54

STANDING COMMITTEE ON COMMUNICATIONS AND INFORMATION TECHNOLOGY (2023-24)

SEVENTEENTH LOK SABHA

MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

DIGITAL PAYMENT AND ONLINE SECURITY MEASURES FOR DATA PROTECTION

FIFTY-FOURTH REPORT

LOK SABHA SECRETARIAT
NEW DELHI

February, 2024/ Magha, 1945 (Saka)

FIFTY-FOURTH REPORT

STANDING COMMITTEE ON COMMUNICATIONS AND INFORMATION TECHNOLOGY (2023-24)

(SEVENTEENTH LOK SABHA)

MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

DIGITAL PAYMENT AND ONLINE SECURITY MEASURES FOR DATA PROTECTION

Presented to Lok Sabha on 08.02.2024

Laid in Rajya Sabha on 08.02.2024

LOK SABHA SECRETARIAT

NEW DELHI

February, 2024/ Magha, 1945 (Saka)

CCIT No. 398

Published under Rule 382 of the Rules of Procedure and Conduct of Business in Lok Sabha (Sixteenth Edition) and Printed by Lok Sabha Secretariat, New Delhi-110 001.

CONTENTS		
		Pg. No.
	COMPOSITION OF THE COMMITTEE	(ii)
	INTRODUCTION	(vi)
	REPORT	
	PART-I	
1.	Introductory	1-2
2.	Growth of Digital Payments, Acceptance Infrastructure and Payment Ecosystem	2-5
3.	Cyber Fraud Landscape and Statistics	5-16
4.	Existing framework of Cyber Security and Issues related to that	16-26
5.	Steps taken to develop robust security mechanisms for digital payments	26-35
	Annexure-I	
	PART-II	
	OBSERVATIONS/RECOMMENDATIONS	36-46
I.	Minutes of the Second Sitting of the Committee held on 30th October, 2023	47-52
II.	Minutes of the Fourth Sitting of the Committee held on 6th February, 2024	53-54

Composition of the Standing Committee on Communications and Information Technology (2023-24)

Shri Prataprao Jadhav - Chairperson

Lok Sabha

2. Smt. Sumalatha Ambareesh
3. Shri Karti P. Chidambaram
4. Dr. Nishikant Dubey
5. Smt. Sunita Duggal
6. Shri Jayadev Galla
7. Shri S. Jagathrakshakan
8. Smt. Raksha Nikhil Khadse
9. Dr. Sukanta Majumdar
10. Shri P. R. Natarajan
11. Shri Santosh Pandey
12. Dr. Gaddam Ranjith Reddy
13. Shri Sanjay Seth
14. Shri Ganesh Singh
15. Shri Parvesh Sahib Singh
16. Shri Shatrughan Prasad Sinha
17. Shri L.S. Tejasvi Surya
18. Dr. T. Sumathy (A) Thamizhachi Thangapandian
19. Dr. M. K. Vishnu Prasad
20. **VACANT***
21. **VACANT****

Rajya Sabha

22. Dr. Anil Agrawal
23. Dr. Laxmikant Bajpayee
24. Dr. John Brittas
25. Shri Syed Nasir Hussain
26. Shri Ilaiyaraaja
27. Shri Jaggesh
28. Shri Praful Patel
29. Shri Kartikeya Sharma
30. Shri Jawhar Sircar
31. Shri Lahar Singh Siroya

Secretariat

1.	Shri Satpal Gulati	-	Additional Secretary
2.	Smt. A. Jyothirmayi	-	Director
3.	Shri Arjun Choudhary	-	Executive Officer

Committee constituted w.e.f. 13th September, 2023 *vide* Para No.7371 of Bulletin Part-II dated 16th September, 2023.

* Col. Rajyavardhan Singh Rathore resigned from Lok Sabha w.e.f. 06th December, 2023.

** Smt. Mahua Moitra ceased to be a Member of the Lok Sabha w.e.f. 08th December, 2023.

INTRODUCTION

I, the Chairperson, Standing Committee on Communications and Information Technology (2023-24), having been authorized by the Committee do present the Fifty-fourth Report on the subject 'Digital Payment and Online Security Measures for Data Protection' relating to the Ministry of Electronics and Information Technology.

2. The Standing Committee on Communications and Information Technology (2023-24) selected this subject for detailed examination and Report to the Parliament. The representatives of the Ministry of Electronics and Information Technology gave evidence before the Committee on the subject on 30th October, 2023.

3. The Committee at their Sitting held on 6th February, 2024 considered and adopted the Report. The Committee wish to express their thanks to the representatives of the Ministry of Electronics and Information Technology, Ministry of Finance, Ministry of Home Affairs, CERT-In, National Informatics Centre, Reserve Bank of India, National Payments Corporation of India, State Bank of India, Punjab National Bank and Bank of Baroda who tendered their evidence before the Committee and furnished valuable information.

4. The Committee also place on record their appreciation for the invaluable assistance rendered by the officials of Lok Sabha Secretariat attached to the Committee.

5. For facility of reference and convenience the Observations/Recommendations of the Committee have been printed in bold in Part-II of the Report.

New Delhi;
06 February, 2024
17 Magha, 1945 (Saka)

PRATAPRAO JADHAV,
Chairperson,
Standing Committee on
Communications and Information Technology.

REPORT
Part-I
(Narration Analysis)

I. Introduction

Digitalization is the key agenda for Government of India and for any financial organization. It is one of the strongest pillars to strengthen the economy. Consequent upon the allocation of Business Rules *vide* the Cabinet Secretariat Notification No.1/21/1/2017.Cab dated 15th February, 2017 MeitY was assigned the responsibility of "Promotion of Digital Transactions including digital payments". Accordingly, DIGIDHAN Mission was set up at MeitY in June, 2017 for promotion of digital payments. MeitY has been coordinating with multiple stakeholders including Banks, Payment Service Providers for promotion of digital payments across the country. (PNB Background note Page 1) However, in July 2023, the portfolio "Promotion of Digital Payments" has been transferred from MeitY to Department of Financial Services *vide* Cabinet Notification No.1/21/6/2023-Cab. dated 17th July 2023.

2. Launched in July 2015, the Digital India Programme envisioned transforming India into a digitally empowered society and knowledge economy by making available digital infrastructure, digital governance and digital services to every citizen. Concerted efforts by the Government to move to a less-cash economy, by pushing digital payments, have begun to pay rich dividends as the volume of such payments has jumped manifold in the past three years. Digital payment transaction volumes have grown from 2,071crore in FY 2017-18 to 13,462 Crore in FY 2022-23 and crossed 7437 Crore number of digital transactions during current financial year i.e. FY 2023-24 (till 24th September, 2023). Further, digital payments in India are expected to grow over threefold by 2025 due to growing Smartphone penetration, COVID-led changes in consumer behaviour and Government policies for financial inclusion.

3. In view of the significance of Digital Payment sector and rising issues related to cyber security/frauds related to that, the Committee selected the subject "Digital payment and online security measures for data protection" for detailed examination during its current term i.e. 2023-24. Accordingly, the Committee called the representatives of Ministry of Electronics and Information Technology, Ministry of Finance (Department of Financial Services), Ministry of Communications (Department of Telecommunications), Indian Cybercrime Coordination Centre (Ministry of Home Affairs), Indian Computer Emergency Response Team (CERT-In), Reserve Bank of India (RBI), National Payments Corporation of India (NPCI), National Informatics Centre (NIC) and Public Sector Banks (State Bank of India, Punjab National bank and Bank of Baroda) for briefing on the subject on 30.10.2023.The various important aspects/issues related to digital payments and cyber security in financial sector *inter-alia* arising during the examination are highlighted in the following paragraphs.

II. Growth of Digital Payments, Acceptance Infrastructure and Payment Ecosystem

4. According to MeitY, Digital payments have significantly increased in recent years, as a result of coordinated efforts of the Government with all stakeholders and following growth has been noticed with regard to different modes of digital payments:

- Share of UPI transactions increased from 4% in FY2017-18 to over 64% in FY2022-23.
- Volume of BHIM-UPI transactions increased from 92 crore in FY 2017-18 to 8,375 crore in FY 2022-23.
- BHIM-UPI QR codes increased from 9.78 crore in March 2021 to 28.8 crore in August 2023.
- Volume of Bharat Bill Payment System (BBPS) transactions increased from 3 crore in FY 2017-18 to 109 crore in FY 2022-23.
- No. of BBPS Billers increased from 129 in 2018-19 to 21,051 in Aug 23.
- Volume of National Electronic Toll Collection (NETC) transactions increased from 13 crore in FY 2017-18 to 340 in FY 2022-23.

5. When the Committee asked the Ministry of Electronics and Information Technology to furnish the details of share of different modes of digital payments in digital transactions for the last five financial years, the Ministry in their written reply have furnished the following details:

> "The percentage share of different modes of digital payments in digital transactions as provided by RBI for the last five financial years is as provided below:

	Percentage Share of Total Digital Payments									
	Volume					**Value**				
	2018-19	**2019-20**	**2020-21**	**2021-22**	**2022-23**	**2018-19**	**2019-20**	**2020-21**	**2021-22**	**2022-23**
	7	**8**	**9**	**10**	**11**	**7**	**8**	**9**	**10**	**11**
RTGS	**0.587%**	**0.443%**	**0.364%**	**0.289%**	**0.213%**	**78.91%**	**77.24%**	**71.79%**	**71.06%**	**69.47%**
AePS(Fund Transfers)	**0.005%**	**0.003%**	**0.003%**	**0.001%**	**0.001%**	**0.0003%**	**0.0003%**	**0.0004%**	**0.0003%**	**0.0002%**
IMPS	**7.536%**	**7.582%**	**7.501%**	**6.478%**	**4.962%**	**0.97%**	**1.44%**	**2.08%**	**2.39%**	**2.68%**
ECS Cr	**0.023**	-	-	-	-	**0.008%**	**0.003%**	-	-	-

	%									
ECS Dr	**0.004 %**	-	-	-	-	**0.001%**	**0.000%**	-	-	-
NACH	**12.3%**	**9.9%**	**9.3%**	**5.8%**	**4.4%**	**0.82%**	**1.07%**	**1.55%**	**1.40%**	**1.47%**
NEFT	**10.0%**	**8.1%**	**7.1%**	**5.6%**	**4.6%**	**13.92%**	**14.17%**	**17.77%**	**16.47%**	**16.16%**
UPI	**23.2%**	**36.8%**	**51.1%**	**63.8%**	**73.5%**	**0.536%**	**1.316%**	**2.901%**	**4.826%**	**6.668%**
BHIM Aadhaar Pay	**0.03%**	**0.03%**	**0.04%**	**0.03%**	**0.02%**	**0.0005 %**	**0.0008 %**	**0.0018 %**	**0.0035 %**	**0.0033 %**
NETC (linked to bank account)	**0.003 %**	**0.027 %**	**0.149 %**	**0.168 %**	**0.143 %**	**0.0000 1%**	**0.0001 2%**	**0.0006 5%**	**0.0009 7%**	**0.0012 5%**
Credit Cards	**7.6%**	**6.4%**	**4.0%**	**3.1%**	**2.6%**	**0.37%**	**0.45%**	**0.45%**	**0.56%**	**0.69%**
Debit Cards	**19.0%**	**14.9%**	**9.2%**	**5.5%**	**3.0%**	**0.36%**	**0.43%**	**0.47%**	**0.42%**	**0.35%**
Prepaid Payment Instruments	**19.8%**	**15.9%**	**11.3%**	**9.1%**	**6.6%**	**0.13%**	**0.13%**	**0.14%**	**0.16%**	**0.14%**
Total Digital Payments	**100.0 %**	**100.0 %**	**100.0 %**	**100.0 %**	**100.0 %**	**100.0%**	**100.0%**	**100.0%**	**100.0%**	**100.0%**

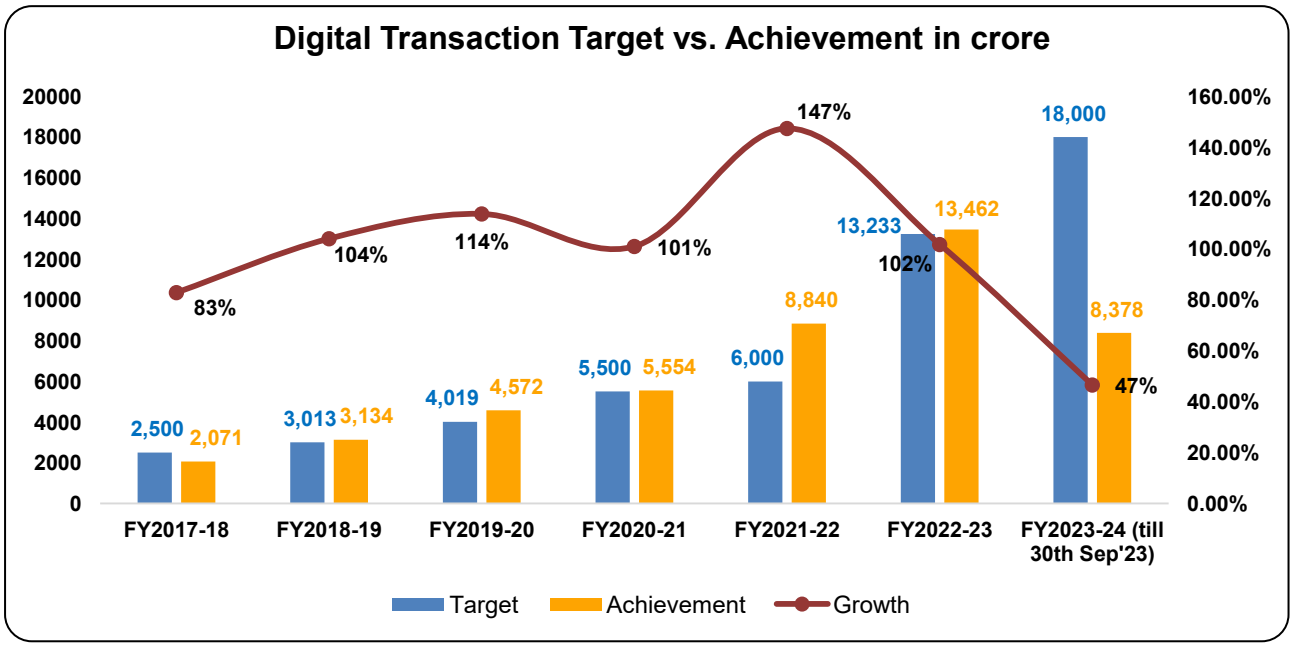
6. Regarding the share of Indian origin/owned/operated apps/platforms/digital payment operators in the digital payment domain, the Ministry in their written reply have provided the following information:

