GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO 6084
TO BE ANSWERED ON 04.04.2018

CYBER THREAT TO FINANCIAL TRANSACTIONS

6084 SHRI S.P. MUDDAHANUME GOWDA:

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

(a) the State-wise details regarding number of cyber crimes reported during the last three years;

(b) the number of cyber crimes which were financial in nature, year-wise for the last three years,

(c) the percentage increase in such crimes during the said period, State-wise; and

(d) whether the Government has taken any steps to tackle cyber crimes and make online financial transactions foolproof and if so, the details thereof and if not, the reasons therefor?

ANSWER
MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI K.J. ALPHONS)

(a): This department does not have specific information about the above mentioned question. However, as per the details shared by National Crime Records Bureau, a total of 9622, 11592 and 12317 cases were registered under total cyber-crimes (involving computer as medium or target) in the country during 2014, 2015 and 2016.

State/UT-wise cases registered, cases charge-sheeted, cases convicted, persons arrested, persons charge-sheeted, persons convicted under all cyber-crimes during 2014-2016 is enclosed in Annexure-1.

(b) and (c): This department and RBI does not have specific information about the above mentioned question. However, as per incidents reported to Indian Computer Emergency Response Team (CERT-In), 79 phishing incidents affecting 22 financial organisations and 13 incidents affecting ATMs, Point of Sales (POS) systems and Unified Payment Interface(UPI) have been reported during November 2016 to November 2017.

RBI Data on frauds related to ATM / Credit / Debit cards & Net banking related frauds reported by the banks during quarter ended September 2016 upto Dec 21, 2017, is given below:

Details of frauds in(Credit Card, ATM/ Debit Cards & Internet Banking)		
during quarter ended Sept 2016 to Dec 21, 2017		
Quarter ended	**No of frauds cases**	**Amount Involved in Rs Lakhs**
Sep-16	3156	1546.37
Dec-16	4147	3004.16
Mar-17	3077	1330.1
Jun-17	5148	1962.71
Sep-17	7372	3420.86
Upto Dec 21, 2017	10220	11185.73

Source: FMR submitted by the banks

Annexure-2 gives the breakup of NCRB data on cases registered under various provisions of IPC and IT Act, in which some of them pertain to crimes which are financial in nature.

Since the data are obtained from three different sources (CERT-In, RBI and NCRB), state-wise trends for comparable data are not available.

(d): Reserve Bank of India (RBI) and Government have taken adequate measures for Risk Mitigation for Online Payments. RBI periodically reviews the cyber security developments and the threats and takes necessary measures to strengthen the cyber resilience of banks.

The measures taken by RBI and Government to ensure security of digital transactions are at Annexure 3.

****

Annexure – 1

State/UT-wise Cases Registered (CR),Cases ChargeSheeted (CCS),Cases Convicted (CON),Persons Arrested (PAR),Persons Charge Sheeted (PCS) and Persons Convicted (PCV) under Total Cyber Crimes during 2014-2016

