the cyber security developments and threats on an ongoing basis and necessary measures are taken to strengthen the cyber resilience of banks. Cyber incidents are analyzed from the point of view of sophistication of attack as well as systemic impact and are categorized as critical, high, medium and low categories.

Wherever required, advisories/alerts are issued to all banks to avoid occurrence of similar incident in other banks.

Reserve Bank of India has also issued circulars dated February 28, 2013 and June 24, 2013 for securing electronic (online and e-banking) transactions advising banks to introduce additional security measures, as under:

- 1) All new debit and credit cards to be issued only for domestic usage unless international use is specifically sought by the customers. Such cards enabling international usage will have to be essentially EMV Chip and PIN enabled.
- 2) Issuing banks should convert all existing MagStripe cards to EMV Chip card for all customers who have used their card internationally at least once (for/through e – commerce/ATM/POS).
- 3) All the active MagStripe International cards used by banks should have threshold limit for international usage which is to be determined by the bank 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.

Further, the Information Technology Act, 2000 has provisions for dealing with various types of cyber crime. Sections 43, 43A, 66, 66B, 66C, 66D, 66E, 66F, 67, 67A, 67B, 71, 72, 72A, 73 and 74 provides punishment/penalty for various cyber crimes. 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.

To spread awareness on cybercrime, Ministry of Home Affairs (MHA) has taken several steps that include dissemination of messages on cybercrime through MHA Twitter handle @cyberDost, radio campaign, publishing of Handbook for Adolescents/Students, publishing of 'Information Security Best practices' for the benefit of Government Officials/ Officers. Organizing of cyber Safety and Security Awareness weeks, in association with police department in different States/UTs etc.

MHA is also implementing a scheme, namely Cyber Crime Prevention against Women and Children (CCPWC) from Nirbhaya Fund of Ministry of Women and Child Development. Under this Scheme, Ministry has provided financial assistance to all States/UTs to set up cyber forensic cum training laboratories, hiring of Junior Cyber Consultant and training/capacity building to provide hands-on training to Law Enforcement Agencies (LEAs) personnel, prosecutors and judicial officers.

**State-wise data on frauds reported by Scheduled Commercial Banks and Select Financial Institutions under the category 'Card/Internet - ATM/Debit card, Credit Card and Internet Banking Frauds' for the last three financial years and period ended December 2019 of current financial year based on date of reporting
(Amount Involved Rupees 1.00 lakh and above)**

State	2016-17		2017-18		2018-19		2019-20 (Up to Q3)	
	No. of FMRs*	Amount Involved in Crores	No. of FMRs	Amount Involved in Crores	No. of FMRs	Amount Involved in Crores	No. of FMRs	Amount Involved in Crores
Andaman & Nicobar Islands					4	0.09	1	0.01
Andhra Pradesh	31	0.64	5	0.16	7	0.15	18	0.87
Arunachal Pradesh			2	0.08			2	0.02
Assam	3	0.11	68	1.37	21	0.60	67	1.12
Bihar	4	0.07	5	0.13	17	0.33	24	0.38
Chandigarh	7	0.19	4	0.06	9	0.18	8	66.43
Chhattisgarh	1	0.01	4	0.12	4	0.12	12	0.21
Goa			2	0.04	10	0.31	4	0.05
Gujarat	16	0.53	23	8.39	39	0.76	32	2.35
Haryana	238	8.28	415	12.94	295	9.09	201	11.79
Himachal Pradesh	1	0.02	2	0.03	1	0.01	9	0.18
Jammu & Kashmir	1	0.09	6	0.19	2	0.04		
Jharkhand	9	0.12	3	0.04	14	0.35	11	0.18
Karnataka	221	9.16	147	7.17	102	2.23	226	13.37
Kerala	9	0.46	13	0.31	17	0.93	37	2.34
Madhya Pradesh	4	0.10	11	0.61	11	0.16	28	0.45
Maharashtra	379	12.10	728	19.54	638	15.62	563	17.89
Manipur					2	0.05		
Meghalaya			1	0.02	2	0.03	4	0.05
Mizoram							2	0.03
Nagaland			2	0.03	1	0.01	3	0.05
New Delhi	156	3.44	196	9.56	242	6.71	209	5.07
Odisha	1	0.06	5	0.24	13	0.27	28	1.23
Overseas	7	0.22	8	0.13	5	0.26	5	0.07
Puducherry	2	0.05	1	0.02	1	0.03	1	0.01
Punjab	3	0.27	23	0.46	18	0.39	21	1.05
Rajasthan	10	0.16	13	0.90	21	0.84	44	7.55
Tamil Nadu	208	4.39	222	40.85	214	10.54	152	5.71
Telangana			54	3.34	39	1.33	32	1.24
Tripura			1	0.02			3	0.03
Uttar Pradesh	37	1.04	55	1.66	77	2.64	86	7.04
Uttarakhand	5	0.13	11	0.18	12	0.19	7	0.14
West Bengal	19	0.67	29	0.98	28	17.11	44	0.65
Grand Total	1372	42.29	2059	109.56	1866	71.38	1884	147.56

