59

STANDING COMMITTEE ON FINANCE
(2022-2023)

SEVENTEENTH LOK SABHA

MINISTRY OF FINANCE
(DEPARTMENT OF FINANCIAL SERVICES),
MINISTRY OF HOME AFFAIRS
AND
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

CYBER SECURITY AND RISING INCIDENCE OF CYBER/WHITE COLLAR CRIMES

FIFTY NINTH REPORT

LOK SABHA SECRETARIAT
NEW DELHI

JULY, 2023/ ASHADHA, 1945 (SAKA)

FIFTY NINTH REPORT

STANDING COMMITTEE ON FINANCE
(2022-2023)

(SEVENTEENTH LOK SABHA)

MINISTRY OF FINANCE
(DEPARTMENT OF FINANCIAL SERVICES),
MINISTRY OF HOME AFFAIRS
AND
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

CYBER SECURITY AND RISING INCIDENCE OF CYBER/WHITE COLLAR CRIMES

Presented to Lok Sabha on 27th July, 2023

Laid in Rajya Sabha on 27th July, 2023

LOK SABHA SECRETARIAT
NEW DELHI

JULY, 2023/ ASHADHA, 1945 (SAKA)

CONTENTS

COMPOSITION OF STANDING COMMITTEE ON FINANCE (2022-23)

Shri Jayant Sinha - Chairperson

MEMBERS

LOK SABHA

2. Shri S.S. Ahluwalia
3. Shri Sukhbir Singh Badal
4. Shri Subhash Chandra Baheria
5. Dr. Subhash Ramrao Bhamre
6. Smt. Sunita Duggal
7. Shri Gaurav Gogoi
8. Shri Sudheer Gupta
9. Shri Manoj Kishorbhai Kotak
10. Shri Pinaki Misra
11. Shri Hemant Shriram Patil
12. Shri Ravi Shankar Prasad
13. Shri Nama Nageshwara Rao
14. Prof. Sougata Ray
15. Shri P.V. Midhun Reddy
16. Shri Gopal Chinayya Shetty
17. Shri Parvesh Sahib Singh
18. Dr. (Prof) Kirit Premjibhai Solanki
19. Shri Manish Tewari
20. Shri Balashowry Vallabbhaneni
21. Shri Rajesh Verma

RAJYA SABHA

22. Dr. Radha Mohan Das Agarwal
23. Shri Raghav Chadha
24. Shri P. Chidambaram
25. Shri Damodar Rao Divakonda
26. Shri Ryaga Krishnaiah
27. Shri Sushil Kumar Modi
28. Dr.Amar Patnaik
29. Dr. C.M. Ramesh
30. Shri G.V.L. Narasimha Rao
31. Shri Pramod Tiwari*

SECRETARIAT

1. Shri Siddharth Mahajan - Joint Secretary
2. Shri Ramkumar Suryanarayanan - Director
3. Shri Puneet Bhatia - Deputy Secretary
4. Ms. Abhiruchi Srivastava - Assistant Committee Officer

---

* *Vide* Rajya Sabha Bulletin Part-II no. 63014 dated 13.03.2023, Shri Pramod Tiwari was nominated to the Standing Committee on Finance (2022-23) on 13th March, 2023 *vice* Dr. Manmohan Singh, who resigned from the Committee w.e.f. 9th February, 2023.

INTRODUCTION

I, the Chairperson of the Parliamentary Standing Committee on Finance, having been authorized by the Committee, present this Fifty-ninth Report on the subject 'Cyber Security and Rising Incidence of Cyber/White Collar Crimes'.

2. At their sitting held on 13 February, 2023, the Committee took oral evidence of the officials of the Ministry of Home Affairs [National Crime Training Centre (NCTC)], Ministry of Finance (Departments of Financial Services and Revenue) and Reserve Bank of India (RBI). On 03 May 2023, the Committee heard the views of representatives of Reserve Bank of India, Indian Banks' Association (IBA), National Payments Corporation of India (NPCI) and Computer Emergency Response Team (CERT-In). The Committee further on 01 June, 2023 heard views of National Association of Software and Service Companies (NASSCOM), Chase India, Pine Labs, Razorpay Software Private Limited, QNu Labs, PhonePe and CRED. The Committee again took the oral evidence of Ministry of Home Affairs, Ministry of Finance (Department of Financial Services), Ministry of Electronics and Information Technology (MeitY) and National Payments Corporation of India (NPCI) on the subject on 15 June, 2023. The Committee further on 04 July, 2023 took evidence of the representatives of the Punjab National Bank, Bank of India, Yes Bank and Computer Emergency Response Team (CERT-In) on the subject and also heard views of representatives of various Tech companies *viz* Apple India, Flipkart and One97 Communications Ltd. (Paytm). The Committee again had the oral evidence of officials of Reserve Bank of India and Computer Emergency Response Team (CERT-In) on the subject on 20 July and also interacted with the representatives of Google India.

3. The Committee considered and adopted this report at their sitting held on 20 July, 2023.

4. The Committee wish to express their thanks to the officials of Ministry of Home Affairs [National Crime Training Centre (NCTC)], Ministry of Finance (Departments of Financial Services and Revenue), Ministry of Electronics and Information Technology (MeitY), Reserve Bank of India (RBI), Indian Banks' Association (IBA), Punjab National Bank, Bank of India, National Payments Corporation of India (NPCI), Computer Emergency Response Team (CERT-In), National Association of Software and Service Companies (NASSCOM), Chase India, Pine Labs, Razorpay Software Private Limited, QNu Labs, PhonePe, CRED, , Yes Bank, Apple India, Flipkart, One97 Communications

Ltd. (Paytm) and Google India for appearing before the Committee and furnishing the requisite material and information which were desired in connection with the examination of the subject.

5. The Committee also wish to express their thanks to the Stakeholders/Organisations for providing their views/suggestions against the Press Communiqué on the aforementioned subject.

6. For facility of reference, the Observations/Recommendations of the Committee have been printed in bold at the end of the Report.

NEW DELHI
20 July, 2023
29 Ashadha, 1945 (Saka)

JAYANT SINHA,
Chairperson,
Standing Committee on Finance

PART - I

Chapter – I

A. Introduction:

Cyber space is a complex and dynamic environment for a variety of interactions among people, software, and services supported by world-wide distribution of Information and Communication Technology (ICT) devices and networks. Cyber space has made geographical boundaries irrelevant for the purpose of exchange of information and interaction across the world with advent of innovative technologies and modern gadgets. However, it has also brought challenges in the form of illegal/unwarranted use of cyber space by criminals.

The exponential increase in the number of internet users in India, clubbed with rapidly evolving technologies has brought in its own unique challenges. Technological innovations like rapid digital service adoption, low-cost internet facility without adequate cyber security and lack of cyber literacy has led to increase in cybercrimes and related incidents. Evolving technologies like Internet of Things (IoT), Artificial Intelligence (AI), Drones, etc. have also brought with them significant risks to cyber space.

1.1 Statistics of Cyber Crime:

The National Crime Records Bureau (NCRB) compiles and publishes statistical data on crimes in its publication “Crime in India”. The published reports are available till the Year 2021. The year-wise summary of cases registered during last three years is as under:

Cyber Crimes Cases registered	Year		
	2019	2020	2021
	44,735	50,035	52,974

Fraud for Cyber Crimes Cases registered	Year		
	2019	2020	2021
	6,229	10,395	14,007

As per the information reported to and tracked by CERT-In, 11,58,208, 14,02,809 and 13,91,457 number of cyber security incidents have been observed and handled by CERT-In during the years 2020, 2021 and 2022 respectively. These are various types of cyber security incidents such as Phishing and SMSing, Fake/Malicious Mobile Applications, Ransomware, etc.

The Ministry of Home Affairs in their post evidence replies have furnished the following with regard to whether all the cyber crime cases are being registered:

NCRP is the main portal where cybercrimes are reported nationally. These complaints can be forwarded to CCTNS as the two systems are interfaced. Complaints are also received directly at Police Stations and other higher levels in the states and UTs and may not be available at the NCRP. However, I4C encourages the states and UTs to enter all the complaints into NCRP. This facilitates identification of linkages between crimes and criminals nationally.