> **"**The percentage wise volume share of key market players of UPI is stated below:

Month	**%Share of Google Pay**	**%Share of Phone Pe**	**%Share of PayTM**	**%Share of AmazonPay**	**%Share of BHIM**	**%Share of WhatsApp Pay**	**%Share of Cred**
Apr-Jun22	34.60%	46.71%	13.31%	1.25%	0.43%	0.16%	0.23%
Jul-Sep22	33.79%	47.63%	13.40%	0.96%	0.38%	0.10%	0.23%
Oct-Dec22	34.53%	46.99%	13.54%	0.81%	0.34%	0.13%	0.35%

Jan-Mar23	34.94%	46.99%	13.64%	0.63%	0.30%	0.15%	0.47%
Apr-Jun23	34.91%	47.66%	13.13%	0.58%	0.25%	0.17%	0.65%
Jul-Sep23	35.49%	47.28%	12.81%	0.50%	0.24%	0.19%	0.81%
Oct-Nov23	36.39%	46.91%	12.32%	0.44%	0.22%	0.20%	0.83%

Digital Transaction Target vs. Achievements from FY 2017-18 to FY 2023-24 (till 30th Sept. 2023)



7. **Digital Payment acceptance infrastructure:** The Ministry has submitted that coordinated efforts of ecosystem partners had led to increase in digital payments acceptance infrastructure in the country. The status is as given below:

Growth of Digital Payment Acceptance System Infrastructures (in Lakhs) from March, 2021 to August, 2023.

Payment System Infrastructures	Mar'21	Aug'23	Growth
BHIM-UPI QR Codes	978.19	2,882	195%
Bharat QR Codes	40.28	59	46%
POS	45.25	82	82%

Source: RBI

8. **Globalisation of Digital Payments:** Regarding platforms for digital payments the Ministry submitted that India's indigenously developed BHIM-UPI and RuPay cards were world class platforms for enabling digital payments. Several countries in Asia, Africa and the Middle East had displayed an inclination towards establishing a 'real time payment system' or 'domestic card scheme' and wish to replicate our model in their country. Government was making efforts to promote these products globally. At present BHIM-UPI was getting accepted at select outlets in Nepal, Bhutan, Singapore, UAE and Mauritius. Similarly, RuPay cards were also being accepted at select outlets in Nepal, Bhutan and Singapore.

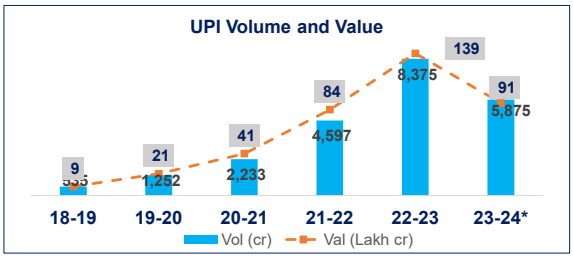
III. Cyber Fraud Landscape and Statistics

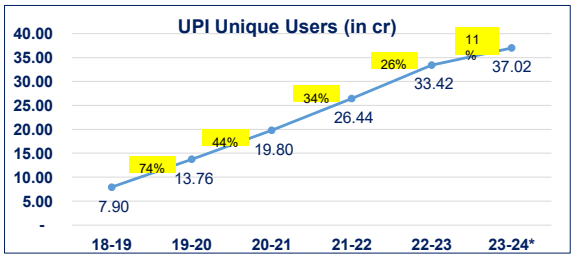
9. While briefing the Committee on the Subject, the Ministry of Home Affairs, outlined the following instances as precursor to cyber frauds:

- "Users fall prey to Greed (e.g. Investment scam), Fear (e.g. disconnection of electricity/KYC) and Ignorance.
- Victims get early benefits on small investment & get duped on making large payment.
- 81% of victims have done at least 10 txns in previous month indicating its not about lack of Product understanding".

UPI Landscape including UPI volume, value, unique users and count of frauds reported till Sept, 2023.

UPI Landscape





UPI	Count of Frauds reported	Fraud Value (in cr)	Fraud v/s Sales	Genuine Txns per Fraud (in Lakhs)
FY 21-22	1,08,509	130.95	0.0016%	1.90
FY 22-23	1,19,067	206.74	0.0015%	3.40
FY 23-24*	70,056	142.52	0.0016%	3.60

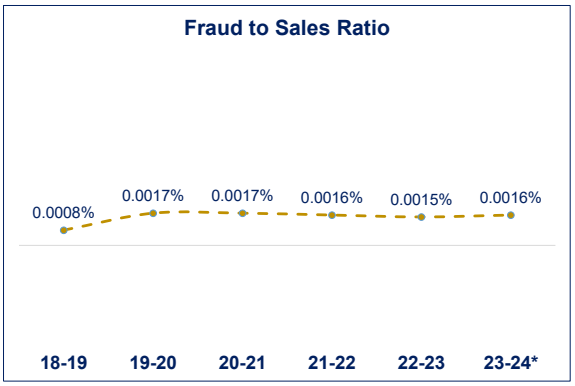
** FY 23-24 pertains to data for Apr'23 to Sept'23 only*

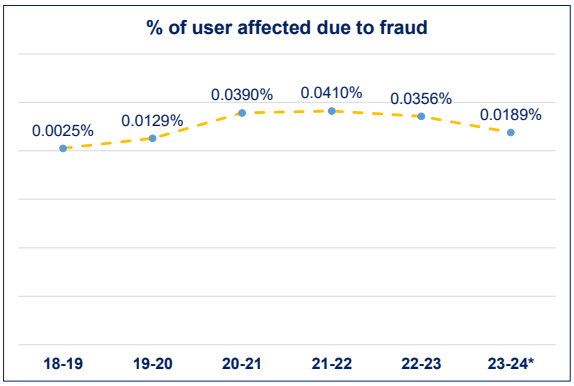
- UPI volume & value has been growing steadily
- Number of unique UPI users have also been increasing
- Genuine transactions per fraud has also been increasing YoY

9

UPI Landscape including Fraud to Sales Ratio and percentage of users affected due to fraud from FY 2018-19 to FY 2023-24(till Sept., 2023).

UPI Landscape





Fraud to sales ratio: Total volume of fraudulent transactions reported in a financial year / total volume of transactions in that financial year

- UPI volume and value have significantly in last 5 years, however, Fraud to Sales Ratio has remained around 0.0015%

10. When the Committee desired to know the details of cyber frauds reported in the last five years according to the apps/platforms/mechanism, the Ministry of Home Affairs in their written submission have furnished the following details:

> "I4C under MHA has developed National Cybercrime Reporting Portal (NCRP) for reporting of all types of cybercrime from anywhere at any time basis. NCRP was launched on 30.08.2019 to enable citizens to report all types of cyber-crimes including financial frauds with special focus of cybercrime against women & children. Since its operationalization, more than 30.60 lakh cyber-crime incidents have been reported through the portal.
>
> **National Cybercrime Helpline number 1930**
> This Helpline number is operational in all States/UTs of the country and are manned by the Police Authorities. Online cyber financial frauds are being reported by the citizens and this is one of the unique facilities available in the country.
>
> Cyber Crime Statistics based on complaints reported on NCRP are as under:

S No.	Category	2021	2022	2023
1	Biometric theft based frauds*	0	0	3986
2	Authorized Push Payments frauds	118525	376531	632267
3	Demat / Depository Fraud	4301	8207	15770
4	Fraud Call/Vishing	27104	55839	66069
5	E-Wallet Related Fraud	28078	30700	23874
6	Business Email Compromise/ Email	1769	2339	2705

	Takeover			
7	Internet Banking Related Fraud	33335	99793	154609
8	Debit/Credit Card Fraud/SIM Swap Fraud	49733	121031	131429

*Note: * This specific category has been introduced in 2023.*

Details of financial fraud complaints reported on NCRP and through helpline 1930 is as under:

Sl. No. (a)	Year (b)	NCRP (c)	Helpline number 1930 (d)	FIR registered by States/UTs for (c) and (d)
1.	2021(from 01.04.23)	26,360	1,08,373	7,385
2.	2022	2,73,235	4,21,205	17,208
3.	2023 (upto 15.11.23)	3,72,173	7,47,888	23,193
	Total	6,71,768	12,77,466	47,786

11. Providing further details on the reporting of cyber frauds, the Ministry of Home Affairs have outlined that:

> "Citizen Financial Cyber Frauds Reporting and Management System (CFCFRMS) has been developed as a part of National Cybercrime Reporting Portal. This module provides an integrated platform, where all stakeholders including Law Enforcement Agencies of States/UTs, all major Banks and financial intermediaries, payment wallets, crypto exchanges and e-commerce companies work in tandem to ensure that quick, decisive, and system-based effective action is taken to prevent the flow of money from victim's account to cyber fraudster's account. The money thus seized is then restored to the victim following due legal process.
>
> The platform enables identification of the various financial channels being misused by the fraudsters for routing the fraud proceeds. Since its launch in April 2021, so far this platform has been able to save more than ₹ 880 crore from going into the hands of fraudsters, and thus benefiting more than 3,50,000 victims.

Details of financial frauds reported on CFCFRMS through National Cybercrime Reporting Portal and National Cybercrime Helpline Number 1930 is as under:

Year	No of Complaints Reported on CFCFRMS	No of Complaints Closed on CFCFRMS	Number of Complaints Where Amount is Put On Hold on CFCFRMS	No of cases in which money is restored to the victim on CFCFRMS
2020	1850	51	17	-
2021	136623	5268	22610	-
2022	513443	45841	97494	95
2023	976441	31428	267866	1112
Total	**1628357**	**82588**	**387987**	**1207**

12. Further, when the Committee raised the issue of complexity of procedure in retrieving the amounts**,** the Committee were informed that:

"On CFCFRMS Platform, 260 entities including 206 banks, 48 wallets, crypto Wallets, merchants, e-commerce platforms, insurance companies and the like have been on-boarded till date. On this platform, complaints are tracked and escalated to the various banks to stop/lien mark the disputed money, while the money is still with these entities. The system has been successful in blocking/lien marking about 10.4% of the transactions reported over the last 3 years".

Year	Amount Lost (Lakhs in INR), as reported by citizens	Amount lien Marked (Lakhs INR)	Amount Returned to Victims (Lakhs in INR)
2021	54714.05	3640.09	0
2022	229479.28	16904.97	57.86
2023	574477.7	67342.19	357.46
Total	858671.03	87887.25	415.32

*upto 31st Oct 2023

The fraudulent money hold in the digital ecosystem is being refunded through Court order, as per the provision of law. Certain issues related to CFCFRMS Platform are being contested in the Courts of Law.

i) The legality of freeze orders u/s 102 CrPC (Criminal Procedure Code) made by Law Enforcement Agencies pertaining to such accounts, even when an FIR is not issued.

ii) How to distinguish a fraudulent transaction from the other genuine ones, when during layering fraudsters, purposely mix genuine transactions with fraudulent ones.

iii) Another area of concern is the process of restoring the frozen money to the victim. Banks and Financial entities have been generally reluctant to order restoration or even interim custody without an investigation or submission made by victims or police agencies.

In few cases, LokAdalat route has been used to obtain such restoration orders. Applications under Sections 451 and 457 of the CrPC are being filed before the Hon'ble Magistrate Courts by the victims for return back of the amounts on lien/frozen.

LEAs of States/UTs are co-coordinating with the judicial officers to ensure streamlining of the return of the amounts on lien/frozen to the victims".