S.No.	State/UT	2014						2015						2016					
		CR	CCS	CON	PAR	PCS	PCV	CR	CCS	CON	PAR	PCS	PCV	CR	CCS	CON	PAR	PCS	PCV
1	Andhra Pradesh	282	90	9	236	116	10	536	139	19	522	197	23	616	144	15	307	177	18
2	Arunachal Pradesh	18	0	0	2	0	0	6	5	0	4	4	0	4	1	0	1	1	0
3	Assam	379	22	1	351	22	1	483	84	11	457	83	11	696	114	3	699	117	3
4	Bihar	114	15	1	111	17	1	242	59	1	1567	116	1	309	105	1	285	110	1
5	Chhattisgarh	123	58	0	105	83	0	103	93	19	99	115	29	90	77	18	105	96	19
6	Goa	62	5	1	14	9	2	17	5	0	5	3	0	31	9	0	18	14	0
7	Gujarat	227	71	0	174	109	0	242	119	0	272	310	0	362	146	0	298	231	0
8	Haryana	151	62	3	121	101	4	224	87	2	205	189	2	401	98	12	148	113	14
9	Himachal Pradesh	38	14	0	16	36	0	50	26	1	38	28	1	31	8	0	15	9	0
10	Jammu & Kashmir	37	3	0	4	3	0	34	7	0	12	9	0	28	11	0	21	18	0
11	Jharkhand	93	24	0	57	29	0	180	37	3	172	41	5	259	103	22	288	121	22
12	Karnataka	1020	118	2	372	177	2	1447	186	3	293	264	3	1101	199	7	318	271	7
13	Kerala	450	168	12	283	209	13	290	219	8	191	267	8	283	160	3	227	176	3
14	Madhya Pradesh	289	237	6	386	386	15	231	143	4	230	221	5	258	144	12	261	242	14
15	Maharashtra	1879	445	3	942	641	3	2195	438	2	825	720	4	2380	502	6	1009	768	12
16	Manipur	13	1	0	3	1	0	6	0	0	0	0	0	11	6	0	10	6	0
17	Meghalaya	60	11	0	12	12	0	56	17	1	20	18	2	39	6	0	1	6	0
18	Mizoram	22	4	0	4	4	0	8	11	8	18	11	10	1	2	2	2	2	2
19	Nagaland	0	1	0	0	1	0	0	0	0	0	0	0	2	0	0	1	0	0
20	Odisha	124	17	0	17	17	0	386	65	0	110	90	0	317	135	4	150	151	7
21	Punjab	226	62	7	159	73	7	149	64	17	136	95	24	102	67	15	137	102	21
22	Rajasthan	697	161	7	248	248	8	949	185	10	295	280	11	941	117	6	226	189	10
23	Sikkim	4	0	0	2	0	0	1	1	0	1	1	0	1	0	0	1	0	0
24	Tamil Nadu	172	23	3	120	28	5	142	77	6	125	88	8	144	53	2	96	77	2
25	Telangana	703	61	1	429	80	1	687	105	15	430	136	25	593	182	0	451	211	0
26	Tripura	5	0	0	1	0	0	13	0	0	8	0	0	8	4	0	8	4	0
27	Uttar Pradesh	1737	267	7	1223	383	8	2208	789	89	1699	1375	112	2639	1094	58	2374	1439	80
28	Uttarakhand	42	21	0	39	37	0	48	15	5	23	16	7	62	25	14	40	37	18
29	West Bengal	355	79	2	212	90	2	398	154	0	287	170	0	478	133	0	416	154	0
	TOTAL STATE(S)	**9322**	**2040**	**65**	**5643**	**2912**	**82**	**11331**	**3130**	**224**	**8044**	**4847**	**291**	**12187**	**3645**	**200**	**7913**	**4842**	**253**
30	A & N Islands	13	2	0	5	3	0	6	4	0	2	4	0	3	1	0	1	1	0
31	Chandigarh	55	24	6	45	24	8	77	17	4	22	20	4	26	23	1	26	23	1
32	D&N Haveli	3	0	0	1	0	0	0	1	0	0	1	0	1	3	0	3	3	0
33	Daman & Diu	1	1	0	2	2	0	1	0	0	0	0	0	0	0	0	0	0	0
34	Delhi UT	226	49	5	56	57	5	177	53	3	53	55	3	98	35	0	47	40	0
35	Lakshadweep	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
36	Puducherry	1	0	0	0	0	0	0	1	3	0	1	4	2	4	0	0	4	0
	TOTAL UT(S)	**300**	**76**	**11**	**109**	**86**	**13**	**261**	**76**	**10**	**77**	**81**	**11**	**130**	**67**	**1**	**77**	**71**	**1**
	TOTAL (ALL INDIA)	**9622**	**2116**	**76**	**5752**	**2998**	**95**	**11592**	**3206**	**234**	**8121**	**4928**	**302**	**12317**	**3712**	**201**	**7990**	**4913**	**254**

Source: Crime in India

Annexure – 2

Summary Report on Cases Registered (CR), Cases ChargeSheeted (CCS), Cases Convicted (CV), Persons Arrested (PAR), Persons Chargesheeted (PCS) and Persons Convicted (PCV) under Cyber Crimes during 2014-2016