Most offences of cybercrime under the Information Technology 2000 are bailable and punishable with up to 3 years of imprisonment".

As per data published by NCRB in 'Crime in India 2021', the conviction rate was 3.6%. As per data available with I4C, in the year 2022 out of 694424 complaints related to financial frauds, in 2.6% cases, FIR were issued.

1.2 Key Characteristics of Cyber Crime:

i. Digital analogy of normal crime committed in physical world
ii. Rapid replication
iii. Vastness of cyberspace makes monitoring difficult
iv. Anonymous, cross-border, multi layered and complex to investigate.
v. Limited resources required for committing cyber crime
vi. Prevention, timely detection, and quick reaction is essential

1.3 Challenges in Cyber Space:

(i) <u>Misuse of Internet</u>

Criminals use digital techniques for committing cybercrimes like financial frauds, ransomware, malware attacks, identity theft, data theft, privacy breach, etc. Due to easy access and extensive use of cyber space, citizens especially women and children are more likely to experience various

forms of cyber crimes, such as online harassment, stalking, bullying, sexting etc.

The COVID pandemic has also led to over-reliance on online medium for day-to-day requirements ranging from buying of basic house hold items, jobs, education, meetings, including financial transactions/businesses, etc. Cyber criminals have utilised this opportunity to commit cyber crime.

(ii) Social media platforms

Major challenges are also being faced on account of increased usage of social media which is multi-jurisdictional and multi-layered in nature and being misused for peddling fake news, wrong information which may trigger law and order problems. Social media platforms provide anonymity thereby making attribution difficult.

(iii) Cyber Literacy/Awareness of general public and Trainings for LEAs:

Low cyber literacy including product literacy (secure use of new technology like UPI, Crypto, IoT, etc.) makes it easier for cyber criminals to dupe citizens.

The lack of specialized investigative skill sets and training of LEAs also poses a challenge in handling of cyber crimes considering rapid technological advancements and frequent changes in modus-operandi by cyber criminals,

1.4 Technological Challenges**:**

i. Many cyber crimes are committed to using modern cyber crime tools, such as malicious software, botnets, onion routing and others. These technologies are used with obfuscation, anonymity, computational power and deniability of trace back to the source.

ii. Malware and botnets allow criminals to avoid technical controls such as antivirus software and internet filters, as well as to avoid law enforcement.

iii. Addressing cyber crime, particularly attribution, requires specialized investigative skill sets and forensic tools. Further, anonymous technologies like TOR network (used for dark web), encryption, absence of support from international intermediaries etc. also make attribution difficult.

1.5 Legal Challenges:

i. The transnational nature of cyber crime leads to jurisdictional complexity, investigation and prosecution is, therefore, time consuming and difficult. Lack of harmonization in legislations among countries leads to difficulty in investigation and prosecution of cyber crimes.

ii. Most of the service providers have their data centers outside the country. Hence seeking data from them remains a challenge despite efforts being made for coordination and collaboration with international agencies.

iii. Information Technology Act, 2000, as amended from time to time, provides the basic legal framework to deal with cybercrimes. However, anonymity, traceability, attribution are key legal challenges.

iv. The speed and trans-border reach of cyber space poses challenge, both legally and technologically, to counter same.

B. Existing Cyber Security Framework in India

1.6 The proposal of National Security Council Secretariat (NSCS) on Framework for Enhancing Cyber Security of Indian Cyberspace was approved by the Cabinet Committee on Security on 08.05.2013 by assigning various responsibilities among following Ministries and Departments/Agencies, securing cyberspace, some of which are reproduced, as under:

(i) The National Security Council Secretariat would co-ordinate, oversee and ensure compliance of cyber security policies.

(ii) National Technical Research Organization (NTRO) would be responsible for the protection of identified Critical Information Infrastructure (CII), initially within the Government.

(iii) Ministry of Defense Service/DRDO would be responsible for defense related cyber threats, vulnerability, detection and mitigation; and

(iv) Ministry of Electronics and Information Technology (MeitY)/CERT-In would be responsible for non-critical Government sectors and CII in the private sector not included in (ii) and (iii) above.

(v) The Ministry of Home Affairs would be responsible for framing policies related to classification, handling and security of information relating to Government in consultation with other stakeholders and monitoring its implementation.

As per the Cyber Security Framework, 2013, MHA was given the responsibility for framing policies related to classification, handling and security of information relating to Government. Accordingly, in the year 2014, "National Information Security Policy and Guidelines (NISPG)" were issued by the MHA to all Ministries and Departments for its implementation. Further, a version of NISPG on 'information security' was also issued by MHA in 2019.

1.7 Further, in order to cater to specialized, specific challenges and issues in securing cyber space, various Ministries and Departments/Agencies have been assigned roles/responsibilities over a period of time as under:

(i) In 2017, National Critical Information and Infrastructure Protection Centre (NCIIPC), an agency under NTRO was set up under Section 70A of Information Technology (IT) Act, 2000, as the national nodal agency for cyber security of Critical Information Infrastructure (CII).

(ii) Ministry of Electronics and Information Technology (MeitY) is the National Nodal Ministry for framing policies relating to cyber space including cyber laws, policies for public procurement with, standardization testing, capacity building and program management through National E-Governance Division, etc. The following agencies function under MeitY:

   (a) Computer Emergency Response Team —India (CERT-In) came into operation in January 2004 as the national nodal agency under section 70B of IT Act, 2000 for responding to computer security incidents, as and when they occur. It performs related functions in the area of cyber security, coordinates cyber incident response activities and issues guidelines.

   (b) National Cyber Coordination Centre (NCCC) is a project under CERT-In which draws its authority from Section 69B of Information Technology (IT) Act, 2000. It became operational in 2017 for monitoring internet traffic data or information through any computer resource for cyber security and analysis of cyberspace from national security perspective.

   (c) National Informatics Centre (NIC) provides network backbone and e-Governance support to Central and State Governments and other Government bodies.

1.8 Coordination mechanism on Cyber Security

Regular coordination meetings on cyber security are held in MHA under the chairmanship of Union Home Secretary, Special Secretary (Internal Security) and Joint

Secretary (CIS) with concerned Ministry/ Department e.g., Ministry of Electronics and Information Technology, Department of Telecommunications and Department of Financial Services etc. and government cyber agencies. Five Coordination meetings have been held so far.

Monitoring Committee under the chairmanship of Special Secretary (Internal Security), MHA was constituted on 26th July 2022 to discuss the compliance regarding the implementation of shared Advisories, Indicator of Compromises (IoCs), TTPs (Tactics, Techniques, and Procedures), Alerts, etc., related to cyber and information security. The committee inter-alia consists of representatives from MeitY, IB, CERT-In, NIC and DoT. Till date, six meetings of the Monitoring Committee have been convened.

1.9 National Cybercrime Reporting Portal

National Cybercrime Reporting Portal (www.cybercrime.gov.in) was launched on 20.09.2018. This portal was a centralized online platform which allowed citizens to report online content pertaining to Child Pornography (CP)/Child Sexual Abuse Material (CSAM) or sexually explicit content such as Rape/Gang Rape (RGR) content. A revamped National Cyber Crime Reporting Portal was launched on 30.08.2019 to enable citizens to report all types of cyber-crimes with special focus of cybercrime against women & children. Since its operationalization, more than 23 lakh cyber crime incidents have been reported through the portal and more than 45700 FIRs and 30550 NCRs have been registered.

(i) toll-free number 1930 was operationalized for citizens to get assistance in lodging online cyber complaints.

(ii) AI based Chat Bots have also been made available to help and assist citizens in filing cybercrime complaints on the National Cybercrime Reporting Portal.

(iii) Since majority of the cyber incidents reported on National Cyber Crime reporting Portal related to financial frauds, a Citizen Financial Cyber Fraud Reporting and Management System has been launched in year 2021 by on-boarding all States/UTs for quick reporting of financial cyber frauds and to prevent flow of funds, siphoned off by fraudsters in the least possible time. Sofar, financial fraud transactions amounting to more than Rs.486 crore have been saved, belonging to over 2.19 lakh persons.

(iv) Ministry of Home Affairs has provided financial assistance to the tune of Rs. 12.127 Cr. to all States/UTs for strengthening of 1930 toll free helpline number.