13. During the course of evidence on the subject, some regions/hotspots of cybercrimes were discussed. Regarding this, when the Committee sought details of cyber frauds reported in last five years in these regions/hotspots, the following submissions have been made by the Ministry**:**

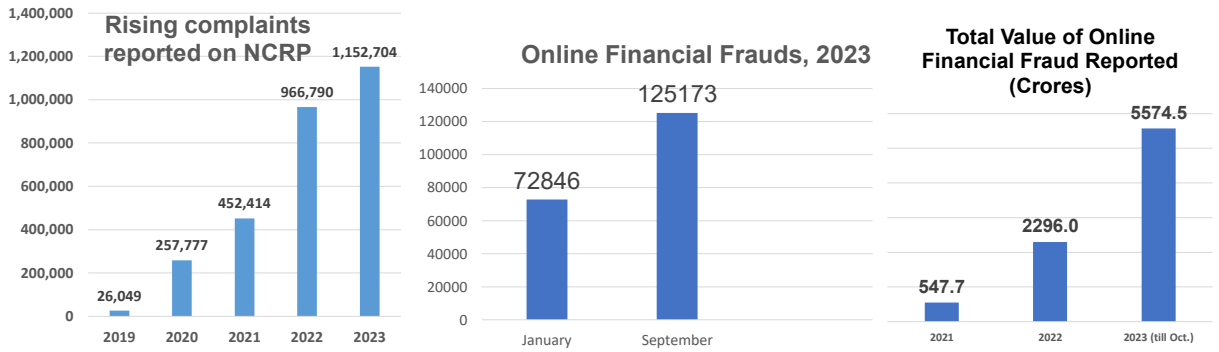
"Hotspots wise details of cyber financial frauds reported on NCRP in last five years is as under:

Sl No	Hotspots	2020	2021	2022	2023
1.	**Mewat Region** (Delhi, Haryana, Uttar Pradesh and Rajasthan)	1055	71586	219736	366490
2.	**Jamtara Region** (Jharkhand, Bihar, West Bengal, Chattisgarh and Odisha)	171	8896	44779	100006
3.	**Ahmedabad Region** (Gujrat, Madhya Pradesh, Dadar& Nagar and Daman & Diu)	60	8247	73482	139547
4.	**Hyderabad Region** (Telangana, Maharashtra, Karnataka and Goa)	351	20896	91902	216309
5.	**Chandigarh Region** (Punjab, Himachal Pradesh, Uttarakhand, Chandigarh, Jammu & Kashmir and Laddakh)	18	6681	25848	40667
6.	**Vishakhapatnam Region** (Andhra Pradesh, Tamil Nadu, Kerala, Pudduchery, A&N Isalnd and Lakshadweep)	175	16417	49867	103205

7.	**Guwahati Region** (Assam, Arunachal Pradesh, Nagaland, Manipur, Mizoram, Tripura, Meghalaya and Sikkim)	20	3900	7830	10218

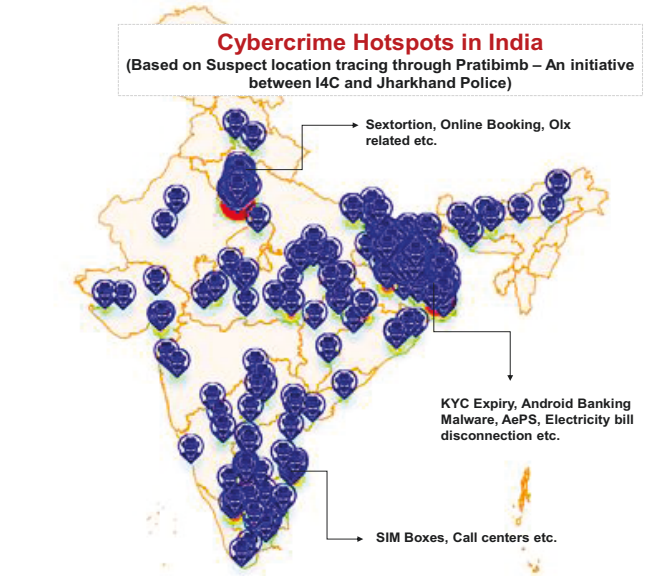
Online Financial fraud statistics as reported on National Cybercrime Reporting Portal (NCRP).

Online Financial Frauds are more than 60% of the total cybercrime complaints reported on **National Cybercrime Reporting Portal (NCRP**).



13

Modus Operandi on Digital Payment Frauds and analysis of data taken from National Cybercrime Reporting Portal (NCRP)



*Indicative representation

Local Origin – Low Value High Volume	International Origin – High Value High Volume
• Customer Care Number / Refund based fraud / KYC expiry – Remote Access	• Investment / Telegram / Task Based scams – Authorized Push Payments
• Sextortion	• Illegal Loan Apps – Unregulated lending
• AePS Frauds – Biometrics Cloning	• Illegal Gaming Apps - Authorized Push Payments
• Online Booking, Fake Franchisee, QR code based etc.	• Matrimony Scams
• Android Mobile Malware	• Ransomware, Hacking etc.

International Hotspots : Dubai, Hong Kong, China, Cambodia, Myanmar

3

14. During examination, the Committee enquired about the quantum of financial fraud reported in the country. To this, the representatives of Ministry of Home Affairs replied as:

> "वर्ष 2021 से 2022 में साइबर फाइनेंशियल फ्रॉड में 128 प्रतिशत की वृद्धि हुई है।इस साल हमारे पोर्टल पर लगभग 5,574 करोड़ रुपये का फ्रॉड रिपोर्ट हो चुका है। पिछले साल 2,296 करोड़ रुपये का फाइनेंशियल फ्रॉड हुआ था"।

15. When the Committee desired to know the types of cyber frauds happening in the country and their origin, the representatives of Ministry of Home Affairs made the following submission:

> "The frauds are happening from two major areas – within the country and without. The frauds which are taking place within the country;

there are two major pockets, one is Mewat region in Rajasthan, Haryana and UP. The second is Jharkhand – Jamtara region; and Bihar. Now it has gone on to West Bengal as well. The Indian fraudsters are largely doing the kinds of frauds such as customer care no., KYC based frauds; remotely accessing the phone, sextortion, largely by Mewat, Aadhar – AEPS frauds, largely from Jharkhand and Bihar; online booking, fake franchise, QR based fraud, now they started writing android malwares also. On the right side, international origin, which is largely done by Chinese actors operating from Dubai, Cambodia, Vietnam and Hong Kong. These are investment scams which run largely through telegrams. Task-based scams, illegal loan apps, illegal gaming apps, ransomware and matrimony scams, largely from Nigeria".

16. When asked to furnish the data of financial frauds particularly about Co-operative Banks vis-a-vis Commercial Banks w.r.t. both the number of frauds and the amount involved, the Ministry of Home Affairs has furnished as follows:

"The data of financial frauds both for Commercial Banks and Co-operative Banks, in terms of number of frauds and amount involved for the last five financial years is tabulated below:

Table 1: Frauds Reported by Commercial Banks and AIFIs (Amount involved ₹1 lakh & above)

FY	No. of Frauds	Amount Involved (₹crore)
2018-19*	6797	71503
2019-20*	8702	185391
2020-21**	7338	132389
2021-22**	9097	59819
2022-23**	13530	30252

*(Source: *Report for Trends and Progress in Banking 2021-22; ** RBI Annual report 2022-23)*
Notes: 1. Refers to frauds of ₹1 lakh and above.
2. The figures reported by banks and AIFI (All India financial institutions) are subject to change based on revisions filed by them.
3. Frauds reported in a year could have occurred several years prior to year of reporting.
4. Amounts involved are as reported and do not reflect the amount of loss

incurred. Depending on recoveries, the loss incurred gets reduced. Further, the entire amount involved in loan accounts is not necessarily diverted.

Table 2: Frauds Reported by UCBs (Amount involved ₹1 lakh & above)		
FY	**No. of Frauds**	**Amount Involved (₹crore)**
2018-19*	1048	625.35
2019-20*	438	6702.39
2020-21**	209	1803.98
2021-22**	304	219.88
2022-23**	633	414.10

Source: RBI, UCBs-Urban Co-operative Banks".

17. When the Committee pointed out that the rising cases of frauds being committed using Aadhaar enabled Payment System (AePS), the representatives of MHA made the following submission:

> "Biometrics cloning: We are seeing this also. They use dummy fingers or rubber fingers to take out money through the Aadhaar-enabled Payment System. This has been enhanced. We are working with the Aadhaar and NPCI to put an end to this. We should see some reduction in the coming weeks".

18. On the issue of banking malwares originating from Google android play store, the Committee were informed as under by the representatives of MHA:

> "Android banking malware: Many of the fraudsters have achieved their level of sophistication and they are sending banking-related malwares. We are seeing some of the malwares which are sent through the SMSes. When a person clicks on the link in the SMS, his phone gets compromised and he would think that he has got a banking application. But actually, it is stealing his credentials. We are working with Google. But everyday new malwares are coming. So, we try to make the Android ecosystem better. We send these samples to Apple as well but this is largely seen in the Android operating system".

19. Regarding the issues related to regulation of Fintech companies in the country, the Committee were informed by the representatives of MHA as follows:

> "What we are seeing is that Fintech companies are being used to launder money also. So, here is one example in which there was an App called Pyypl. The Chinese investment scamsters are using Pyypl. Pyypl is onboarded on to the master card payment system. It is very simple. Anybody using any debit card or credit card can just put the money in Pyypl and withdraw it from any part of the world. So, we are seeing a lot of money going out. The Pyypl App is based in Abu Dhabi. In fact, Abu Dhabi's regulator has fined them also recently about being non-compliant to anti-money laundering legislation. This also highlights the need for a better regulation of the Fintech companies which are operating in the country".

20. Asked to brief about various modes of cyber frauds, the representatives of MHA informed the Committee as follows:

> "Virtual accounts: This is again one issue which the fraudsters have been using. One single current account or an escrow account can be mapped to multiple virtual accounts. The law enforcement agencies do not have any knowledge about what is happening through the virtual accounts. The banks need to closely monitor what they are doing in the virtual accounts and what kind of transactions are taking place in the virtual accounts because this is one of the most common things that we are seeing in the investment scam and also in the loan application scam. One escrow account or one current account can be linked to lakhs of virtual accounts at one go".

21. When the Committee sought to know the modus operandi of frauds using virtual accounts, the representatives of MHA informed the Committee as follows:

> "The person opens an account and I need to receive or pay money to multiple people. What I will do, I will create multiple virtual accounts in the same account and then using a Fintech company, from my virtual account, at one go I will give an instruction to debit or credit money into any of these virtual accounts. It will go through that but visibility will not be there. So, when we look at the transactions, they all will be attributed to one account, that is, the original account".

22. Elaborating further on the issues relating to virtual accounts, the representatives of MHA highlighted that:

"On the issue of for example, if you look at, there are so many loan App-related cases of suicide or harassment in the country. So, what we are seeing, at one go, from multiple virtual accounts the payments are going out. So, the victim will see only one virtual account and it is nowhere recorded. So, how do we go about? Then, we will have to go and write to the law enforcement agencies which freeze the nodal account. So, the nodal account holder will come and say since it is his genuine account, why they are freezing it. So, our portal, the system that we run with all the banks, gets a bad name there. So, that way the virtual accounts are creating problems and there is little KYC for virtual accounts".

23. When the Committee queried about the necessity of virtual accounts when they were being used for cyber frauds, the Ministry of Electronics and Information Technology have made the following submission:

"Virtual accounts are provided by many leading Indian Banks. These accounts are used to create payment aggregator like infrastructure for financial transactions. Each virtual account, created on top of a current bank account, can be used to onboard multiple merchants which practically behave like a separate account. While virtual accounts provide convenience in making fund payments and reconciliation, it has come to notice that virtual accounts are used to mask the funds trail while making payments. Virtual accounts are not monitored at present and may evade AML/CTF mechanism.

Virtual cards provided by international Fintech companies serving as virtual accounts have been used to egress money out of India using VISA and MasterCard network".

IV. **Existing framework of Cyber Security and Issues related to that**

24. As per National Cyber Security Framework, 2013, National Security Council Secretariat (NSCS) is responsible to co-ordinate, oversee and ensure compliance of cyber security policies. Ministry of Home Affairs acts as the nodal Ministry for cyber security and is given the responsibility for framing policies related to classification, handling and security of information relating to Government. Matters relating to cyber laws, administration of the Information Technology (IT) Act 2000 (21 of 2000), other IT related laws are within the purview of Ministry of Electronics and Information Technology (MeitY).

25. Under the Ministry of Electronics and Information Technology, Indian Computer Emergency Response Team (CERT-In) acts as the National agency (under Section 70B

of the IT Act) for cyber security incident response and creates awareness on security issues through dissemination of information. In exercise of its powers under Section 70A of the IT Act, the Central Government has also established the National Critical Information Infrastructure Protection Centre (NCIIPC). NCIIPC is taking all measures including associated research and development for protected systems of Critical Information Infrastructures in India and is designated as the National Nodal Agency in respect of Critical Information Infrastructure Protection ("CIIP").

26. In financial services sector, the regulation and supervision of the financial system in India is carried out by different regulatory authorities. Reserve Bank of India (RBI) plays a critical role in ensuring the cyber security of banks in India through its regular IT examinations, assess bank's compliance with cyber security regulations and guidelines, and identify and address any vulnerabilities in their systems. Insurance Regulatory and Development Authority of India (IRDAI) and Pension Fund Regulatory and Development Authority (PFRDA), under Ministry of Finance play important roles in ensuring the cyber security preparedness of the insurance and pension sector in India.

27. Further, the Ministry of Electronics and Information Technology have submitted that the Hon'ble Finance Minister in the Budget Speech 2017-18, announced setting up of Computer Emergency Response Team in Financial Sector (CERT-Fin). Accordingly, Computer Security Incident Response Team-Finance Sector (CSIRT-Fin) was made operational under the umbrella and leadership of CERT-In. The overall supervisory structure of CSIRT-Fin is through an Advisory committee co-chaired by Secretary, Department of Economic Affairs and Secretary, MeitY.