* FMRs: Fraud Monitoring Returns

Source: RBI

State-wise data on frauds reported by Scheduled Commercial Banks and Select Financial Institutions under the category 'Card/Internet - ATM/Debit card, Credit Card and Internet Banking Frauds' for the last two financial years and period ended December 2019 of current financial year based on date of reporting (Amount Involved is less than Rupees 1.00 lakh)

State	2017-18		2018-19		2019-20(Up to Q3)	
	No. of FMRs*	Amount Involved in Crores	No. of FMRs	Amount Involved in Crores	No. of FMRs	Amount Involved in Crores
Andaman & Nicobar Islands			6	0.03	19	0.08
Andhra Pradesh	67	0.10	174	0.21	447	0.97
Arunachal Pradesh	9	0.05	1	0.01	4	0.02
Assam	150	0.67	66	0.25	356	1.47
Bihar	45	0.11	134	0.28	236	0.65
Chandigarh	86	0.22	102	0.19	138	0.24
Chhattisgarh	42	0.10	102	0.29	152	0.36
Dadra & Nagar Haveli	10	0.01	16	0.02	21	0.03
Daman & Diu					20	0.04
Goa	16	0.04	104	0.26	172	0.39
Gujarat	540	1.02	1096	1.47	1756	2.44
Haryana	8029	11.11	8688	12.12	4882	5.72
Himachal Pradesh	24	0.13	46	0.16	116	0.40
Jammu & Kashmir	47	0.18	25	0.02	71	0.20
Jharkhand	37	0.11	95	0.25	144	0.35
Karnataka	1426	3.41	1784	2.95	2619	4.20
Kerala	107	0.33	195	0.53	708	1.40
Madhya Pradesh	93	0.23	201	0.46	487	1.28
Maharashtra	14901	23.90	21035	26.73	21334	27.10
Manipur	1	0.00	6	0.02	5	0.02
Meghalaya	7	0.02	10	0.02	16	0.08
Mizoram			5	0.01	6	0.03
Nagaland	7	0.01	2	0.01	6	0.02
New Delhi	1501	3.82	3949	9.05	5290	10.30
Odisha	46	0.11	102	0.26	428	1.32
Overseas	19	0.03	22	0.03	7	0.02
Puducherry	8	0.03	5	0.01	11	0.03
Punjab	191	0.53	270	0.53	480	1.09
Rajasthan	119	0.29	353	0.63	711	1.62
Sikkim	2	0.01	4	0.00	15	0.06
Tamil Nadu	3633	9.50	5283	13.52	5106	11.32
Telangana	532	0.96	935	1.29	1252	1.51
Tripura	5	0.02	9	0.03	22	0.07
Uttar Pradesh	708	1.49	5032	5.17	2044	3.53
Uttarakhand	108	0.39	116	0.34	134	0.31
West Bengal	216	0.51	465	0.88	907	2.21
Grand Total	32732	59.43	50438	78.04	50122	80.89

* FMRs: Fraud Monitoring Returns

Source: RBI

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