1.10 Cyber Forensics & Investigation

National Cyber Forensic Laboratory (NCFL), a state-of-the- art facility has been set up at Dwarka, New Delhi under I4C on 18.02.2019 with the objective of providing forensic assistance during investigation to LEAs and other central agencies. The NCFL is uniquely placed as a cyber-forensicfacility that works closely with investigators, especially during the early stage of investigation and gives significant insight into the current and the latest trends of cybercrimes.

As on date, National Cyber Forensics Laboratory (NCFL) have provided its services to State LEAs in around 7,800 cyber forensics like mobile forensics, memory forensics, CDR Analysis, etc. to help them in investigation of cases pertaining to cyber crimes.

NCFL has been made functional and its services or facilities are being utilized by States/UTs across the country. Around 608 personnel of State/UT LEA have been trained by NCFL in various specialised advance cyber forensic fields. Intensive practical training program in “Digital Investigation and Cyber Forensics” commenced from 20.09.2021 for Police officials of States/UTs in batches of 20 participants for 10 days hands-on-training on latest forensic tools. Training in 16 batches has been conducted so far.

C. Cyber Security Framework in Financial Services Sector

Cyber space is a complex and dynamic environment which has made geographical boundaries irrelevant for the purpose of exchange of information and interactions across the world. However, the exponential increase in the number of internet users in India, clubbed with rapidly evolving technologies has brought in its own unique challenges in the form of illegal/ unwarranted use of cyber space by criminals.

1.11 The regulation and supervision of the financial system in India is carried out by different regulatory authorities. The supervisory role of the Reserve Bank of India (RBI) covers Scheduled commercial banks, urban cooperative banks (UCBs), financial institutions and non-banking finance companies (NBFCs). Regional Rural Banks and the rural co-operative banks are supervised by National Bank for Agriculture and Rural Development (NABARD) whereas insurance sector and pension funds are regulated by Insurance Regulatory and Development Authority of India (IRDAI) and the Pension Funds Regulatory and Development Authority (PFRDA) respectively.

1.12 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. Similarly, IRDAI and PFRDA also play important roles in ensuring the cyber security preparedness of the insurance & pension sector in India.

1.13 The financial services sector regulators have been taking various initiatives to address cyber security in their respective domain, in consultation with Indian Computer Emergency Response Team (CERT-In). CERT-In acts as the National agency for cyber security incident response and creates awareness on security issues through dissemination of information. Similarly, National Critical Information Infrastructure Protection Centre (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 ("CIP").

1.14Hon'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 at strategic level with representation from Department of Economic Affairs (DEA), Ministry of Electronics and Information Technology (MeitY), Department of Financial Services, National Security Council Secretariat, CERT-In, NCIIPC and financial sector Regulators etc. The Co-chairs of the strategic advisory Committee are Secretary, DEA and Secretary, MeitY.

> "The Central Payments Fraud Information Registry (CPFIR), a web-based payment-related fraud reporting solution has been implemented by RBI from March 23, 2020. All payment-related frauds, undertaken using various payment instruments (bank account, credit card, debit card, paper-based instruments and PPIs), and processed through authorised payment systems, either reported by the customer to the Supervised Entity (bank or non-banks) or detected by the Supervised Entity themselves, are required to be reported to the CPFIR. The reporting to CPFIR is undertaken by Scheduled Commercial Banks, Non-bank Prepaid Payment Instrument Issuers and non-bank Credit Card Issuers. The reporting is being expanded to other banks including urban cooperative banks."

1.15 The domestic payment fraud data as reported by Supervised Entities, during the past three financial years is as under:

Domestic Actual Frauds		
	Volume (lakh)	**Value (INR Crore)**
FY2021	7.05	542.7
FY2022	12.27	1357.06
FY2023	19.94	2537.35

** Due to CoVID pandemic, the Supervised Entities commenced reporting in a gradual manner. Some major SEs commenced reporting at a later date in 2021 and 2022.*

1.16 Majority of the payment frauds are understood to be in the nature of phishing attacks in various forms (such as vishing, phishing, Smishing, etc.), while the payment systems are ensured that they are safe, secure, sound, resilient and efficient.

On the issue of increasing incidents of cyber crime, representative of Razorpay stated as under:

> "Sometimes when the investigation starts, it starts too late and it happens by multiple or different law enforcement agencies, some of which do not understand what the modus-operandi is, how the digital payment system operates and so on. Having some sort of a centralized agency which is responsible for investigating these frauds, which is trained in these matters, especially the widespread frauds, who are deeply trained in these matters, who can pick up the report that come from various different law enforcement agency and do a single investigation will be helpful."

1.17 Regarding the volume of Financial Crime being reported in the Country, the ministry of Home Affairs stated as under:

> "The volume of financial crimes which were reported in financial year 2020-21 was 2.62 lakhs. It has gone up to 6.94 lakhs in 2022".

1.18 Highlighting the role of Financial Intelligence Unit (FIU-IND), Department of Revenue submitted as under:

> "As part of such operational analysis, FIU-IND has flagged several key suspected money laundering and terrorist financing trends, typologies and developments including those relating to cyber-crimes. The resulting Operational Analysis (OA) reports have also been shared with relevant law enforcement agencies (LEAs) /

intelligence agencies (IAs). Some of the key suspect trends and typologies which have been thus identified and shared are the following:

(i) A large number of money mule accounts were opened via the Video Customer Identification Process (V-CIP) based KYC procedure. Majority of these accounts were opened with common email addresses and postal addresses. It was observed that these accounts had been used to receive proceeds of cyber frauds, which were withdrawn as cash through ATMs. Subsequent to the discovery of frauds, enhanced due diligence exercises carried out by banks have revealed that most of the accountholders are not reachable on their registered mobile numbers or they are not aware of the transactions being carried out via their accounts.

(ii) A number of illegal applications available for download from Google Play Store are created to lure gullible investors to invest money in the application promising huge returns to investors by investing their money into crypto currency mining and trading, forex trading, etc. In some cases, the entities fled with investors' money and deleted the application, as per complaints received by various Indian law enforcement agencies.

(iii) Reporting Entities have filed suspicious transaction reports linked to suspicious transactions of multiple UPI ids linked to certain gaming websites. Prima facie, it appeared that these websites are registered overseas in Curacao, Malta, Cyprus etc. Though the websites itself were registered in foreign countries, but all of them were linked to Indian Bank Accounts. During analysis of the financial transactions linked to the UPI ids, it was found that the network of foreign registered websites linked to Indian bank accounts appear to be engaged in fraudulent means of collecting money from individuals through false inducements. The collected funds were not distributed back to those who invested or played and were instead diverted to bank accounts of a few individuals and entities including those based abroad, and by investing the said funds for purchase of crypto currency. KYC documents of bank accounts linked to the gaming websites did not mention linkages with any gaming activities, most of them are linked to trading of grocery items etc.

(iv) In a recent act of terrorism, the main accused was found to have been funded through crypto currency. He received crypto currency in his wallet account with Indian crypto currency exchange from multiple wallets held with foreign

crypto currency exchange. This implied that he did not buy any crypto currency. Crypto currency was transferred to his account from other accounts, and he merely sold it in the exchange and redeemed the money in his bank account and another mule account controlled by him.

1.19 On asking about trends in cybercrime, Department of Revenue, Ministry of Finance stated as under:

"There are four major trends that we have seen. The first one is the use of crypto for money laundering and terror financing. The second is the use of mule accounts with false addresses. That is the second typology. The third typology is the use of international online betting sites both for purpose of money laundering and terror financing. The fourth trend we have seen is the lending apps and apps for investments which have been used and which have been caught in the system. So, these four typologies have been primarily reported. as regards the mule account, it is mostly in India. But in the three other instances, the offshore entities are involved. It may be crypto. It may be the online betting sites. There is a clear set of online betting sites which are based out of tax havens.

In the year 2021, we saw the total frauds reported for ATMs and other frauds were about 10.80 lakhs and the value was Rs. 1,119 crore. That means, for every 67,000 transaction, one fraud was being committed. For 2022, 17.60 lakh is the number we have. The amount is Rs. 2,113 crore. For every 64,000 transaction, one fraud was being committed."