28. During the course of examination the Ministry of Electronics and Information Technology were asked to elaborate on the institutionalized measures that were taken to combat cyber frauds. To this, the Ministry in their written reply have stated the following:

> "The Government has institutionalized a nationwide integrated and coordinated system to deal with the cyber security threats, which inter alia includes":

i. National Cyber Security Coordinator (NCSC) under the National Security Council Secretariat (NSCS) coordinates with different agencies at the national level for cyber security matters.

ii. The Indian Computer Emergency Response Team (CERT-In) setup by Ministry of Electronics and Information Technology (MeitY) under section 70B of the Information Technology (IT) Act, 2000, for 24x7 cyber security incident response. CERT-In is designated as the national agency for responding to cyber security incidents.

iii. National Cyber Coordination Centre (NCCC) has been setup by CERT-In/MeitY to generate near real-time situational awareness about existing and potential cyber security threats. NCCC provides a structured system and facilitates coordination among different agencies by sharing with them the metadata from cyberspace for taking actions to mitigate the cyber security threats.

iv. CERT-In operates Cyber Swachhta Kendra - CSK (Botnet Cleaning and Malware Analysis Centre) to detect malicious programs and free tools to remove the same, and to provide cyber security tips and best practices for citizens and organisations.

v. National Critical Information Infrastructure Protection Centre (NCIIPC) has been under the section 70A of IT Act, 2000, for protection of critical information infrastructure in the country. NCIIPC provides near real-time threat intelligence and situational awareness based on which regular alerts and advisories are sent to Critical Information Infrastructure (CII) / Protected System (PS) entities.

vi. Department of Telecommunications (DoT) has established Telecom Security Operations Centre (TSOC) for effective management of security incidents including prevention, identification and response system for national telecom infrastructure.

vii. Ministry of Defence has set-up Defence Cyber Agency (DCyA) a tri –service command of the Indian Armed Forces to handle cyber security threats in defense.

viii. MHA has created Indian Cybercrime Coordination Centre (I4C) to deal with cybercrimes in a coordinated and effective manner".

29. While examining the subject, the representatives of Ministry of Home Affairs were queried about the conviction rate in the cases of cyber crime. To this, the following written submission has been made:

> "As per Crime in India (2017-2021) report published by National Crime Record Bureau, details of conviction rate from 2017 to 2021 are as under:

Year	Total cybercrime cases for trial (includes cases under IT Act, IPC and SLL)	Total cybercrime cases disposed off by courts	Cybercrime Cases disposed off without trail (Abated, compounded, withdrawn from prosecution, disposed off by plea bargaining, quashed)	Cyber Crime Cases disposed off after trail	Nature of disposal of cybercrime cases in column 4			% of conviction (All India)	%of conviction (metro-politan cities)
	1	2	3	4	5	6	7	8 = (5/4*100)	9
					C	D	A		
2017	13941	759	85	674	152	22	500	**22.6**	12.5
2018	20320	1354	310	1044	495	36	513	**47.4**	20.2
2019	27826	1426	388	1032	366	57	609	**35.5**	17.2
2020	40656	4420	2794	1626	1110	69	447	**68.3**	28.8
2021	54979	7139	5984	1155	491	87	577	**42.5**	52.3

C- Conviction, D- Discharge, A-Acquittal

30. Concerning about the issue of Aadhaar Enabled Payment System (AePS) frauds, the Committee specifically asked the Ministry whether Aadhaar data had been leaked in instances of misuse of AePS and what actions had been taken to prevent leakage of Aadhar data in misuse of AePS. To this, the Ministry of Electronics and Information Technology in their reply have made the following submission:

> "As reported by UIDAI (Unique Identification Authority of India), no breach of Aadhaar card holders' data has occurred from the Central Identities Data Repository (CIDR) maintained by the UIDAI in which the database of biometric and demographic information of Aadhaar is maintained".

31. On the issue, the Committee were further apprised that:

> "Further, as per National Payments Corporation of India (NPCI) circular dated 26.10.2023, banks are to disable AePS services for accounts with No AePS debit transactions in the preceding 12 months by 30.11.2023

except for the accounts which has received DBT credits and PMJDY, BSBDA accounts".

32. While submitting details about the steps to be taken to prevent AePS frauds, the Committee have been informed by the MeitY as follows:

> "UIDAI has also asked acquirer banks to enforce stringent guidelines/checks for on-boarding of Business Correspondent (BC) agents and Corporate BCs (CBCs) and to ensure the use of verifiable and reliable identity to be used for on-boarding BC, mechanism to obtain police verification during BC on boarding.
>
> UIDAI suggested the mandatory need of reporting of frauds to law enforcement agencies by the issuer and acquirer bank for every case of AePS fraudulent transaction reported and Acquirer banks to file FIR for frauds reports on BC agents after expeditiously investigating the same and issuer banks to file mandatory a complaint on the I4C National Cybercrime Reporting Portal".

33. Further, on the issue of alleged leakage of Aadhaar data of more than 80 Crore citizens, the Committee sought information from the Ministry of Electronics and Information Technology and the following has been submitted:

> i. "The data fields or field name in database structure of sample data either do not exist in the UIDAI database or is different from that of UIDAI database.
>
> ii. UIDAI has neither made available Aadhaar data to ICMR nor authenticated any Aadhaar data held by ICMR.
>
> iii. The source of data is unrelated to UIDAI and there is no leakage of data from UIDAI database.
>
> CERT-In received threat intelligence reports regarding sale of personal data with samples claiming to be of Indian Council of Medical Research (ICMR) and notified ICMR of the same and suggested remedial measures.
>
> CERT-In is coordinating incident analysis with law enforcement agency".

34. When asked whether Operating Systems being used by financial institutions are using updated software for strengthening security, the Ministry of Electronics and

Information Technology have made the following submission:

> "RBI has issued comprehensive guidelines as part of the Cyber security Framework, 2016 emphasizing the critical importance of maintaining up-to-date security posture including application of latest patches and not using End of Life/ End of Support Software. Banks have been advised to continuously monitor the release of patches by various vendors / Original Equipment Manufacturers. Banks have been further advised to periodically evaluate critical devices (such as firewalls, network switches, security devices, etc.) to ensure that their configurations are appropriate to achieve the desired levels of security. The same is monitored through offsite returns and during onsite IT Examination of supervised entities".

35. Outlining the role of nodal officers in Banks/Financial Institutions with respect to Financial frauds, the Ministry of Electronics and Information Technology have submitted as:

- "With regards to the reporting of payment fraud data to Central Payments Fraud Information Registry (CPFIR), following guidelines have been issued by RBI to regulated entities:
- All RBI authorised Payment System Operators (PSOs)/ providers and payment system participants operating in India are required to report all payment frauds, including attempted incidents, irrespective of value, either reported by their customers or detected by the entities themselves.
- The responsibility to submit the reported payment fraud transactions shall be of the issuer bank/ PPI issuer / credit card issuing NBFCs, whose issued payment instrument has been used in the fraud.
- Entities are required to validate the payment fraud information reported by the customer in their own systems to ensure the authenticity and completeness, before reporting the same to RBI on individual transaction basis.
- Entities are required to report payment frauds (domestic and international) to CPFIR as per the specified timelines (currently within 7 calendar days from date of reporting by customer / date of detection by the entity)".

36. When the Ministry were asked whether guidelines related to appointment of nodal officers were also applicable to payment system operators/fintech companies involved in digital transactions business, the following reply have been submitted by MeitY:

> "As per the draft Master Directions on Cyber Resilience and Digital Payment Security Controls for Payment System Operators (PSOs), PSOs shall appoint a dedicated nodal officer(s) to function on 24x7x365 basis

for instant resolution of unauthorised / fraudulent transactions reported by customers and also to facilitate prompt response to Law Enforcement Agencies (LEAs). Comments received for the draft Master Direction are being examined by the Department.

In case of digital lending undertaken by RBI Regulated Entities (RE) through the apps of their outsourced Lending Service Providers (LSP) which are mostly FinTech entities, vide a circular on "Guidelines on Digital Lending" dated September 02, 2022, RBI has mandated REs to ensure that the LSPs appoint suitable nodal grievance redressal officer to deal with FinTech/ digital lending related complaints/ issues raised by the borrowers. If any complaint lodged by the borrower against RE or the LSP engaged by the RE is not resolved by the RE within the stipulated period (currently 30 days), he/she can lodge a complaint over the Complaint Management System (CMS) portal under the Reserve Bank-Integrated Ombudsman Scheme (RB-IOS)".

37. When the Committee pointed out that the number of incidents related to malwares were significantly higher in Android phones, the Ministry of Electronics and Information Technology have submitted the following response:

"Android platforms provide sideloading installation feature which is exploited by cyber criminals for creating Malicious Financial Apps. These apps are developed by cyber criminals and sent to victims via links on messengers/SMSs. Upon installation of these apps by the citizens, sensitive information of phone like SMS, call logs etc gets compromised. I4C, MHA has started maintaining a repository of android and banking malwares causing threat to digital payment security. I4C periodically sends hash values of these apps to Google for appropriate action. More than 200 android and banking malwares have been identified and shared with Google and LEAs. Illegal and fraudulent lending apps are found on both Google Playstore and Apple App Store and these are being regularly sent to these entities for urgent action against such apps".

38. On the number of cases of cyber threat related to malware originating from Google Android play store that have been reported and actions taken in those cases, the Ministry of Electronics and Information Technology have made the following submission:

"It has been observed that adversaries are developing and hosting malicious mobile apps (apk) using various hosting platforms other than Google Play store and then distributing these malicious apk to the targets

by way of SMSs or e-mails masquerading as Credit/Debit card activation, eKYC update etc.

As per the information reported to and tracked by CERT-In, a total number of 141 and 67 incidents related to malicious apk were observed during the year 2022 and 2023 (upto September) respectively from the 3rd party hosting platforms other than Google Play store.

In such cases, CERT-In coordinates response and mitigation measures with concerned service providers and Law Enforcement Agencies".

39. While dealing with the issues related to cyber hacking of Government Infrastructure, the Committee enquired about the number of incidents that have been reported in the last five years in the country. To this the Ministry of Electronics and Information Technology in their reply have submitted:

"As per the information reported to and tracked by CERT-In, a total number of 110, 54, 59, 42, 50 and 58 website hacking incidents of Central Ministries/Departments and State Government organizations were observed during the years 2018, 2019, 2020, 2021, 2022 and 2023 (upto September) respectively".

40. On the need for statutory/legislative measures to be envisaged to address the challenge of cyber frauds, e.g., amendment in IT and other Acts, etc, the Ministry of Electronics and Information Technology in their reply have made the following submission:

"Currently, the Information Technology Act, 2000 ("IT Act") and rules made there under contain several provisions for safeguarding Digital Nagriks from cybercrimes of varied nature. The IT Act penalises various acts relating to computer resources, including those done fraudulently, inter alia, dishonestly or fraudulently damaging computer systems (section 66), identity theft (section 66C), publication of electronic signature for fraudulent purposes (section 74), etc. These offences are in addition to various penal provisions under the Indian Penal Code".

41. Elaborating further on the issue, the MHA have submitted that:

"Frauds of the nature of unauthorized access to computer systems are penalized under section 43 of the IT Act and such acts when done dishonestly and fraudulently are punished with fine and imprisonment under section 66 of the IT Act. The Adjudicating Officer appointed under section 46 of the IT Act (currently the Secretary, Department of IT in the states) is empowered to impose monetary penalties and the offence under section 66 of the IT Act is triable by a court of competent

jurisdiction.

Further, the Central Government, in exercise of powers conferred by IT Act, has notified the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021("IT Rules, 2021") which replaces the Information Technology (Intermediary Guidelines) Rules, 2011 regulating intermediaries. The 2021 Rules cast specific obligation on intermediaries vis-à-vis what kind of information is to be hosted, displayed, uploaded, published, transmitted, stored or shared. Intermediaries are also required to remove any content violative of any law for the time being in force as and when brought to their knowledge either through a court order or through a notice by appropriate government or its authorised agency. In case of failure to follow diligence as provided in the IT Rules, 2021, by intermediaries, they shall lose their exemption from liability under section 79 of the IT Act and shall be liable for consequential action as provided in such law. Further, in case an intermediary is a significant social media intermediary (an intermediary having more than 50 lakh registered users in India), to additionally observe due diligence in terms of appointing, in India, a Grievance Officer, a Chief Compliance Officer and a nodal contact person for 24x7 coordination with law enforcement agencies. As per the IT Rules, 2021, the Chief Compliance Officer is responsible for ensuring compliance with the IT Act and the rules made there under".

42. Regarding the procedure to deal with digital evidence in cases of cyber crimes, the Ministry of Home Affairs in their reply have outlined the procedure as:

"The admissibility of electronic evidence in India is governed by Section 65A and Section 65B of the Indian Evidence Act, 1872 ("Evidence Act"). The provisions were inserted into the Evidence Act by way of the Indian Evidence (Amendment) Act 2000.Section 65A provides that contents of electronic records may be admitted as evidence if the criteria provided in Section 65B are complied with. Section 65B(1) of the Evidence Act establishes that any information present in an electronic record will be considered a document if it is printed on paper or stored, recorded, or copied on optical or magnetic media by a computer. However, this classification as a document is subject to the fulfilment of the conditions mentioned in Section 65B (2), namely:

a. The computer from which the output is produced must have been regularly in use for regular activities by a person who has lawful control over that computer during that period.

b. During the same period, the information contained in electronic records or data derived from other source that is included in an electronic record was regularly fed into the computer from which computer output is produced.

c. During the same period, the computer was working properly. Even when it wasn't working properly, this defect did not affect the electronics record.

d. The information contained in the electronic record reproduces or is derived from such information fed into the computer in the ordinary course of the said activities".