S.No.	CrimeHead	2014						2015						2016					
		CR	CCS	CV	PAR	PCS	PCV	CR	CCS	CV	PAR	PCS	PCV	CR	CCS	CV	PAR	PCS	PCV
A	IT Act																		
1	IT - Tampering computer source documents	89	18	0	64	19	0	88	36	2	62	54	2	78	32	1	66	43	1
2	IT - Computer Related Offences (Section 66 and Section 66B to 66E)	5548	1094	40	3131	1407	44	6567	1841	159	4217	2558	207	6818	2018	134	4674	2579	172
2.1	Computer Related Offences-Under Section 66	4192	860	38	2423	1125	42	4154	1510	143	3137	2104	179	3321	1453	119	2792	1807	150
2.2	Computer Related Offences-Under Section 66B	82	27	0	53	30	0	132	38	3	91	49	3	196	52	1	150	58	1
2.3	Computer Related Offences-Under Section 66C	784	112	0	446	147	0	1081	160	8	562	210	18	1545	267	5	755	331	8
2.4	Computer Related Offences-Under Section 66D	428	76	2	176	84	2	1083	100	2	327	156	2	1597	205	9	882	300	13
2.5	Computer Related Offences-Under Section 66E	62	19	0	33	21	0	117	33	3	100	39	5	159	41	0	95	83	0
3	IT - Cyber Terrorism (Section 66F)	5	0	0	0	0	0	13	1	0	3	1	0	12	6	0	7	7	0
4	IT - Publication/Transmission of Obscene/Sexually Explicit Content (Sec 67 And Sec 67A to 67C)	758	186	5	491	270	6	816	335	15	555	506	21	957	409	10	829	484	12
4.1	Under Section 67 And Section 67A	749	183	5	487	266	6	792	329	13	545	500	19	930	400	9	810	472	11
4.2	Under Section 67B	5	2	0	3	3	0	8	5	2	7	6	2	17	6	1	15	9	1
4.3	Under Section 67C	4	1	0	1	1	0	16	1	0	3	0	0	10	3	0	4	3	0
5	IT - Intentionally not complying with the Order of Controller	3	0	0	4	0	0	2	3	0	3	5	0	6	1	0	1	1	0
6	IT - Failure to Provide or Monitor or Intercept or Decrypt Information	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
7	IT - Failure to Block Access any Information Hosted etc	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	IT - Not Providing Technical Assistance to Govt. to Enable Online Access	0	0	0	0	0	0	3	0	0	0	0	0	0	2	0	2	2	0
9	IT - Un-authorized Access/Attempt to Access to Protected Computer System	0	0	0	0	0	0	8	3	0	4	4	0	0	3	0	3	3	0
10	IT - Misrepresentation/Suppression of Fact for Obtaining License etc	5	2	0	13	3	0	4	5	0	2	12	0	2	1	0	0	0	0

11	IT - Breach of Confidentiality/Privacy	16	3	0	13	3	0	20	5	2	6	6	2	20	13	0	23	17	0
12	IT - Disclosure of Information in Breach of Lawful Contract	2	1	0	5	5	0	4	1	0	2	2	0	15	3	0	14	9	0
13	IT - Publishing /Making Available False Elect. Signature Certificate	0	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0
14	IT - Create/Publish/Make Available Elec. Signature Certificate for Unlawful Purpose	3	3	0	5	4	0	3	2	0	3	2	0	1	0	0	1	0	0
15	IT - Others	769	144	7	520	220	15	514	164	15	245	352	18	704	222	14	343	269	17
	Total Offences under IT Act (A)	**7201**	**1451**	**52**	**4246**	**1931**	**65**	**8045**	**2396**	**193**	**5102**	**3502**	**250**	**8613**	**2710**	**159**	**5964**	**3414**	**202**
B	**IPC**																		
1	IPC - Offences by Public Servant	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	IPC - Fabrication/Destruction of Electronic Records for Evidence	1	0	0	1	0	0	4	2	1	2	2	1	6	4	0	4	4	0
3	IPC - Cheating	1115	168	2	335	243	3	2255	259	10	754	441	14	2329	355	4	853	569	6
4	IPC - Forgery	63	13	0	58	38	0	45	13	0	72	63	0	81	16	0	64	37	0
5	IPC - Data Theft	55	5	0	11	7	0	84	19	0	135	128	0	86	22	0	34	26	0
6	IPC - Criminal Breach of Trust/Fraud	54	20	0	39	22	0	42	21	0	1292	34	0	56	12	0	20	15	0
6.1	IPC - Credit /Debit Card	10	2	0	3	2	0	18	10	0	18	15	0	26	4	0	4	4	0
6.2	IPC - Others	44	18	0	36	20	0	24	11	0	1274	19	0	30	8	0	16	11	0
7	IPC - Counterfeiting	10	3	0	8	8	0	12	10	0	14	10	0	10	12	0	17	19	0
7.1	IPC - Currency	10	3	0	8	8	0	12	10	0	14	10	0	10	12	0	17	19	0
7.2	IPC - Stamps	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	IPC - Others	974	349	4	772	522	4	980	386	4	598	584	5	950	438	9	793	601	15
	Total Offences under IPC (B)	**2272**	**558**	**6**	**1224**	**840**	**7**	**3422**	**710**	**15**	**2867**	**1262**	**20**	**3518**	**859**	**13**	**1785**	**1271**	**21**
C	**Others Laws**																		
1	Copyright Act, 1957	118	95	18	167	135	23	113	90	26	135	139	32	181	136	29	237	212	31
1.1	Under Section 63	74	60	15	108	80	19	55	54	17	66	80	19	129	89	15	182	164	15
1.2	Under Section 68A	4	3	2	3	3	3	18	12	0	18	16	0	16	16	0	21	17	0
1.3	Others	40	32	1	56	52	1	40	24	9	51	43	13	36	31	14	34	31	16
2	Trade Marks Act, 1999	1	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0
2.1	Under Section 102	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
2.2	Under Section 103	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.3	Under Section 104	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.4	Others	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
3	Other SLL Offences	30	12	0	115	92	0	12	10	0	17	25	0	3	7	0	4	16	0
	Total SLL Offences (C)	**149**	**107**	**18**	**282**	**227**	**23**	**125**	**100**	**26**	**152**	**164**	**32**	**186**	**143**	**29**	**241**	**228**	**31**
	Total Offences under Cyber Crime (A+B+C)	**9622**	**2116**	**76**	**5752**	**2998**	**95**	**11592**	**3206**	**234**	**8121**	**4928**	**302**	**12317**	**3712**	**201**	**7990**	**4913**	**254**