1.20 On the question of number of impacted customers due to cyber fraud, representative from NPCI stated as under

"The number of impacted customers is 2,000 per month. I am quoting average numbers. In this, social engineering coupled with BCs involvement is the major reason for the fraud where the poor customers in the rural areas are sweet talked and made to participate in doing a transaction and obviously the business correspondent who is interacting with the person on the field is the main source of fraud.

As far as cyber security aspect is concerned, I do not have the exact figures, but I can give you one proxy figure which is called BitSight rating which is universally accepted as a standard. Even the insurance providers take the BitSight rating as a standard before quoting the premium. SBI BitSight rating is the highest in the

economy in India and much better than many of the global banks operating outside India.”

Chapter - II

Social Engineering Frauds and Consumer Awareness Campaigns

2.1 Regarding social engineering frauds, the representatives from Razorpay during the sitting held on 01.06,2023 deposed as under:

> "Statistics show that fraud rates in India are considerably low. The average fraud rate in India is about 0.1 to 0.2 per cent compared to western markets which are at about one to two per cent. The difference here is that in most of the western markets, the most significant kind of a fraud is 'stolen credential fraud' because they do not have a two-factor authentication and other things. In India, that fraud is fairly limited, but the kind of fraud that happens in India is more of a social engineering, phishing, identity theft, and white-collar frauds like Ponzi schemes and fraudulent apps. The challenge with these kinds of frauds is that even while the percentage might be low, but I would just like to give an example. Today, as Razorpay, we notice almost 400 to 500 fraudulent apps that try to onboard themselves on our platform every month. We block them but that does not stop these apps. They go to any other payment provider and banking system and get themselves onboarded and start conducting their fraud. Today, there is no way for us to notify any Department or any Body regarding the fraudulent app. It becomes an easy option for the fraudster to start with one payment platform, and if they get noticed and blocked, they move to another payment platform."

2.2 On the question of pattern of cyber frauds committed in India, the representative of PhonePe stated as under:

> "It is largely under the purview of what we call as social engineering frauds, broadly three buckets, one of them is basically this. You may call it sophisticated to the point of trying to take over a device through SIM cloning or trying to actually get malicious apps installed on victims' phone and then be able to take over their account.
>
> The second one is largely under the phishing bucket, which is false websites, fake merchant sites, etc. that consumers are encouraged to shop on and then, no goods are delivered, etc. and the money is just siphoned off.
>
> The third one which is very large is basically push payments wherein the consumers are actually led to send payments to the fraudsters by actually

entering their own credentials as they would do for normal transactions. These could be like the Ponzi schemes where they are promised some sort of job and they have to pay some sort of registration fee to a particular phone number or UPI VPA or even a bank account and that gets transferred through different bank accounts and finally, it gets removed or it could be about saying that I am representing somebody else. We have seen people talk about fake donations, saying that this is for a great cause and there is even greed that is played on the consumers mind where they say that if you send this money, you are going to get this much of cash back, recharge etc. So, these are the various modus-operandi under social engineering that we and all other platforms try to actually detect proactively but it is always evolving and they have to be on their toes there."

2.3 Phishing sites and malicious Apps

A total number of 1714 and 135 phishing incidents were reported during the year 2022 and 2023 (till April) respectively. All of the phishing websites were taken down in coordination with concerned service providers, within 24 to 48 hours. However, some of the phishing websites might not be reported to CERT-In. CERT-In is coordinating with banks and service providers to mitigate phishing sites.

A total number of 141 and 21malicious app incidents were observed during the year 2022 and 2023 (till April) respectively. All of the malicious apps were taken down within 24 to 48 hours.

2.4 Various customer awareness initiatives as undertaken by RBI are listed below:

(i) A detailed framework has been formulated for financial education with a focus on customer protection. The implementation of the framework is underway, including the intensified/ focused awareness campaign set for 2022-23 regarding safe banking practices/ grievance redress avenues of RBI, etc. Further, the content for enhancing financial awareness and safe banking practices have been taken up for inclusion in the education curriculum of school students in coordination with the National Centre for Financial Education (NCFE) through the Financial Inclusion and Development Department (FIDD) of the Reserve Bank.

(ii) To enhance the level of financial education and awareness amongst the customers, a pan India Intensive Awareness Campaign was launched starting March 2022. On the event of "World Consumer Rights Day" on March 15, 2022, all 22 RBI Ombudsmen interacted with the local/ regional multimedia channels

(including regional channels of Doordarshan) in their respective regions, covering a wide range of areas such as 'Frequently Asked Questions on Reserve Bank-Integrated Ombudsman Scheme, 2021 (RB-IOS)', Charter of Customer Rights, safe digital banking practices, etc., in order to ensure deeper and focused percolation of the financial consumer awareness on safe banking, RBI's alternate grievance redress avenues and extant regulations for protection of consumer interests. The event was undertaken in English, Hindi and vernacular languages and was aired on Doordarshan, All India Radio, RED FM, and Private local TV channels such as TV9, Gulistan, Sahyadri, Asmita, etc. across all regions/states of India.

(iii) A media interaction was addressed by RBI at New Delhi Regional Office on August 29, 2022, covering various facilities of RBI under its Alternate Grievance Redressal mechanism viz., RB-IOS, 2021, Centralized Receipt and Processing Center (CRPC), Contact Center (CC), the roles and responsibilities of the customers as well as measures (Do's and Don'ts) for safeguarding them against digital/electronic frauds.

(iv) A "Nation-wide Intensive Awareness Programme" (NIAP) was carried out during November 1-302022, by RBI in collaboration with the REs. Considering that REs act as the first touch point for their customers, their support, reach, and infrastructure was leveraged for ensuring percolation of the awareness initiative to the very last mile, especially the Tier-III to VI cities, rural areas, and the remotest locations. During the campaign around 1.63 lakh programmes were carried out through multiple channels, of which around 1.28 lakh programmes were carried out in physical mode. As reported by the REs, approximately three crore persons participated physically in these programmes and the online channel reached out to around 25 crore people. Special drives were conducted for vulnerable sections of the population and around 16,361 differently abled and 82,436 senior citizens participated in these activities.

(v) A booklet on BE(A)WARE (English and Hindi) and Raju and the Forty Thieves covering the modus operandi of frauds and the way to escape/ avoid getting trapped by fraudsters has been issued by RBI and placed on its website for use by members of public and the REs. These are also distributed in physical programmes conducted by Regional Offices of RBI Ombudsmen.

2.5 On a macro level (in coordination with RBI's Department of Communication), various initiatives were taken for creating customer awareness with respect to digital transactions such as:

(i) Making customer aware of RBI instructions on frauds in electronic banking transactions by having a re-run of the campaigns on its regulations limiting the liability of customers in fraudulent electronic banking transactions.
(ii) Making customer aware of the RB-IOS as an integrated ombudsman scheme for all the customers of digital financial services offered by entities regulated by RBI (bank as well as non-bank payment system participants).
(iii) A multi-media campaign on RB-IOS, 2021 is being carried out at Pan-India level.
(iv) Campaigns on Safe Digital Banking focusing on UPI frauds and AEPS are also being carried out.