43. Further, the MHA have stated:

"When the conditions under Section 65B(2) are met, the paper containing the information from the electronic record or the optical or magnetic media produced by the computer that stores, records, or copies such information can be presented as admissible evidence in any legal proceedings. In such cases, there is no need for the original record to be provided as evidence, and the paper or media can serve as proof of the original's contents or any facts stated therein where the same is accompanied by a certificate issued under section 65B(4) of the Evidence Act in the manner specified there under. A Section 65B certificate shall have to be produced which identifies the electronic record and gives particulars of the device involved in the production of the electronic record. This certificate shall have to be signed by a person occupying a responsible official position in relation to the operation of the relevant device, or from a person who is in the management of the relevant activities involved. This signature shall be evidence of the authenticity of the certificate".

44. In addition to the above, the MHA have also submitted that:

"In addition to the Evidence Act, the Information Technology Act, 2000 ("IT Act") empowers the Central Government to notify any Department, body or agency of the Central Government or a State Government as the Examiner of Electronic Records under section 79A of the IT Act for the purposes of providing expert opinion on electronic form evidence before any court or authority. Under this provision, the Central Government has notified several agencies to function as the Examiner of Electronic Evidence. A list of all the notifications issued under section 79A of the IT Act may be accessed here. Under Section 45A of the Evidence Act, the Examiner of Electronic Record notified under Section 79A of the IT Act is

an expert and their opinion is a relevant fact in relation to any electronic evidence in any court proceeding".

45. The Committee while examining the various issues involved, sought details of sanctioned strength and current vacancies in the CERT-In and Computer Security Incident Response Team- Finance (CSIRT-Fin). To this, the following details have been provided:

"CERT-In has a sanctioned strength of 142 posts including 127 S&T and 15 non S&T posts out of which 26 posts are currently vacant (23 S&T and 3 non S&T).

CSIRT-Fin is currently managed by 6 officers of CERT-In and regulators i.e. RBI, SEBI and IRDA. Proposal for 25 technical posts for CSIRT-Fin has been included in the overall manpower proposal of CERT-In which is under submission to Department of Expenditure".

46. When asked about the current specialised cyber staff available in the country across institutions and needed specialised staff to ensure cyber security in the country, the Ministry in their written reply have made the following submission:

"As per Data Security Council of India (DSCI), Indian cyber security products and services industry has almost 5,00,000 security professionals working on diverse set of areas in cyber security.

As per NASSCOM strategic review (2023), demand of 2,21,000 cyber security professionals was identified which is in diverse domains of cyber security".

V. **Steps taken to develop robust security mechanisms for digital payments**

47. During cross examination, the Committee highlighted the significance of preventive measures to combat cyber frauds by emphasizing that preventive actions were first line of defence. The Ministry of Electronics and Information Technology in their written reply have outlined the following steps taken by MeitY to prevent Cyber Financial frauds and to strengthen the security:

"Government of India is implementing a Framework for enhancing cyber security, which envisages a multi-layered approach for ensuring defence-in-depth with clear demarcation of responsibilities for threat monitoring assessment, mitigation, risk management, forensics, hardening of systems and audit, R&D, capacity-building in respect of both technical and human resources.

To address the challenges posed by the rapid evolution of cyber threats:

a) MeitY launched G20-Stay Safe Online Campaign in December 2022 during India's G20 Presidency with an objective to raise awareness among citizens to stay safe in online world on the widespread use of social media platforms and rapid adoption of digital payments. The target groups of users are Children/ Students, Women, Senior Citizens, Teachers/ Faculty, General Public, Specially-abled and Government officials. The campaign has been actively promoted by States, UTs, Google, META, CSC, DSCI, CSI, Paytm, NIC, etc. from their respective social media handles.

b) MeitY is observing 'Cyber JagrooktaDiwas' on the first Wednesday of every month since May 2022 onwards towards for capacity building of Government employees and creating awareness for prevention of cyber crimes.

c) MeitY conducts programmes to generate information security awareness. Specific books, videos and online materials are developed for children, parents and general users about information security, which are disseminated through portals such as www.infosecawareness.in and www.csk.gov.in.

d) Government Officials online Training - In December 2020, MeitY initiated two types of online training in cyber security for officials of Central Government Ministries/Departments:

   (i). Generic (Awareness level) training of about 6-8 hrs duration for Government officials/staff and

   (ii). Foundation (Advanced level) training for the officials of Government of India who are technically qualified or those with requisite aptitude in cyber security/IT.
   Both the training programmes are being conducted online.

e) With the increasing digitisation, challenges of online cyber threats have increased manifold. The Government is running capacity building, awareness and training programmes such as :

   (i) **Information Security Education and Awareness (ISEA)**

MeitY is implementing 'Information Security Education and Awareness' (ISEA) programme, which envisions capacity building, promotion of formal/non-formal education, training and creation of mass awareness in the area of Information Security in the country. The academic activities of the project are implemented through a network of 52 academic and training institutions across the country. Mass awareness programmes are conducted across schools, colleges and for senior citizen, women, Government officials and general public.

(ii) **Online trainings in cyber security for Government officials** –

MeitY is running two types of online training courses in Cyber Security for officials of Central Government Ministries/Departments:

- Generic Training in Cyber Security (Awareness training) of about 6-8 hrs duration for all officials/staff.

- Foundation Training (Advance Level) in Cyber Security for technically qualified or with requisite aptitude in cyber security / IT officials.

(iii) **Cyber Surakshit Bharat (CSB)**

This programme was initiated by MeitY on 19th January 2018 in Public-Private Partnership with the objective to educate & enable the Chief Information Security Officers (CISOs) & broader IT community of Central/State Governments, Banks and PSUs to address the challenges of cyber security. Under this programme, CISO Deep Dive training is being conducted in cities such as Delhi, Kolkata, Mumbai, Pune, Bangalore, Chennai, Hyderabad, Vijayawada, Gurugram, Chandigarh and Bhopal.

(iv) **Stay Safe OnlineCampaign**

MeitY launched G20-Stay Safe Online Campaign in December 2022 during India's G20 Presidency with an objective to raise awareness among citizens to stay safe in online world on the widespread use of social media platforms and rapid adoption of digital payments. The target groups of users are Children/ Students, Women, Senior Citizens, Teachers/ Faculty, General Public, Specially-abled and Government officials. The campaign has been actively promoted by States, UTs, Google, META, CSC, DSCI, CSI, Paytm, NIC, etc. from their respective social media handles".

48. Regarding coordinated approach to address the challenges posed by the rapid evolution of cyber threats in the digital payment ecosystem, the Ministry of Electronics and Information Technology in their written reply have outlined the following steps that have been taken by CERT-In to enhance the cyber security posture of digital payment ecosystem and prevent cyber attacks:

i. "Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers and networks on an ongoing basis. CERT-In has issued 71 focused advisories on awareness of security aspects of digital payments, from November 2016 to August 2023, that aim at creating cyber security know-how by analyzing the threat vectors and suggesting best practices for the specific area in cyber security for organisations and users.

ii. Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) of CERT-In is working with various banks and financial institutions to track infected systems and vulnerable services/systems within their networks. Cyber Swachhta Kendra advises the infected/vulnerable systems to Banks and Financial institutions on daily basis along with remedial measures to clean and secure the systems. CERT-In is regularly issuing tailored alerts to financial institutions to enable proactive threat prevention by the respective entities. Currently 240 financial sector organizations are receiving daily inputs related to malware and vulnerable services.

iii. CERT-In is operating incident response help desk wherein incidents like phishing websites which lures victims to divulge sensitive credential information are reported by users and organisations. CERT-In is working in coordination with banks, RBI, Internet Service Providers, Law Enforcement Agencies and international CERTs to track and disable such phishing websites and mitigate fraudulent activities.

iv. CERT-In has formulated a Cyber Crisis Management Plan (CCMP) for countering cyber-attacks and cyber terrorism for implementation by all Ministries/ Departments of Central Government, State Governments and their organizations and critical sectors. Guideline documents and templates have been published to assist development and implementation of sectoral

Crisis Management Plans. CERT-In along with RBI is enabling implementation of CCMP in Banks by means of cyber security framework and best cyber security practices/guidelines.

v. Cyber Security Mock Drills and Exercises are being conducted regularly by CERT-In for assessment of cyber security posture and preparedness of organizations in Government and critical sectors. So far 83 such exercises & drills and table top exercises have been conducted by CERT-In, where 1100 organisations from different States and sectors have participated. CERT-In is enabling the finance sector to deal with cyber-attacks by conducting workshops as well as dedicated cyber security exercises and joint cyber security exercises with Reserve Bank of India (RBI) and Institute for Development and Research in Banking Technology (IDRBT).

vi. CERT-In is providing the requisite leadership for the Computer Security Incident Response Team-Finance Sector (CSIRT-Fin) operations under its umbrella for responding to, containment and mitigation of cyber security incidents reported from the financial sector.

vii. CERT-In operates an automated cyber threat exchange platform for proactively collecting, analysing and sharing tailored alerts with organisations across sectors for proactive threat mitigation actions by them.

viii. CERT-In has empanelled 150 security auditing organisations to support and audit implementation of Information Security Best Practices.

ix. CERT-In has set up the National Cyber Coordination Centre to generate situational awareness regarding existing and potential cyber security threats.

x. As part of services of CERT-In, for creation of awareness in the area of cyber security as well as training / upgrading the technical knowhow of various stakeholders, CERT-In observing the Cyber Security Awareness Month during October of every year, Safer Internet Day on 1st Tuesday of February Month every year, SwachhtaPakhwada from 1 to 15 February of every year and Cyber JagrooktaDiwas (CJD) on 1st Wednesday of every month by organising various events and activities for citizens as well as

the technical cyber community in India. CERT-In, in association with C-DAC, conducted an online awareness campaign for citizens, covering topics such as general online safety, social media risks and safety, mobile related frauds and safety, secure digital payment practices etc. through videos and quizzes on MyGov platform.

xi. CERT-In and the Reserve Bank of India (RBI) jointly carry out a cyber security awareness campaign on 'beware and be aware of financial frauds' through the Digital India Platform".

49. Further, the Ministry of Electronics and Information Technology have also outlined the following steps taken by Reserve Bank of India (RBI) to enhance security of digital payment transactions (including card transactions) and reduce frauds:

i. "It is mandatory to put in place a system of providing for additional authentication/ validation based on information not visible on the cards for all on-line card not present transactions. In case of customer complaint regarding issues, if any, about transactions effected without the Additional Factor of Authentication (AFA), the issuer bank shall reimburse the loss to the customer further without demur.

ii. The mandate for additional authentication / validation shall apply to all transactions using cards issued in India.

iii. Card networks have been advised to ensure mandatory PIN authentication for all transactions performed using credit, debit and prepaid cards – magnetic stripe or EMV Chip and PIN based.

iv. Banks have been advised to put a system in place of online alerts for all types of transactions irrespective of the amount, involving usage of cards at various channels.

v. At the time of issue/ re-issue, all cards (physical and virtual) shall be enabled for use only at contact-based points of usage (viz. ATMs and PoS devices) within India. Issuers shall provide cardholders a facility for enabling card not present (domestic and international) transactions and card present (international) transactions and contactless transactions.

vi. All new cards issued - debit and credit, domestic and international - by banks shall be EMV Chip and PIN based cards.

vii. Instructions have been issued to limit the liability of customers in case of unauthorised electronic payment transactions resulting in debit to PPIs issued by banks and authorised non-banks.

viii. Prepaid Payment Instruments (PPIs) shall establish a mechanism for monitoring, handling and follow-up of cyber security incidents and cyber security breaches. The same shall be reported immediately to DPSS, Central Office, RBI, Mumbai. It shall also be reported to CERT-In as per the details notified by CERT-In.

ix. Banks have been advised to put in place appropriate risk mitigation measures like transaction limit, transaction velocity limit, fraud checks and others depending on the bank's own risk perception, unless otherwise mandated by the RBI.

x. All mobile banking transactions involving debit to the account shall be permitted only by validation through a two-factor authentication (2FA). One of the factors of authentication shall be mPIN or any higher standard".

50. About the measures that have been taken by Department of Telecommunications to prevent the cyber financial frauds, the Committee were apprised as:

"DoT has designed and implemented indigenous AI and Facial Recognition powered solution ASTR for detecting and weeding SIMs taken on fake/forged documents. The vision of ASTR is to generate pro-active digital intelligence and disconnect such SIMs even before they are used in any cyber-crime, financial frauds etc. ASTR is being utilized on pan-India basis. As there is a close relation between cyber-crime and SIMs taken on fraudulent documents. Looking at the seriousness of the matter, DoT field units have been directed to take the matter with States Police for taking legal action against the Point of Sale (PoS) involved in selling such mobile connections Digital Intelligence is being shared with the respective State Police for taking legal action against the perpetrators. List of disconnected fake/forged mobile numbers is being shared with all social media platforms, banks,

financial intermediaries, MEITY, MHA I4C and MCA on regular basis for removal of such mobile numbers from all platforms".