Annexure – 3

The measures taken by RBI are as follows-

1. A comprehensive circular on Cyber Security Framework in Banks issued on June 2, 2016 (DBS.CO/CSITE/BC.11/33.01.001/2015-16), includes section on **'Arrangement for continuous surveillance'** in banks and also covers best practices pertaining to various aspects of cyber security

2. RBI has also set up a Cyber Crisis Management Group to address any major incidents reported including suggesting ways to respond. Based on market intelligence and incidents reported by the banks, advisories are issued to the banks for sensitizing them about various threats and ensure prompt preventive/corrective action.

3. Department of Banking Supervision under RBI, with the help of Indian – Computer Emergency Response Team (CERT-In), conducts cyber security preparedness testing among banks on the basis of hypothetical scenarios.

4. RBI issues Circulars/advisories to all Commercial Banks on phishing attacks and preventive / detective measures to tackle phishing attacks. Banks have also been following the same with their users.

5. RBI has set up a Cyber Security and IT Examination (CSITE) cell in 2015
And carries out Information Technology (IT) Examination of banks separately from the regular financial examination of the banks to assess their cyber resilience. The examination, inter-alia, evaluates the processes implemented by banks for security checks like Vulnerability Assessment (VA) / Penetration Testing (PT) etc. and their follow up action.

6. An inter-disciplinary Standing Committee on Cyber Security at RBI, reviews the threats inherent in the existing/emerging technology and suggests appropriate policy interventions to strengthen cyber security and resilience.

7. RBI has set up an Information Technology (IT) Subsidiary, which would focus, among other things, on cyber security within RBI as well as in regulated entities.

8. Banks and Payment System Operators have been advised to enhance the security and risk mitigation measures for (a) card transactions (includes card based online transactions) and (b) electronic payment transactions (includes e-banking transactions) by taking following measures –

a) Banks have been advised to provide **online alerts** for all card transactions (card present and card not present), vide, RBI circular dated February 18, 2009 (RBI / DPSS No. 1501 / 02.14.003 / 2008-2009) and March 29, 2011 (DPSS. CO. PD 2224 /02.14.003/2010-2011).
b) Banks have been advised, vide, circular February 18, 2009 (RBI / DPSS No. 1501 / 02.14.003 / 2008-2009) and December 31, 2010 (DPSS.CO.No.1503/02.14.003/2010-2011) to put in place a system of providing **additional factor of authentication** (2FA) for all card not present transactions using the information which is not available on the card.
c) Banks have also been advised vide circulars dated February 28, 2013 (DPSS (CO) PD No.1462 / 02.14.003 / 2012-13) and June 24, 2013 (DPSS (CO) PD No.2377 / 02.14.003 / 2012-13) for securing electronic (online and e-banking) transactions, to introduce **additional security measures**.