All these campaigns are aired on Doordarshan and All India Radio, and in other national/local dailies to help in reaching the rural areas. These campaigns also form a part of the popular TV series "Kaun Banega Crorepati", which is widely watched by public in rural areas. Ombudsman offices carry out Town-hall meetings and Awareness programmes on various issues including digital and online frauds related aspects in the areas under their jurisdiction, including the rural areas. Further, a large number of awareness programmes (204 in the year 2021-22) are conducted by RBIOs where cyber care is emphasised as an important element for all public members. To strengthen the systems at RE levels, meetings are conducted with banks wherein the REs have been advised to onboard psychologists, ethical hackers and innovators on their risk management teams to reduce and mitigate the incidences of cyber-crimes. To provide efficient and effective redress to victims of cyber frauds, common public are made aware of aspects such as RB-IOS 2021, RBI's circular on Limiting Liability of Customers in Unauthorised Electronic Banking Transactions through advertisements and campaigns. In line with the G20 finance track, of which financial literacy and consumer protection is an important part, G20 logo is included in the banners on grievance redress mechanism of RBI, and the banks are being advised to host the same in all their branches. Meetings are held with TRAI and Ministry of Home Affairs, Government of India on mitigating cyber frauds. Options are being explored to have a dedicated system/ number for financial institutions. Various awareness messages related to safe digital banking in the form of tickers/scrolls are being hosted on the RBI website and RBI's Complaint

Management System (CMS) webpage, which is the online portal for filing of complaints lodged under the Reserve Bank –Integrated Ombudsman Scheme (RB-IOS), 2021. The RB-IOS, 2021 was launched by the Honourable Prime Minister on November 12, 2021.The Centralised Receipt and Processing Centre (CRPC) has a Contact Centre with 24x7x365 IVRS (#14448) as an "on-tap resource" on RBI's Alternate Grievance Redress and facility for human interface is available from 8.00 am to 10.00 pm in Hindi and English on all weekdays except national holidays and for 10 other regional languages i.e., Assamese, Bengali, Gujarati, Kannada, Malayalam, Marathi, Odia, Punjabi Tamil and Telugu from 9:30 am to 5:15 pm on all weekdays except national holidays. A Press Release on Consumer Awareness - Cyber Threats and Frauds was issued on January 282022, urging the members of public to practice safe digital banking by taking all due precautions, while carrying out any digital (online / mobile) banking / payment transactions. Regional Offices of RBI organise regular e-BAAT (electronic Banking Awareness and Training) programmes to improve customer awareness. Since 2020, nearly 1000 eBAAT programs have been conducted by various offices of RBI. RBI encourages customers to report phishing mails/ phishing sites and on such reporting take effective remedial action and educate them on the downside risk of sharing their login credentials /passwords etc. to any third-party and the consequences thereof.

2.6 On the question of online payment and consumer awareness, the RBI stated as under:

> “Over the last five years we have seen a CAGR of 51 per cent in terms of volume of payments, and we expect the growth rate to continue in the same fashion.
>
> We have around 38 crore transactions that happen every day in our payment system and UPI is the main system that accounts for almost 76 per cent of the transactions. The average system sees around one fraud on 60,000 transactions, but in the case of UPI, it is one fraud for 1.15 lakh transactions.
>
> Recently, we have started a mega campaign called 'Har Payment Digital'. We have also been telling that each one should adopt digital payments and also teach somebody else who needs to make digital payments. 'डिजिटल पेमेंट अपनाओ औरों को भी सिखाओ' is one campaign that we have started. We are very much focused on seeing that these campaigns reach the length and breadth of the country including having those material in 13 languages. We are also partnering with the banks and non-banks to see that they also take these campaigns

forward. we have a zero-liability concept as well and if the customer can complain within three days, the liability also ends there. So, we have taken all these measures and every effort is to see that the customer becomes comfortable."

2.7 To the query whether the Government has specific figures/data for cyber crime and comparison with other countries, the Ministry of Electronics and Information Technology stated that they don't have this data as it is topic covered by Ministry of Home Affairs.

Highlighting the measures taken to enhance the cyber security for citizens Ministry of Electronics and Information Technology stated as under:

(i) "Cyber Security Awareness for Citizens and Technical Cyber Community

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, Swachhta Pakhwada 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.

In 2021, CERT-In observed the Cyber Security Awareness Month during October 2021 by organising various events and activities for citizens as well as the technical cyber community in India with a theme of "Do Your Part, #BeCyberSmart". The total outreach of National Cyber Security Awareness Month October 2021 was 2,15,00,000+.

CERT-In in association with C-DAC, Noida hosted online short sessions for citizens on "Securing Digital Space" during the Cyber Security Awareness through MyGov platform during the National Cyber security awareness month in October 2021.

In 2022, CERT-In conducted various cyber security awareness activities during National Cyber Security Awareness Month (NCSAM), October 2022 with a theme "See yourself in cyber". Total outreach during the NCSAM 2022 was 72,03,34,700.

CERT-In organized 32 different awareness programs for different sectors including Ministries, Government Organizations, Industry and Academia in 2022 covering approximately 17,165 participants.

CERT-In regularly shares its important activities, alerts issued, safety and security tips and awareness posters, infographics and videos through its official websites and social media handles such as Facebook, Twitter, Koo, and Pixstory for sensitizing internet users on cyber frauds and cybercrime and prevention measures. As of now, CERT-In has 85K followers across its social media handles.

(ii) Cyber Security Tools for Citizens for safeguarding their digital devices

Cyber Swachhta Kendra (CSK) - The Botnet Cleaning and Malware Analysis Centre has been setup with an eye to create a secure cyber space by detecting botnet infections in India and to notify, enable cleaning and securing systems of end users so as to prevent further infections. CSK is covering about 94% of Indian internet users as well as 755 organizations across sectors.

Cyber Swachhta Kendra is a citizen centric service operated in PPP model which extends the vision of Swachh Bharat to the Cyber Space. Cyber Swachhta Kendra aims to secure India's digital IT Infrastructure by creating a dedicated mechanism for providing timely information about Botnet/Malware threats to the victim organization/user and suggesting remedial actions to be taken by the concerned entity. The centre aims to maintain cyber hygiene in ICT infrastructure of the country.

CSK enables users to secure their digital devices against any malware infection. CSK is providing Free Botnet Removal Tool (FBRT) to citizens through its portal/website for disinfecting Microsoft Windows based systems/devices and mobile devices through collaboration with cyber security companies.

CSK is also providing various other security tools to the users for securing their mobile devices. The tools include M-Kavach for securing Android Mobile devices, USB Pratirodh - a desktop solution for controlling the usage of removable storage media like pen drives and external hard drives, AppSamvid - desktop based Application Whitelisting solution for Windows operating system and Browser JSGuard - a browser extension which detects and defends malicious HTML &JavaScript attacks made through the web browser based on Heuristics. It

alerts the user on visiting any malicious web pages and provides the detailed analysis threat report of the web page.

(iii) Security tips for users on CERT-In website

CERT-In has published various safety and security for end users related to securing desktops/laptops, security mobile phone, securing broadband Internet, securing USB Devices, secure uses of Credit/Debit Card and preventing phishing attacks."

Chapter - III

Mitigation measures taken by Regulatory Agencies

With regard to mitigation measures taken by the Government, Ministry of Electronics and Information Technology (MeitY) in its written reply submitted as under:

3.1 The Indian Computer Emergency Response Team (CERT-In) has been designated under Section 70B of the Information Technology Act, 2000 to serve as the national agency for cyber security incident response.

CERT-In, through RBI, has advised all authorised entities and banks issuing pre-paid payment instruments (wallets) in the country to carryout special audit by CERT-In-empanelled auditors, close the non-compliances identified in the audit report and ensure implementation of security best practices.

To facilitate effective incident response measures as well as to addresscertaingapscausinghindranceinincidentanalysis,CERT-Inhasissued directions relating to information security practices, procedure, prevention, response and reporting of cyber incidents on 28.04.2022 in exercise of powers under section 70B(6) of the Information Technology Act, 2000. Subsequently, a set of Frequently Asked Questions (FAQs) document was also issued on 18.05.2022, to enable better understanding of the various stakeholders and to facilitate compliance. The directions cover aspects relating to mandatory reporting of cyber incidents to CERT-In; maintenance of logs of ICT systems; KYC norms and practices by virtual asset service providers, virtual asset exchange providers and custodian wallet providers. These directions aim to enhance overall cyber security posture and ensure Safe & Trusted Internet in the country.

The role of DFS is limited in identification of Critical Information Infrastructure (CII) in the financial sector in consultation with MeitY, NCIIPC, sectoral regulators and the concerned regulated entities. In the recent past, DFS proactively engaged with all the concerned stakeholders and identified & notified the core systems of RBI (NEFT, RTGS, e-KUBER), core systems of NPCI (UPI, NFS, IMPS) and the core systems of LIC, SBI and various other banks such as HDFC Bank, ICICI Bank, PNB, Bank of Baroda, Union Bank of India, Kotak Mahindra Bank, Canara Bank and Axis Bank as Critical Information Infrastructure (CII), to reduce the vulnerabilities to various cyber threats and attacks.