51. On the role of Ministry of Home Affairs, the Ministry of Electronics and Information Technology informed the Committee that Ministry of Home Affairs acts as the nodal Ministry for cyber security and following steps had been taken by MHA to ensure cyber security:

i. "'Police' and 'Public Order' are State subjects as per the Seventh Schedule of the Constitution of India. States/UTs are primarily responsible for the capacity building of their Law Enforcement Agencies (LEAs), prevention, detection, investigation and prosecution of crimes including cyber-crimes through their LEAs. The LEAs take legal action as per provisions of law against the offenders. MHA has taken various steps to enhance security of digital payment transactions (including card transactions) and reduce frauds.

ii. Ministry of Home Affairs, Government has launched the National Cyber Crime Reporting Portal (www.cybercrime.gov.in), to enable public to report incidents pertaining to all types of cyber-crimes, with a special focus on cyber-crimes against women and children. A toll-free number 1930 has been operationalised to get assistance in lodging online cyber complaints.

iii. Coordination mechanism of Law Enforcement Agencies of States/UTs established by constituting Joint Cyber Coordination Teams (JCCT) based upon cybercrime hotspots/areas reporting more cyber crimes and in consultation with States/UTs for; (a) Mewat (Rajasthan, UP, Delhi and Haryana), (b) Jamtara (Jharkhand, West Bengal, Bihar, Odisha, Chhattisgarh and UP), (c) Ahmedabad (Gujarat, MP, Rajasthan, UT of Daman & Diu and DNH), (d) Hyderabad (Telangana, Maharashtra, Karnataka and Goa) (e) Chandigarh (UT of Chandigarh, Punjab, Himachal Pradesh, Uttarakhand, UT of Jammu& Kashmir and UT of Ladakh), (f) Vishakhapatnam (Andhra Pradesh, Tamil Nadu, Kerala, Odisha, UT of Puducherry, UT of A&N Islands, UT of Lakshadweep) and (g) Guwahati (Assam, Nagaland, Arunachal Pradesh, Manipur, Meghalaya, Mizoram, Tripura, Sikkim).

iv. MHA's twitter handle '@CyberDost' to spread awareness on cybercrime prevention. Over 1430 cyber safety tips through short videos, images and creatives have been tweeted. Now, cyberdost

is available at multiple social media handles such as Instagram, Facebook, LinkedIn, YouTube, Public, Koo, sharechat& Telegram. Various videos in relation to cyber safety tips viz. part time job fraud, phishing, ransomware, cyber stalking, internet safety tips, etc have been released on multiple social media platforms by I4C. Published 'Handbook for adolescents/students on cyber safety'. Published 'Information Security Best practices' for the benefit of Government Officials.

v. States/UTs have been requested by MHA to organize "Cyber Jaagrookta (awareness) Diwas" on first Wednesday of every month at 11 am on cyber hygiene and launch mass awareness in vernacular languages for all schools and colleges Universities/ Panchayati Raj Institutions and Municipalities by involving District Magistrates, Police authorities, Officers of Education Department, PRIs etc. MHA on 03.02.2022 published the book "Cyber Pravah", Book for Cyber Awareness, "Cyber Swachhata – General" to tackle the challenges related to Cyber Crime and Cyber Security".

52. When the Committee desired to know how the issues/cases of cyber security having international linkages were being dealt with international cooperation, the Ministry of Electronics and Information Technology in their reply have furnished the following:

"Indian Computer Emergency Response Team (CERT-In) co-operates, works and coordinates incident response measures with international CERTs, overseas organisations and service providers as well as Law Enforcement Agencies.

Further, National Payments Corporation of India(NPCI) which is managing several Digital payments platforms has taken subscription from various threat intelligence feeds to be prepared and receives regular updates from Cert-IN, National Cyber Coordination Centre (NCCC), National Critical Information Infrastructure Protection Centre (NCIIPC), The Institute for Development and Research in Banking Technology (IDRBT), Financial Services Information Sharing and Analysis Center (FS-ISAC) and various other sources on emerging vulnerabilities and threats. NPCI also receive threat intelligence from international channels and have setup a monitoring team that investigates deep and dark web environments, forums, telegram channels etc., to scout for any relevant information. NPCI share this information with various banks and financial institutions for their consumption as well".

53. When the Ministry of Electronics and Information Technology were asked to outline the international best practices in tackling cybercrimes/frauds which could be implemented in India, the following submissions have been made by them:

> "Various countries has adopted innovative modules for tackling the menace of cybercrime. Some of the best practices across the world are as under;
>
> **The Financial Fraud Kill Chain (FFKC)** was created by the FBI and Financial Crimes Enforcement Network (U.S. FIU) in 2016 in response to the rise in business e-mail compromise schemes. The FFKC attempts to aid in the recovery of international wire transfers sent pursuant to fraud schemes by leveraging FinCEN's relationships with the Egmont Group of Financial Intelligence Units.
>
> **FBI's Internet Crime Complaint Center (IC3)** established the Recovery Asset Team (RAT) in order to address vulnerabilities in domestic wire transfers. The RAT streamlines communication withfinancial institutions and assists FBI field offices with the freezing of funds for domestic transfers made under fraudulent pretences. The RAT has experienced a number of notable successes, freezing 73% of funds.
>
> Singapore is leveraging **robotic process automation (RPA)** to obtain banking information at a fraction of the time it previously took. Orders are now served electronically on banks via a standardised template. Banks automate the financial information retrieval process and then send it back to LEAs electronically. The electronic data can also be used immediately for LEA analysis. The process has improved turnaround time by up to 97%, leading to more efficient investigations. Information is now provided in a digital format, which is ready for analyses.
>
> Singapore has established an **Anti Scam Centre** where representatives of all the stakeholders sit together to act on the financial frauds complaints. Similarly, I4C is also in process of creating a National Cyber Frauds Command Centre where representatives of Banks, Fintechs, Telecom Service Providers and Social media platforms may sit together to act on the complaints".

*****

PART-II

RECOMMENDATIONS/OBSERVATIONS

Introductory

1. Digital India programme, launched in 2015 aims at ushering India towards a digitally empowered society and knowledge economy by making available digital infrastructure, digital governance and digital services to every citizen. Under the domain of Digital India, promotion of digital means for payments is one of the significant components to formalise Indian economy. Government in coordination with other stakeholders have undertaken several efforts to promote digital transactions such as concession on Merchant Discount Rate, launch of BHIM UPI and so on. Accordingly, efforts by Government are fructifying as digital transactions have become primary means for business and retail transactions in India. Digital payment transaction volumes have grown from 2,071 Crore in FY 2017-18 to 13,462 Crore in FY 2022-23 and crossed 7437 Crore number of digital transactions during current financial year i.e. FY 2023-24 (till 24th September, 2023). However, success in promotion of digital payments has been facing enormous challenges with the rising online financial frauds, Cyber scams and social engineering tactics to extort money. The Committee are concerned to note that the volume and value of money lost in cyber frauds are very high in comparison to recovery rate which has been abysmally low. According to the submissions made to the Committee, cyber frauds of Rs. 5574 Crore has been reported in the current financial year till September, 2023 on 'National Cybercrime Reporting Portal' which is very much higher than Rs. 2296 Crore of cyber frauds reported in the year 2022. Further, the recovery rate has been about 10.4 per cent of the transactions reported over the last three years i.e. 2020, 2021 and 2022. This scenario brings about a trust deficit in the digital payment system which needs to be attended to at the earliest. In view of this, the Committee took up for an in depth examination of the subject 'Digital payment and online security measures for data protection'. The various issues dealt with are brought out in the following paragraphs.

Need for a multipronged approach to deal with cyber crime

2. According to MeitY, Digital payments have significantly increased in recent years owing to coordinated efforts of the Government with all stakeholders. The total payment transactions volume had increased from 2,071 crore in FY 2017-18 to 13,462 crore in FY 2022-23 and crossed 7437 crore during current Financial year till 24th Sept., 2023. Further, digital payments in India are expected to grow over threefold by 2025 due to growing smartphone penetration, COVID-led

changes in consumer behaviour and Government policies for financial inclusion. The Ministry has submitted that coordinated efforts of ecosystem partners had led to increase in digital payments acceptance infrastructure in the country. This shows that there is a growing penetration of digital payments which is a big step towards formalization of Indian economy. However, the rising cases of cyber frauds is a big challenge to it. Online financial frauds as reported on National Cybercrime Reporting portal (NCRP) constitute more than 60% of the total cyber crime complaints reported. As per Indian Cyber Crime Coordination Centre (14C), cyber frauds that were reported increased by 128% in 2022 in comparison to 2021. This exponential increase of cyber frauds is alarming and the Committee see a necessity to have multipronged approach to deal with the issues of cyber frauds. With a view to tackle this, opining that punitive measures are long drawn, time consuming and less effective, the Committee emphasize on having a multipronged approach with effective coordination of all stakeholders to deal with cyber frauds. The Committee call upon the various Ministries involved to focus on preventive measures to ensure that cyber frauds are held under check and the action taken in this regard may be submitted at the earliest.

<u>Rationalisation of Micro-ATMs and Banking correspondents in hotspots</u>

3. During the course of examination of the subject, the Committee dealt on the various types of cyber frauds that were taking place in the country and were desirous to know the details about them and their origin. To this, the representatives of Ministry of Home Affairs submitted that there were two major pockets where the frauds were taking place within the country and named them as Mewat region in Rajasthan, Haryana and U.P. and Jamtara region in Jharkhand and Bihar. It was added that now it had spread to other regions like West Bengal also. The representatives of MHA elaborated that frauds committed by Indian fraudsters were mainly customer care no. and KYC based frauds; remotely accessing the phone, sextortion, largely by Mewat, Aadhar – AEPS frauds, largely from Jharkhand and Bihar; online booking, fake franchise, QR based frauds and recent addition was writing android malwares also. The Committee were given to understand that cyber scams of local origin were of low value but high volume. Elaborating on the subject further, the Committee were informed that Micro-ATMs installed in these hotspots for the convenience of general public were being used for siphoning off money through cyber frauds. Exhibiting concern on this emerging pattern of exploiting resources meant for financial inclusion and last mile connectivity in rural and remote areas of the country, the Committee urge MeitY to thoroughly look into the matter and formulate region specific strategies to arrest reoccurrence of cyber frauds in these regions. The Committee would also like to urge the Ministry to ensure that these cyber

frauds are dealt with sternly. The Committee would like to be apprised of the action taken in this regard.

Aadhaar Enabled Payment System (AePS) frauds

4. The Committee note that the Aadhaar System is a Unique Data Collection and Storage System which has enabled the Government to launch Aadhaar enabled payment system for financial inclusion in rural and remote areas of the country. An AePS facilitates customers to carry out financial transactions from their Aadhaar linked accounts and biometric authentication. While examining this, the Committee pointed out that the cases of frauds using AePS were on the rise. To this, the Ministry of Home Affairs submitted that biometric cloning was by way of using dummy fingers or rubber fingers to withdraw money through the AePS system. The Ministry assured that they were working with Aadhaar and NPCI to put an end to this and they hoped that there would be reduction in future. Further, expressing concern with regard to security and privacy of Aadhaar data of citizens, the Committee pointedly asked whether there was any breach of Aadhaar Card Holders' data. To this, the Ministry has categorically stated that there has been no breach of Aadhaar Card Holders' data from the Central Identities Data Repository (CIDR) maintained by the UIDAI in which the data base of biometric and demographic information of Aadhaar is maintained. Further, it was stated that CERT-In received threat intelligence reports regarding sale of personal data with samples claiming to be of Indian Council of Medical Research (ICMR) and ICMR was notified of the same and were suggested remedial measures. It was also added then CERT-In is coordinating incident analysis with law enforcement agency. The Committee were apprised that as per National Payments Corporation of India (NPCI) Circular dated 26.10.2023, banks had been directed to disable AePS services for accounts with No AePS debit transactions in the preceding 12 months by 30.11.2023 except for the accounts which had received DBT credits and PMJDY, BSBDA accounts. Among the measures taken to prevent AePS frauds, the Committee have been apprised that UIDAI had asked acquirer banks to enforce stringent guidelines/checks for on-boarding of Business Correspondent agents and Corporate Business Correspondent and to ensure the use of verifiable and reliable identity. UIDAI had also suggested for mandatory need of reporting of frauds to law enforcement agencies. Taking note that the Ministry had put certain concrete measures in place, the Committee urge the Ministry to enforce these measures to the hilt so that there would be tangible outcomes. Expressing surprise with regard to submission of the Ministry in respect of data breach, the Committee do call upon the Ministry to remain vigilant and ensure the safety of Aadhaar Card Holders' data. Regarding intelligence reports received by CERT-In with regard to sale of personal data, the Committee may be apprised about the outcome of the measures suggested and the finding of the analysis by CERT-In.