9. For Non-Bank Entities operating Payment Systems in India, in order to ensure that the technology deployed to operate the payment system/s authorised is/are being operated in a safe, secure, sound and efficient manner, RBI has, vide circulars DPSS.AD.No.1206 / 02.27.005 / 2009-2010 dated December 7, 2009 and DPSS.1444/ 06.11.001/ 2010-2011 dated December 27, 2010, which was subsequently amended vide circular DPSS.CO.OSD.No.2374 / 06.11.001 / 2010-2011 dated April 15, 2011 (copy is available on https: // www .rbi. org. in/ scripts/ FS_Notification .aspx?Id =6344&fn=9&Mode=0), mandated System Audit to be done on an annual basis by Certified Information Systems Auditor (CISA), registered with Information Systems Audit and Control Association (ISACA) or by a holder of a Diploma in Information System Audit (DISA) qualification of the Institute of Chartered Accountants of India (ICAI). Further, the scope of the System Audit should include

evaluation of the hardware structure, operating systems and critical applications, security and controls in place, including access controls on key applications, disaster recovery plans, training of personnel managing systems and applications, documentation, etc. The audit should also comment on the deviations, if any, in the processes followed from the process flow submitted to the Reserve Bank while seeking authorization.

10. With a view to address the issue of cyber resilience, RBI had, vide circular DPSS.CO.OSD.No.1485/06.08.005/2016-17 dated December 9, 2016 (copy is available on https :// www. rbi.org.in / scripts / FS_Notification.aspx ?Id =10772&fn =9&Mode=0), instructed all authorised entities/ banks issuing PPIs in the country to carry out special audit by empanelled CERT-In auditors and take appropriate measures on mitigating phishing attacks.

In addition, details of direction pertaining to security for PPI transactions, are available in section 'Security, Fraud prevention and Risk Management Framework' of the Master Directions for PPI issued by RBI (DPSS.CO.PD.No.1164/02.14.006/2017-18) .

11. RBI has issued various circulars wherein customer banks are advised to educate customers. These circulars are as follows:

a) Card Payments – Relaxation in requirement of Additional Factor of Authentication for small value card present transactions dated May 14, 2015 (DPSS.CO.PD.No.2163/02.14.003/2014-2015).
b) Cash Withdrawal at Point-of-Sale (POS) - Enhanced limit at Tier III to VI Centres dated August 27, 2015 (DPSS.CO.PD.No.449/02.14.003/2015-16).
c) Card Not Present transactions –Relaxation in Additional Factor of Authentication for payments upto 2000/- for card network provided authentication solutions dated December 6, 2016 (DPSS.CO.PDNo.1431/02.14.003/2016-17).
d) Master Direction on Issuance and Operation of Prepaid Payment Instruments dated October 11, 2017 (DPSS.CO.PD.No.1164/02.14.006/2017-18).
e) Banks have also been requested to educate customers about cyber security risks, as per the circular on Cyber Security Framework in Banks dated June 2, 2016 (DBS.CO/CSITE/BC.11/33.01.001/2015-16).

In addition, steps taken by Government to secure digital payment system are as under:

1. Government has formulated Cyber Crisis Management Plan for countering cyber-attacks for implementation by all Ministries/ Departments of Central Government, State Governments and their organizations and critical sectors.
2. CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities along with countermeasures to create awareness among stakeholders to take appropriate measures to ensure safe usage of digital technologies. Regarding securing digital payments, 27 advisories have been issued for users and institutions.
3. CERT-In has empanelled 67 security auditing organizations to support and audit implementation of Information Security Best Practices.
4. All organizations providing digital payment services have been mandated to report cyber security incidents to CERT-In expeditiously.
5. Cyber security exercises are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors. 25 such exercises have so far been conducted by CERT-In where organisations from different States and sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space, IT/ITeS, etc participated.
6. Cyber security awareness sessions are conducted by Ministry of Electronics and Information technology (MeitY) under the Digishala Awareness Campaign.
7. Government has established Botnet Cleaning and Malware Analysis Centre to detect and clean infected systems in the country. The project is initiated in coordination with the Internet Service Providers and Industry.
8. Government has issued general guidelines for Chief Information Security Officers (CISOs) for securing applications and infrastructure and their key roles and responsibilities for compliance;
9. CERT-In is regularly conducting cyber security trainings for IT / cyber security professionals including CISOs of Government and critical sector organisations to give an exposure on current threat landscape and

countermeasures. In addition, CERT-In has also conducted a workshop on security of digital payments systems for stakeholder organisations covering 110 participants.

****