In addition to this, DFS holds regular meetings with the senior functionaries/ security officers of the financial sectoral regulators to review the cyber security threats across the financial sector and emerging technologies to counter such threats.

DFS also proactively follows up any cyber security threats and vulnerabilities pointed out by NTRO/ NCIIPC/ IB/ MHA etc. with the financial regulators/ regulated entities on immediate and action-oriented basis.

Further, DFS organized a half-day conference on "FINSCY" (Financial Services Cyber Security) in February 2023 to assess the cyber security measures currently in place and readiness of the sector to any future cyber threats. From the response and outcome of the said conference, DFS has now proposed to organize this event on a half-yearly basis.

The specific mitigation measures implemented by RBI to enhance cyber security in the critical digital sector and prevent cybercrimes:

3.2 Cyber security measures put in place by RBI

(i) The changing business model of banks from branch based to electronic, anytime banking and its concomitant technology risks was recognized by RBI as early as 2011 when regulatory expectations were issued by RBI to all banks as a report by the Working Group on “Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds” under Shri G. Gopalakrishnan, the then Executive Director of RBI. The banks were advised to implement the recommendations based on risks commensurate with the nature and scope of activities engaged by them, the technology environment prevalent and the support rendered by technology to the business processes.

(ii) In order to provide focused attention on IT related matters, RBI set up a Cyber Security and IT Risk (CSITE) Group within its Department of Supervision in 2015. Under CSITE Group, appropriate regulatory and supervisory mechanism has been put in place to take care of regulation and supervision of the Regulated Entities (REs) from cyber security perspective. A detailed cyber security framework was prescribed for all Commercial Banks in 2016. The framework was derived from international frameworks (such as NIST) and tuned to the requirements of the Indian banking sector. The requirements have been articulated in the form of baseline expectations on various aspects of cyber security. Care is taken to adopt a principle-based and risk-based approach to

mitigate cyber risks. Appropriate regulatory frameworks have been put in place for Non-Banking Financial Companies (NBFCs) and Urban Cooperative Banks (UCBs) as well in 2017 and 2019 respectively. For Rural Cooperative Banks, State Cooperative Banks and District Central Cooperative Banks NABARD have extended these guidelines in 2020.

(iii) Based on the evolving threat landscape in certain systems of the banks, specific controls measures have also been prescribed in addition to existing guidelines. Thus, while there are principle-based baseline expectations for achieving cyber resilience, it is necessary to identify idiosyncratic risks associated with the type of products / services offered and, accordingly, tailor the regulatory expectations to mitigate risks associated with them as well. Since June 2016, several circulars and advisories (mostly confidential in nature) have been issued to banks. Some of them are in the areas such as ATM control measures to protect from skimming/malware attacks; securing SWIFT and ATM Switch ecosystem; Effectiveness of VA/PT (Vulnerability Assessment/Penetration Testing) exercise; Sustained Assurance of Cyber Resilience Framework by identifying the deficiencies/shortcomings and initiating timely action to address them promptly; Securing payment ecosystem-Rupay, UPI, e-commerce transactions, safeguarding against email spoofing attacks, etc.

(iv) An expert panel / inter-disciplinary Standing Committee on Cyber Security has been constituted by RBI in February 2017 with external members from the CERT-IN, Academia, Professionals in the field and a forensic auditor which inter alia, reviews the threats inherent in the existing/ emerging technology areas and suggests appropriate policy interventions to strengthen cyber security and resilience. The Committee meets on a quarterly basis.

(a) The banks vide the circular on “Control measures for ATMs – Timeline for compliance” dated June 21 2018 have been advised to take various measures to strengthen security of ATMs. These measures, inter alia include - enabling BIOS passwords, disabling USB ports, applying the latest patches of operating system and other software, terminal security solution, time-based admin access, implementing anti-skimming and whitelisting, etc.

(b) To further strengthen the cyber security resilience of the UCBs, a comprehensive cyber security framework was issued on December 31,

2019. The framework, inter alia, mandates the implementation of progressively stronger security measures based on the nature, variety, and scale of digital product offerings of such banks.

(c) When it was observed that CISO function was not adequately skilled or duly empowered in many entities to ensure effective implementation of cyber security measures, a circular was issued to banks, clarifying the role and functions of CISO including details of reporting structure, having requisite technical expertise, adequate staffing in CISO's office, etc.

(d) With an aim to strengthen the cyber resilience of the UCBs against the evolving IT and cyber threat environment, in September 2020, the Reserve Bank released the 'Technology Vision for Cyber Security: 2020-2023' for UCBs, based on inputs from various stakeholders. It envisages a five-pillared strategic approach covering (i) Governance oversight; (ii) Utile technology investment; (iii) Appropriate regulation and supervision; (iv) Robust collaboration; and (v) Developing necessary IT and cyber security skills sets.

(e) The emerging risks from recent trends of banking such as proliferation of digital banking services have been addressed through issue of Master Direction (Digital Payment Security Controls). The Master Direction (MD) envisages RBI Regulated Entities (REs) to set up robust governance structure and implement common minimum standards of security controls for digital payment products and services.

(f) REs are extensively leveraging Information Technology (IT) and IT-enabled services (ITeS) in their businesses, products and services with increasing dependence on third parties. Such reliance on IT/ITeS provided by third parties exposes the REs to various risks. In view of the same, guidelines were published recently on April 10 2023 viz., Master Direction on Outsourcing of IT Services covering instructions relating to establishing a risk management framework for Outsourcing of IT Services, managing related concentration risk, Outsourcing within a Group/ Conglomerate, specific requirements on Usage of Cloud Computing Services, etc.

(g) The instructions on IT Governance and Controls, Business Continuity Management and Information Systems Audit have been updated and consolidated in the form of another draft Master Direction. This Master

Direction is expected to be issued shortly, after considering the comments received.

3.3 Security Measures for Payment Transactions

Various steps taken by Reserve Bank of India (RBI) to enhance safety and security of digital payment transactions (including card transactions, online transactions, etc.) and check and reduce frauds are given below:

(i) Additional Factor of Authentication (AFA) for digital payment transactions (Card Present, CNP, mobile banking and internet banking)

(a) AFA mandatory for all on-line CNP transactions so as to provide additional authentication / validation based on information not visible on the cards.

(b) Mandatory PIN authentication for all face-to-face / CP transactions performed using cards (credit, debit, and prepaid cards) issued and acquired by banks in India.

(c) While processing an EMV Chip and PIN card, fall back to magnetic stripe option shall be enabled only if the transaction cannot be completed as a Chip-based transaction, i.e., ab initio processing of EMV Chip and PIN-based cards on the basis of magnetic stripe data shall not be done.

(d) 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.

(e) For carrying out transactions like fund transfers through internet banking, the banks, at the least, need to implement robust and dynamic two-factor authentication through user id/password combination and second factor like (a) a digital signature (through a token containing digital certificate and associated private key) (preferably for the corporate customers) or (b) OTP/dynamic access code through various modes (like SMS over mobile phones or hardware token).

(f) All wallet transactions involving debit to the wallet, including cash withdrawal transactions, shall be permitted only by validation through a Two Factor Authentication. AFA is not mandatory for PPIs issued under PPIs for Mass Transit Systems (PPI-MTS) and gift PPIs.

(ii) Online Alerts

(a) Banks to put in place a system of online alerts for all types of transactions irrespective of the amount, involving usage of any payment instrument at various channels.

(iii) Electronic transactions

(a) Banks are required to mandatorily register their customers for SMS alerts and wherever available, for e-mail alerts as well, for electronic banking transactions. The SMS alerts are mandatorily required to be sent to the customers.

(b) Banks are also required to provide customers with 24x7 access through multiple channels (at a minimum, via website, phone banking, SMS, e-mail, IVR, a dedicated toll-free helpline, reporting to home branch, etc.) for reporting unauthorized transactions that have taken place and/ or loss or theft of payment instrument such as card, etc.

(c) Safety measures are also prescribed for consideration by banks for electronic payment modes like RTGS, NEFT and IMPS, viz - system of alert when a beneficiary is added; limit on the number of beneficiaries added in a day per account; introduction of AFA (preferably dynamic in nature) for such payment transactions; etc.