Virtual accounts used for cyber frauds

5. While briefing the Committee about the various modes of cyber frauds, the representatives of MHA submitted that a virtual account was one such issue which the fraudsters were using for committing frauds. Elaborating on the modus operandi, they submitted that one single current account or an escrow account could be mapped to multiple virtual accounts. The law enforcement agencies would have no knowledge about the happenings through the virtual accounts. They further submitted that the banks had to closely monitor what was happening in the virtual accounts and what kind of transactions were taking place in the virtual accounts as this was one of the common things that was seen in the investment scam and also in the loan application scam. When the Committee sought to know further details on this, the representatives of MHA informed that a person who had to receive or pay money to multiple people would create multiple virtual accounts in the account through which he operates. Then using the Fintech company from the virtual account at one go, instructions would be issued to debit or credit money into all these virtual accounts. The transactions would go through but its visibility would not be there. Further, on looking at the transactions, it would be attributed to one account i.e. the original account. It was further submitted that these virtual accounts were creating problems as there was little KYC for virtual accounts. To a pointed query of the Committee, with regard to the necessity of virtual accounts when they were being used for cyber frauds, the representatives of Meity submitted that these accounts which were provided by leading Indian banks were used to create payment aggregator like infrastructure for financial transactions. They further added that these virtual accounts provided convenience in making fund payments and reconciliation. However, the Ministry had noticed that these virtual accounts were used to mask the funds trail while making payments and at present were not monitored and could evade AML/CTF mechanism. MeitY also submitted that the virtual cards provided by International Fintech companies serving as virtual accounts were used to egress money out of India using VISA and Master Card network. Given the submissions of the various Ministries, the Committee note that there is a very serious lacuna in the banking system which is being exploited by scamsters for committing online financial frauds. Taking the serious view of the situation, the Committee call upon the concerned Ministries to look into these issues at the earliest and evolve a mechanism wherein such misuse can be checked. The Committee would like to be apprised of the action taken in this regard.

Cyber Security Framework

6. While examining the Operating Systems being used by financial institutions, the Committee sought to know whether these financial institutions were using updated software for strengthening security. The Committee were informed that RBI had issued comprehensive guidelines as part of Cyber Security Framework,

2016 wherein emphasis was laid on maintaining up-to-date security including application of latest patches and not using End of Life/End of Support Software. It was added that the banks had been advised to continuously monitor the release of patches by various vendors/Original Equipment Manufacturers and also periodically evaluate critical devices such as firewalls, network switches, security devices and so on, so as to ensure that their configurations are appropriate to achieve the desired levels of security. It was also added that this was being monitored through offsite returns and during onsite IT Examination of supervised entities. Outlining the role of nodal officers in Banks/Financial institutions with regard to financial frauds, the Ministry of Electronics and Information Technology submitted that guidelines had been issued by RBI to regulated entities with regard to reporting of payment fraud data to Central Payments Fraud Information Registry (CPFIR). Elaborating on this, the Committee were informed that all the RBI authorized payment system operators/providers and payment system participants operating in India are required to report all payment frauds including attempted incidents irrespective of value either reported by their customers or detected by the entities by themselves. The guidelines included that the responsibility to submit the reported payment for transaction was with the issuer of bank/PPI issuer/credit card issuing NBFCs, whose payment instruments have been used in the fraud. Before reporting to RBI on individual transaction basis, entities are required to validate the payment fraud information reported by the customer in their own system to ensure authenticity and completeness. Further, the timeline specified was that entities are required to report payment frauds both domestic and international to CPFIR within 7 calendar days from the date of reporting by customer/date of detection by the entity. Noting the various steps taken by the Ministry with regard to strengthening security in financial institutions, the Committee would like to know to what extent these measures have been successful in checking financial frauds/helped in reporting frauds so as to ensure the customers are put to least trouble. The Committee may be apprised of the action taken in this regard.

<u>Cyber Security of Android Play Store</u>

7. Dwelling on the incidents of cyber fraud, the Committee pointed out the number of incidents related to malwares were significantly higher in Android phones and sought the comments of Ministry of Electronics and Information Technology. Elaborating on this, the Ministry submitted that Android platforms provide side loading installation feature which is exploited by cyber criminals for creating Malicious Financial Apps. These apps are developed by cyber criminals and sent to victims via links on messengers/SMSs. Upon installation of these apps by the citizens, sensitive information of phone like SMS, call logs etc gets compromised. I4C, MHA has started maintaining a repository of android and banking malwares causing threat to digital payment security. I4C periodically sends hash values of these apps to Google for appropriate action. More than 200

android and banking malwares have been identified and shared with Google and LEAs. Illegal and fraudulent lending apps are found on both Google Playstore and Apple App Store and these are being regularly sent to these entities for urgent action against such apps. From the submissions of the Ministry, it is seen that MHA has started maintaining a repository of Android and banking malwares which are causing threat to digital payment security. The Committee would like to know how effective has this measure been in containing/checking such frauds. The Committee would also like to know the action taken by Google and Law Enforcement Agencies with regard to the information that has been sent to them for taking urgent action.

Compliance to guidelines issued by RBI from Banks

8. While dwelling on the issue of regulation of the payment sector, the Committee have been informed that Reserve Bank of India issues guidelines related to safe and secure digital banking system from time to time to all the Scheduled Commercial Banks, Cooperative Banks, Payment system operators and others. RBI also regulates online fintech companies involved in Digital Payment sector having no physical presence. Further, the Committee have been informed that as per the draft Master Directions on Cyber Resilience and Digital Payment Security Controls for Payment System Operators (PSOs), shall appoint a dedicated nodal officer(s) to function on 24x7x365 basis for instant resolution of unauthorised/fraudulent transactions reported by customers and also to facilitate prompt response to Law Enforcement Agencies (LEAs). The Committee would like to emphasize on the significance of nodal officers for not only redressal of grievances of citizens related to cyber frauds but also for prompt response by Law Enforcement Agencies. The Committee would also like to be apprised once these draft directions are finalized and issued for compliance. Further, the Committee would like to stress that these directions may be formulated wherein lack of compliance of these guidelines would be taken seriously and dealt sternly with the Payment System operators, banks and other financial entities. The Committee may be apprised of the action taken in this regard.

Rate of recovery and Grievance Redressal Mechanism

9. The Committee during the course of examination noted that online financial frauds are rising at an alarming rate and in comparison to that recovery made and the amount returned to the victim is very low. As per the data furnished by I4C, Rs. 547.14 Crore amount was lost in cyber frauds in the year 2021 as reported by citizens, however, no amount could be returned to victims in the year 2021. Similarly, Rs. 2294.79 Crore was lost in cyber frauds in the year 2022 by victims but only .57 Crore was returned to the victims in 2022. The Committee have also been informed that the system has been successful in blocking/lien marking about 10.4 per cent of the transactions reported over the last 3 years i.e. 2020, 2021 and 2022. Further, the Committee during the course of evidence raised the

issue of complexity of procedure to file complaints and procedure involved in retrieving the money lost in the cases of cyber frauds. The Committee found that there is a high turnaround time to close the complaint to the satisfaction of the complainant. The Committee note with concern that the recovery percentage in the cases of cyber frauds is abysmally low. The Committee would like to impress upon the Ministry to take concerted efforts in ensuring that the defrauded money is recovered. The Committee have been informed that the fraudulent money hold in the digital ecosystem is being refunded through court order, as per the provision of law and there are certain issues related to CFCFRMS platform that are being contested in the court of law. In this context, not delving on the legal aspects involved, the Committee urge the Ministry to streamline the process of the return of the amounts on lien/frozen to the victims and apprise them of the actions taken in this regard.

Coordination among the agencies involved in tackling cybercrimes

10. The Committee note that in this era of digital India, there is increasing threat of online financial frauds, cyber scams and social engineering tactics to extort money for financial gains and nefarious motives. Further, there are several methods being employed by fraudsters to dupe people. The quantum and magnitude of cyber frauds are increasing at an alarming rate. Accordingly, to combat these cyber frauds a multistakeholder approach is required to tackle scamsters. The Committee note that issues related to cyber security are diverse in nature ranging from hacking of critical digital infrastructure to social engineering techniques to lure people for quick financial gains. It is not possible for a single agency to focus on all aspects of cyber security. Accordingly, multiple agencies such as MEITY,I4S, DFS,CERT-In, RBI and NPCI are involved in promotion of Digital Payments, ensuring cyber security and tackling issues related to cyber frauds. The Committee were informed that Indian Cyber Crime Coordination Centre under Ministry of Home Affairs is the nodal agency which works closely with MEITY and CERT-In along with various banks, RBI and NPCI to ensure reduction and mitigation of incidents related to cyber frauds. All these organizations have taken different initiatives at their level to tackle and combat issues related to cyber security and cyber frauds. However, the Committee are concerned to note that effective coordination among the different agencies which is required to tackle cybercrimes is found wanting going by the rising magnitude of cybercrimes. To fight the menace of cybercrimes, better management and coordination among all the agencies involved are sine qua non. The Committee would like the Ministry to see the feasibility of having a nodal centre which houses representatives of all the agencies and address issues holistically. The Ministry may apprise the Committee of the action taken in this regard.

Cyber-attacks on Government agencies

11. The Committee while deliberating on the significance of cyber security of

Government digital infrastructure in the wake of emphasis on Digital India have been apprised by the representatives of CERT-In that attempts are made every day to hack government websites. Even the websites of Indian Space Research Organization were targeted during the launch of Chandrayaan Mission. The Committee while pointing out the issues related to cyber hacking of Government Infrastructure, enquired about the number of incidents that have been reported in the last five years in the country. The Ministry of Electronics and Information Technology have submitted that a total number of 110, 54, 59, 42, 50 and 58 website hacking incidents of Central Ministries/Departments and State Government organizations were observed during the years 2018, 2019, 2020, 2021, 2022 and 2023 (upto September) respectively. Appreciating the efforts of Government agencies to fight this cyber battle on daily basis with state and non-state cyber attackers the Committee emphasize that the cyber security of Government websites and other critical digital infrastructure needs to be strengthened. The Committee were also informed that some Government branches/wings/sections are still using out-dated Windows in their official computer and laptops making them vulnerable for cyber threats. Though MeitY has come up with regular guidelines regarding ensuring cyber security of Government cyber infrastructure, the Committee would emphasize on the adherence to these guidelines and recommend the Ministry to update entire government infrastructure regarding handling of cyber threats. The Committee would like to be apprised of the actions taken in this regard.

<u>Promotion of local players in fintech universe</u>

12. The Committee note that fintech companies, apps and platforms such as PhonePe and Google Pay owned by foreign entities dominate Indian fintech sector. The market share in terms of volume of key players of UPI Google pay and Phonepe was 36.39 per cent and 46.91 per cent respectively in October-November 2023. However, market share by volume of Indigenous BHIM UPI was only 0.22 per cent in the same period. On the other hand, while dwelling on the issue of different modes used by scamsters to dupe people and park illegal money, the Committee have been informed that fintech companies are being used for money laundering also. During the course of evidence, the representatives of I4C gave example of Pyypl app which was being used by Chinese investment scamsters making it difficult for Indian Law Enforcement Agencies to track the trail of the money collected through scams. The Committee highlight that as the magnitude of digital payments increase in India, use of fintech apps is slated to increase for digital financial transactions. In this context, the Committee recommend that there should be focus on promotion of local Indian players in fintech universe. Indigenously developed BHIM UPI is a good example of it, however it's share in the UPI market is very low. The Committee opine that regulation of Indian fintech apps would be more feasible for the regulatory bodies such as RBI and NPCI in comparison to foreign entities which have multiple jurisdictions. As India,

focusing on 'Make in India' in other sectors, the Committee are of the opinion that local entities are to be promoted in fintech sector. The Committee may be apprised of the action taken in this regard.

Lack of Punitive measures to combat cyber frauds

13. While examining the issue of cyber crimes occurring in the Country, the Committee have been informed that 10,30,709 Cyber Crime complaints have been reported on National Cybercrime Reporting Portal in the year 2023 (upto 15.11.23) which is much higher than the 6,94,440 complaints received in the year 2022. The Committee note that cybercrimes are increasing in the country at an exponential rate. However, as per the data furnished by Ministry of Home Affairs the conviction rate in the cases of cyber crimes is very low. As per Crime in India (2017-2021) report published by National Crime Records Bureau, as against the 54979 cyber cases registered for trial in the year 2021, in only 491 cases the accused have been convicted making it only 0.89 per cent of the cases registered. Similarly, in the year 2020, 1110 conviction cases were disposed off after trial out of 40656 total cybercrime cases registered for trial making it only 2.73 per cent of the cases which is not encouraging. The Committee therefore are compelled to conclude that punitive measures have not been very effective in tackling cyber crimes. Expressing concern towards the low conviction rates in the cases of cyber crimes the Committee call upon the Ministry to make all efforts to ensure accused in the cases of cybercrimes are brought to justice. The Committee opine that there is an imperative need for a statutory and legislative overhaul in the domain of cybercrimes and emphasize that punitive measures under the law should act as deterrent for the criminals. The Committee would like to be apprised of the actions taken in this regard.

Requirement of specialised cyber staff

14. The Committee during the course of examination highlighted the need for specialised and trained cyber staff in monitoring and in law enforcement agencies. To assess the current scenario of cyber staff in the country, the Committee enquired about the sanctioned strength and current vacancies in the two specialised agencies dealing with the issues of cyber security and cyber security in financial sector i.e. CERT-In and CSIRT-Fin respectively. In their reply, the Ministry have submitted that CERT-In has a sanctioned strength of 142 posts of which 26 posts are currently vacant. Further, CSIRT-Fin is currently managed by 6 officers of CERT-In and regulators i.e. RBI, SEBI and IRDA. Further, proposal for 25 technical posts for CSIRT-Fin has been included in the overall manpower proposal of CERT-In which is under submission to Department of Expenditure. The Committee emphasize that cyber security has diverse domains and to cater to these domains adequate staff specialised and trained in tackling cybercrimes is need of the hour. Therefore, the Committee recommend the Ministry to assess the staff requirements of these two nodal agencies viz. CERT-In & CSIRT-Fin and

fill the current vacancies at the earliest. The Committee also emphasize that posts in these agencies should not be manned by human resource which have general skills but by human resource with technical expertise as nature of work is purely technical in nature. The Committee have also been informed by the MeitY that as per NASSCOM strategic review (2023), demand of 2,21,000 cyber security professionals was identified which is in diverse domains of cyber security. The Committee stress that the Ministry should focus on the training of staff of Central monitoring agencies and State Law Enforcement Agencies to equip them with the necessary skills and talent required to be cyber security professionals in order to cater to the rising demand in the cyber security domain. The Committee would like to be apprised of the actions taken in this regard.