(iv) Switch on / off facility for cards

(a) The issuers shall provide to all cardholders a facility on a 24X7 basis to switch on / off and set / modify transaction limits for all types of transactions – domestic and international, at PoS / ATM / online transactions / contactless transactions, etc. through one or more channels - mobile application / internet banking / ATMs / Interactive Voice Response (IVR) or at branches / offices.

(b) At the time of issue / re-issue, all cards shall be enabled for use only at contact-based points of usage [viz. ATMs and PoS devices] within India.

(c) All new cards issued – debit / credit / PPI, domestic and international – by banks as well as non-bank PPI Issuers shall be EMV Chip and PIN based cards. Gift PPIs may continue to be issued with or without EMV Chip and PIN enablement.

(v) Card Tokenisation

(a) Tokenisation refers to the replacement of actual card details with a unique alternate code called the 'token', which shall be unique for a combination of card, token requester.

(b) In order to make card transactions more safe, secure, and convenient for the users, RBI has permitted authorised card networks and card issuers to offer card tokenisation services to any token requestor (third party App provider), subject to conditions.

(c) It has also been extended to Card-on-File Tokenisation (CoFT).

(vi) Storage of Card Data

(a) With effect from January 1, 2022, no entity in the card transaction / payment chain, other than the card issuers and / or card networks, shall store the actual card data. Any such data stored previously shall be purged.

(b) For transaction tracking and / or reconciliation purposes, entities in the card payment chain can store limited data – last four digits of actual card number and card issuer's name.

1. Banks are required to frame rules based on the transaction pattern of the usage of cards by the customers in coordination with the authorized card payment networks for arresting fraud. This would act as a fraud prevention measure. Also, banks are required to move towards real time fraud monitoring system. Further, banks are required to provide easier methods (like SMS) for the customer to block his / her card and get a confirmation to that effect after blocking the card
2. With effect from July 1, 2022, no entity in the card transaction / payment chain, other than the card issuers and / or card networks, was permitted to store the actual card data. Further, any such data stored previously was required to be purged.

(vii) e-Mandates

(a) RBI has permitted processing of e-mandate for recurring transactions (merchant payments) with AFA during e-mandate registration, modification, and revocation, as also for the first transaction, and simple / automatic subsequent successive transactions, subject to conditions listed in the

circulars. This arrangement is applicable for transactions performed using all types of cards – debit, credit, and Prepaid Payment Instruments (PPIs), including wallets, and Unified Payments Interface (UPI).

(b) As a risk mitigant and customer facilitation measure, the issuer shall send a pre-transaction notification to the cardholder, at least 24 hours prior to the actual charge / debit to the card.

(c) The pre-transaction notification shall inform the cardholder about the name of merchant, transaction amount, date / time of debit, reference number of e-mandate, reason for debit, etc. On receipt of pre-transaction notification, the cardholder shall have the facility to opt out of that particular transaction or the e-mandate, with AFA validation.

(viii) Interoperable card less cash withdrawal (ICCW)

(a) The Reserve Bank permitted banks, ATM networks and White Label ATM Operators (WLAOs) to provide an option of ICCW at their ATMs. Under this facility, UPI is used for customer authentication in ATM transactions with the settlement facilitated through the National Financial Switch (NFS) / ATM networks. The absence of need for a card to initiate cash withdrawal transactions is expected to help contain frauds like skimming, card cloning and device tampering.

(ix) Payment Aggregators

(a) PAs are not permitted to give an option for ATM PIN as a factor of authentication for card-not-present transactions. PAs are not permitted to store the customer card credentials within their database or the server accessed by the merchant.

(b) PAs are required to put in place Board approved information security policy for the safety and security of the payment systems operated by them and implement security measures in accordance with this policy to mitigate identified risks.

(c) PAs are required to establish a mechanism for monitoring, handling and follow-up of cyber security incidents and breaches and report the same to RBI immediately. PAs are also required to report the same to CERT-In as per the details notified by CERT-In.

(x) PPIs

(a) Non-bank PPI issuers are required to maintain their outstanding balance in escrow account/s with any scheduled commercial bank. The balance in the escrow account/s shall not, at the end of the day, be lower than the value of outstanding PPIs and payments due to merchants.

(b) PPI Issuers are required to introduce a system where all wallet transactions involving debit to the wallet, including cash withdrawal transactions, are permitted only by validation through a Two Factor Authentication (2FA). The AFA requirements for PPI Cards (physical or virtual) is same as required for debit cards. 2FA / AFA is not mandatory for PPIs issued under PPIs for Mass Transit Systems (PPI-MTS) and gift PPIs.

(c) Issuer are required to put in place a mechanism to send alerts when transactions are done using the PPIs.

(d) Banks and non-banks are required to ensure that all new PPIs (including reissuance / renewal) issued in the form of cards are EMV Chip and PIN compliant. Gift PPIs may continue to be issued with or without EMV Chip and PIN enablement.

(e) PPI issuers are required to establish a mechanism for monitoring, handling and follow-up of cyber security incidents and cyber security breaches. The same shall be reported immediately to RBI. It shall also be reported to CERT-IN as per the details notified by CERT-IN.

(xi) UPI

(a) Financial transactions follow mandatory two factor authentication process. The first factor is validated by the Payment Service Provider (PSP) & the second factor is validated by the Issuer (Customer) Bank.

(b) In case of a UPI App, when the customer is trying to register for UPI for the first time, there is an SMS – based verification done to register the customer's device.

(c) Device binding is the process in which the customer will be sent an SMS by the Payment Service Provider while registering the customer to ascertain the veracity of the customer. The PSP also does the device fingerprinting through an automated outward encrypted SMS (Mobile number to PSP system) which hard binds the Mobile number with the device. This ensures that the transactions originating from the customer

are secured at the first step itself. This outward SMS being sent should be encrypted and should not have any customer intervention. Subsequently on transaction such details are verified and in case of any mismatch, then the transaction shall be declined.

(d) For customer to authenticate a transaction, he/she will have to enter the UPI PIN in NPCI Common Library in the Apps. (UPI PIN can be created by using Debit Card/ Credit Card / Aadhaar Credentials of the customer)

(e) Over and above the prescribed transaction limits, there are specific limits with respect to velocity and functionalities wise checks like collect, scan and pay, nature of merchants etc. which is communicated to the ecosystem. Such transaction limits ensure additional safety to the customers from fraud transactions.

(f) 'Collect' for P2P & non-verified merchants are limited to Rs 2000 per transaction. A single P2P beneficiary is allowed a maximum of 5 collect requests in a day.

(g) NPCI has completely disallowed P2P intent transactions

(h) Device binding controls have been deployed by Apps

i. SMS token expiry - 30 seconds
ii. SMS token length – 35 characters (Min)
iii. SIM should be active & available in SIM slot
iv. Registration fails on toggling of screens during registration
v. Allow device binding on latest App version
vi. Decline device binding if short code is received from more than 1 mobile number

(i) NPCI Fraud Monitoring (UPI) - NPCI has an additional mechanism to monitor transaction and in case of any transaction which is flagged as fraud, the system can decline such transactions. And in extension to this, there are certain limits set to protect the eco-system from potential frauds like:

i. There are per day transaction limit applicable in UPI which is Rs 1 lakh per transactions for regular UPI P2P/P2M transactions.
ii. There are also monthly transaction limits set for UPI, i.e., from the same account the customer shall not be allowed to initiate more than 100 transactions.

iii. Members can report the fraudsters account details / UPI ID which NPCI considers under the negative list and shall not permit the transaction to be processed. The same is also communicated to the eco-system as well for keeping relevant checks at their end.

(j) System Audit –

i. All authorised Payment System Operators (PSOs) were, vide circulars dated December 7, 2009, December 27, 2010 and April 15, 2011, directed to get a System Audit conducted by CERT-In empanelled auditors or Certified Information System Auditor (CISA) and registered with Information Systems Audit and Control Association (ISACA) or by a holder of a Diploma in Information System Audit (DISA) qualification of the Institute of Chartered Accountants of India (ICAI), on an annual basis.

ii. The scope of the System Audit was reviewed and enhanced in January 2020 in order to ensure standardisation along with the need to encompass all relevant areas of information system processes and applications to be covered as part of the audit. The scope includes, inter-alia, information security governance, access control, network and data security, physical and environmental security, human resource security, business continuity management, vendor management, incident management, change management, patch management, etc.