<u>Use of fintech apps/platforms to sensitize users about safe and secure transactions</u>

15. The Committee note that cyber frauds emanating from digital payments are a serious issue as it not only results in financial loss to vulnerable but also result in loss of trust in the whole ecosystem of digital payments forcing the people to revert back to cash transactions. Owing to quantum of this issue, there is an urgent need to tackle it to provide safe and secure digital payment ecosystem. The Committee have been informed that as precursor to cyber frauds, users fall prey to Greed (e.g. Investment scam), Fear (e.g. disconnection of electricity/KYC) and Ignorance. The Committee while deliberating on the issue emphasized that to address any issue, preventive action is one of the major aspect that can really make a difference. Prevention is the first line of defence and one of the major preventive actions in tackling cyber frauds can be creation of awareness among the users. The Committee have been apprised by the Ministry about the initiatives that are being taken by MEITY, MHA and other stakeholders to sensitize people about safe digital transactions on social media and other platforms like mygov. The Committee, however emphasize on the generation of awareness regarding the fintech apps and platforms such as Paytm, Phonepe and Googlepay itself. Use of fintech apps and platforms for financial transactions have increased multifold due to accessibility and convenience provided by them. Moreover, these apps/platforms or companies operating them run commercial ads to attract attention of citizens towards convenience of using them for financial transactions. These apps also contain details of bank accounts and other personal information of individual users linked to them. The Committee consider that interfaces of these apps can be very significant for generation of awareness regarding not only about safe transactions methods but also about bogus methods being used by fraudsters to dupe people. The Committee, in view of the foregoing recommend the Ministry of Electronics and Information Technology to come up with guidelines for Banks/fintech companies/apps/platforms to focus mainly on generating awareness in the form of creative, pop ups etc. among general public at the interface of apps promoted by them. Further, the Committee

are of the considered view that generation of awareness in local/regional languages to users in rural and remote areas of the country can curb the cases of social engineering to certain extent. The action taken of the Ministry in this regard may be submitted at the earliest.

Institutionalised measures across jurisdictions

16. The Committee during the course of evidence were apprised by the representatives of I4C that the cyber frauds are happening both from within and outside the country. The international origin frauds are largely done by Chinese actors operating from Dubai, Cambodia, Vietnam and Hongkong. These are investment scams which run largely through telegram app. Moreover, task based scams, illegal loan apps, illegal gaming apps, ransomware and matrimony scams were largely from Nigeria. The Committee are concerned about the cybercrimes committed from the other International jurisdictions in India as it is difficult for the agencies to locate the accused due to interspersed jurisdictions. The Committee, therefore recommend that the Ministry may focus on proper coordination with Law Enforcement Agencies of the countries from which these scamsters operate. Further, the best practices of other countries such as the Financial Fraud Kill Chain (FFKC) and FBI's Internet Crime Complaint Center (IC3) both followed in United States of America may be explored for implementation in India as well. The Committee have also been informed that Singapore has established an Anti Scam Centre where representatives of all the stakeholders sit together to act on the financial frauds complaints. The Committee suggest for replication of such nodal point/agency in India and emphasis on prompt action on the scamsters. The Committee would like to be apprised of the actions taken in this regard.

*****

New Delhi;
06 February, 2024
17 Magha, 1945 (Saka)

PRATAPRAO JADHAV,
Chairperson,
Standing Committee on
Communications and Information Technology.

Annexure-I

MINUTES OF THE SECOND SITTING OF THE STANDING COMMITTEE ON COMMUNICATIONS AND INFORMATION TECHNOLOGY (2023-24) HELD ON 30TH OCTOBER, 2023.

The Committee sat on Monday, the 30th October, 2023 from 1130 hours to 1300 hours in Committee Room No. '3', Block 'A' Extension to Parliament House Annexe, New Delhi.

PRESENT

Shri Prataprao Jadhav – Chairperson

MEMBERS

Lok Sabha

2. Shri Sanjay Seth
3. Shri Shatrughan Prasad Sinha
4. Shri L.S. Tejasvi Surya
5. Dr. T. Sumathy (A) Thamizhachi Thangapandian
6. Dr. M.K. Vishnu Prasad

Rajya Sabha

7. Dr. Anil Agrawal
8. Dr. John Brittas
9. Shri Praful Patel
10. Shri Kartikeya Sharma
11. Shri Jawhar Sircar
12. Shri Lahar Singh Siroya

SECRETARIAT

1.	Shri Satpal Gulati	-	Additional Secretary
2.	Smt. A. Jyothirmayi	-	Director
3.	Shri Nishant Mehra	-	Deputy Secretary

Representatives of the Ministry of Electronics and Information Technology (Meity)

Sl. No.	Name	Designation
1.	Shri S. Krishnan	Secretary
2.	Shri Kuntal Sensarma	Economic Adviser
3.	Shri Deepak Goel	Scientist 'G'

Representatives of the Ministry of Home Affairs (MHA)

Sl. No.	Name	Designation
1.	Sh. Rajesh Kumar	CEO, Indian Cybercrime Coordination Centre
2.	Ms. Roopa M.	Director, MHA

Representatives of the Department of Telecommunications

Sl. No.	Name	Designation
1.	Mr. Mukesh Mangal	DDG (AI & DIU)

Representatives from Department of Financial Services

Sl. No.	Name	Designation
1.	Shri Prashant Kumar Goyal	Joint Secretary
2.	Shri Abhijit Phukon	Economic Advisor

Representatives of the CERT-IN

Sl. No.	Name	Designation
1.	Dr. Sanjay Bahl	DG, CERT-IN

Representatives of the NPCI

Sl. No.	Name	Designation
1.	Shri Viswanath Krishnamurthy	Chief Risk Officer, NPCI

Representatives from Reserve Bank of India

Sl. No.	Name	Designation
1.	Shri Gunveer Singh	Chief General Manager
2.	Shri Sandeep Kumar	General Manager

Representatives from State Bank of India

Sl. No.	Name	Designation
1.	Shri Ashwini Kumar Tewari	Managing Director

Representatives from Punjab National Bank

Sl. No.	Name	Designation
1.	Shri Binod Kumar	Executive Director
2.	Shri Hemant Verma	Chief General Manager

Representatives from Bank of Baroda

Sl. No.	Name	Designation
1.	Shri Lal Singh	Executive Director
2.	Ms. K.V. Sheetal	Chief General Manager
3.	Shri Ajay Kumar K.R	CISO

2. At the onset of the Sitting, the Chairperson welcomed the representatives of the Ministry. In his welcome address, the Chairperson highlighted that financial transactions are increasingly moving from real world to the online space and this shift is driven in part by the availability of a wide variety of digital payment options ranging from the Credit/Debit cards, NEFT/IMPS/RTGS, Aadhar Enabled Payments System (AEPS), virtual wallets to the Unified Payments Interface (UPI). He added that the total payment transactions volume increased from 2,071 crore in FY 2017-18 to 13,462 crore in FY 2022-23 and crossed 7437 crore during current Financial year till 24th Sept, 2023. The Chairperson emphasized that while digital payment offered a number of advantages over the conventional cash transactions, its use has its own set of perils including threat to cyber security and personal data breaches.

3. Further, he mentioned that with online fraudsters deploying increasingly sophisticated tools to dupe the unsuspecting victims, the role of cyber security had become sine qua non in this regard and there was a growing realization that the need for online security measures for data protection cannot be overlooked. With the enactment of Digital Personal Data Protection Act, 2023 on 11th August, 2023 obligations were cast on Data Fiduciaries to safeguard digital personal data and held them accountable, apart from enshrining the rights and duties of Data Principals.

4. In this scenario, the Chairperson called upon the Ministry to apprise the Committee of the steps warranted to strengthen basic infrastructure for a shift towards a cashless digital economy, agencies dealing with issues related to digital payments, availability of a user-centric time bound grievance redressal mechanism, adequacy of recently enacted legal framework for ensuring data protection and coordination amongst various stakeholders and so on.

5. Thereafter, the representatives of the Ministry of Electronics and Information Technology made a power-point presentation covering various aspects related to digital payments such as growth trajectory of digital transactions, Growth in Digital Payments Acceptance Infrastructure & Payment Ecosystem and key initiatives taken by MEITY and other concerned government organizations including CERT-In, RBI, NPCI & DOT related to cyber security of Digital Payments such as:

(i). Formulation of a Cyber Crisis Management Plan (CCMP),

(ii). Online training in cyber security for Government officials and Stay Safe Online Campaign,

(iii). Appointment of Chief Information Security Officers (CISOs) in all Scheduled Commercial Banks,

(iv). Establishment of Cyber Swachhta Kendra and National Cyber Coordination Centre by CERT-In,

(v). Real time Fraud Risk Management (FRM) solution for Banks with AI/ML based scoring for all online Products by NPCI,

(vi). Analysing fraud trends and deploying corrective measures on an ongoing basis for the entire ecosystem also by NPCI,

(vii). Issuing Cyber Security Framework of Banks, 2016 and Digital Payments Security Controls, 2021 by RBI, and

(viii). Development and use of Artificial Intelligence, Facial Recognition powered Solution for Telecom SIM Subscriber verification (ASTR), Sanchar Saathi portal and Digital Intelligence Platform (DIP) by Department of Telecommunications.

6. The presentation of MEITY was followed by a power point presentation by Indian Cybercrime Coordination Centre (I4C), MHA outlining various measures taken by MHA to curb cybercrime in the country including coordination with all related stakeholders. It was also highlighted that around 60 percent of all cyber crime cases reported in India were financial frauds in nature.

7. Thereafter, Members sought clarification on various issues which *interalia* included:

(i). Institutional, legislative & statutory measures to combat financial data frauds,

(ii). Preventive measures to tackle cyber crime,

(iii). Punitive measures to check rising reoccurrence of cyber crimes from the same region/areas,

(iv). Lack of data related to conviction rates in cases of cyber crimes,

(v). Complexity in procedures to file complaints and long turnaround time to close the complaint,

(vi). Issues related to tokenization of cards,

(vii). Lack of compliance to guidelines issued by RBI from time to time by Banks,

(viii). Treatment of juvenile cyber crime offenders as adults,

(ix). Need of regular Cyber security awareness drives, and

(x). Regulation of virtual digital assets such as crypto currencies.

8. The Members also raised queries relating to recovery made in the cases of financial frauds, complaints received on Toll Free helpline 1930 and coordination that was lacking among Ministries, RBI, Banks and other stakeholders.

9. The Chairperson, then, thanked the representatives of the Ministries/organizations for deposing before the Committee and asked them to send the replies to the unanswered queries within ten days without fail.

The witnesses then withdrew.

Verbatim Proceedings of the Sitting have been kept on record.

The Committee, then, adjourned.

*****

Annexure-II

STANDING COMMITTEE ON COMMUNICATIONS AND INFORMATION TECHNOLOGY

(2023-24)

MINUTES OF THE FOURTH SITTING OF THE COMMITTEE

The Committee sat on Tuesday, the 6th Feb, 2024 from 1500 hours to 1535 hours in Main Committee Room, Parliament House Annexe, New Delhi.

PRESENT

Shri Prataprao Jadhav- Chairperson

MEMBERS

Lok Sabha

2. Shri Karti P. Chidambaram
3. Smt. Raksha Nikhil Khadse
4. Dr. Sukanta Majumdar
5. Shri Santosh Pandey
6. Shri Shatrughan Prasad Sinha
7. Dr. M.K. Vishnu Prasad

Rajya Sabha

8. Dr. Anil Agrawal
9. Dr. John Brittas
10. Shri Jaggesh
11. Shri Jawahar Sircar
12. Shri Lahar Singh Siroya

SECRETARIAT

4.	Shri Satpal Gulati	-	Additional Secretary
5.	Smt. Jyothirmayi	-	Director
6.	Shri Nishant Mehra	-	Deputy Secretary

2. At the outset, the Chairperson welcomed the Members to the Sitting of the Committee convened to consider and adopt Reports relating to the Ministries/Departments under their jurisdiction.

3. The Committee, then, took up the following draft Reports for consideration and adoption:-

(i) Draft Report on the subject 'Digital Payment and online security measures for data protection' relating to the Ministry of Electronics and Information Technology

(ii) xxxxxxxx……xxxxxxxx……xxxxxxxx……xxxxxxxx

(iii) xxxxxxxx……xxxxxxxx……xxxxxxxx……xxxxxxxx

(iv) xxxxxxxx……xxxxxxxx……xxxxxxxx……xxxxxxxx

4. After due deliberations, the Committee adopted the Reports with slight modifications.

5. The Committee authorized the Chairperson to finalize the draft Reports and present the same to the House during the current Session of Parliament.

The Committee, then, adjourned.

---

xxxxxxxx……xxxxxxxx…. **Matter not related**