(k) Security Measures for PSOs

i. RBI issues advisories and alerts to authorised PSOs from time to time on information security threats including cyber-attacks, outlining best practices to combat such threats.

3.4 When asked about the level of collaboration and information sharing between the Government and Private Sector entities in combating cyber threats, the Ministry of Finance stated as under:

"An inter-disciplinary Standing Committee on Cyber Security was constituted by RBI. The Committee, *inter alia,* reviews the threats inherent in the existing/emerging technology and suggests appropriate policy interventions to strengthen cyber security and resilience. The Committee is chaired by the

Executive Director in charge of the supervisory vertical of RBI (specifically CSITE Group) and there are internal as well as external members having expertise in relevant areas. The Committee has been meeting on a regular basis to review the developments in the technology implementations and associated risks in the regulated entities of the Bank. So far, 18 meetings have been held.

(i) The major Terms of Reference of the Committee include, taking stock of the new developments in financial technology, reviewing the emerging threats inherent in the existing/emerging technology, studying various Security Standards and adoption of appropriate Security Protocols, examining the instances of cyber-attacks across the globe and the possible vulnerabilities that contributed to their occurrence, recommending pre-emptive step to ward off such risks to our banks, guiding in formulating recommended safeguards in specific operational areas such as, internet mobile banking, wallets payment systems, suggesting appropriate policy interventions, etc.

(ii) Major policy contributions of the Standing committee include Comprehensive Cyber Security framework for UCBs, Cyber Security Framework for Third party ATM switch application service providers, Master Directions on Digital Payment Security Controls, Master Directions on IT Outsourcing (Vendor Risk Management and Cloud Computing Services and Security).

(iii) Other contributions of the Standing Committee in providing guidance towards:

  (a) Circular on DMARC (Domain based Message Authentication Reporting and Conformance)
  (b) Impact assessment methodology of unusual cyber security assessment
  (c) ATM controls
  (d) Subjecting mobile banking applications to source code review
  (e) Reviewing Cyber Key Risk Indicators framework
  (f) Conduct of active cyber security drills rather than just table-top drills conducted at the moment (Phishing Exercise, Cyber Reconnaissance Exercise)

(g) Expectations from Vulnerability Assessment -Penetration Testing, Forensic Readiness, Data Governance aspects

(h) Specific inputs on conduct of IT Examination

(i) Conduct of Cyber Drill for UCBs in collaboration with CERT-In in Department of Supervision, RBI.

3.5 On the same issue, Ministry of Electronics and Information Technology stated as under:

(i) To deal with the complex, sophisticated cyber-attacks, sharing and exchange of threat intelligence and capacity building CERT-In partners with cyber security / product organizations from industry. CERT-In has signed Memorandum of Understandings (MoUs) for collaboration in the area of cyber security with CISCO India Pvt. Ltd, CloudSEK, Quick Heal, Information Sharing and Analysis Centre (ISAC), Microsoft, MicroWorld Technologies (Escan), K7 Computing, Kaspersky, Redinent Innovations Pvt. Ltd and SkillsDA.

(ii) CERT-In is organizing cyber security trainings and cyber security awareness programs in collaboration with its Industry partners who have signed MoUs. CERT-In has conducted 12 and 7 programs covering 5754 and 3215 participants from Government, Public sector Units, Private sector organizations and Citizens in 2022 and 2023 (up to June), respectively.

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

(iv) Cyber Swachhta Kendra is a citizen centric service operated in PPP model. This centre operates in close coordination and collaboration with Internet Service Providers and Product/Antivirus companies. Free bot removal tools were developed in collaboration with Antivirus companies Quickheal, K7 Computing and Escan which are disseminated through Cyber Swchhta Kendra website for citizens and organisations.

(v) Cyber Swachhta Kendra 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 182 financial sector organizations are receiving daily inputs related to malware and vulnerable services to combat cyber threats.

3.6 Upon enquiry regarding the issue of coordination with multi stakeholders, the representatives of Reserve Bank of India submitted as under:

"A coordinated approach is required with all stakeholders [including government departments (MoF, MHA, DoT, MeitY) and other regulators (SEBI, IRDA, TRAI, etc.)] to handle the menace of cyber frauds, ensure swift response and reduce the loss to the customers and increase the trust in digital payments/ banking ecosystem. In this regard, a Working Group has been set up under MHA with members from various ministries as well as regulatory bodies to examine the issue of online frauds and suggest and coordinate ways to prevent and mitigate impact of online frauds. RBI has been providing relevant inputs for deliberations of the Working Group. The Working Group also recommends cyber fraud mitigation measures which are then examined by RBI for implementation.

An inter-regulatory Working Group (WG) of RBI, SEBI, IRDA, PFRDA and NHB has been constituted under the Chairmanship of CGM (Cyber Security and IT Risk Group, DoS), RBI to explore the possibility of issuance of uniform baseline cyber security guidelines amongst the regulated entities. The WG is expected to submit its report by end of June 2023".

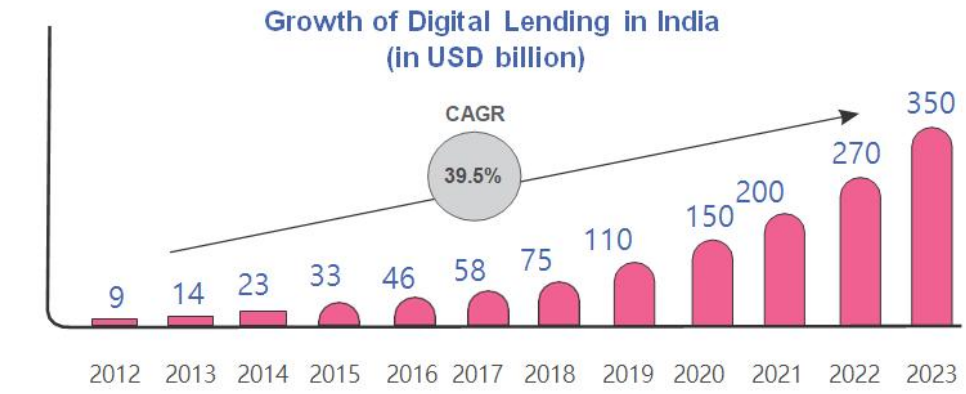
3.7 Regarding products and services specifically are not being appropriately regulated by the RBI and what are the gaps in the digital architecture, Indian Banks Association submitted as under:

"Digital lending Apps: There are increasing instances of illegal Loan Apps offering loans/micro credits, especially to people from low-income groups at exorbitantly high interest rates, and predatory recovery practices. RBI took several measures to tackle the problem."

3.8 On the issue of regulation of digital lending in India, the representative from Chase India, a public policy and advisory firm submitted as under:

"India witnessed twelvefold increase in the digital lending sector as per the Working Group on digital Lending (WGDL) report of the RBI. However, owing to unchecked industry practices, customers bore the brunt of unscrupulous lending practices such as providing loans at excessive interest rates, unethical and

predatory recovery practices, additional hidden charges applicable on lending transactions, misuse of customers' data, and much more.



Source:AReview ofIndia's Credit Ecosystem– joint reportby Experian andInvest India

With many individuals falling prey to the unscrupulous and usurious digital lending practices adopted by unauthorised DLAs, the RBI issued a Press Release on 23rd December 2020, warning consumers to be cautious while taking loans from such entities.

These concerns led RBI to set up the WGDL on 13th January 2021. WGDL was presented with a wide array of representation across public sectors as well as industry players. The WGDL report released on 18thNovember 2021 wherein it recommended the creation of a "list of NBFCs and the brand names and apps associated with them, which will serve as a whitelist of all the regulated apps in public domain.

Based on WGDL's Report, the RBI issued a Press Release on Digital Lending in August 2022, wherein recommendations made by the RBI's WGDL were identified for implementation; for in-principle approval requiring further examination; and for consideration by legislature stating further detailed guidelines. Pursuant to the Press Release, the RBI issued Guidelines on Digital Lending (DLG) in September 2022. The DLG laid out norms for players in the digital lending ecosystem with respect to their conduct, loan disbursal methods, fee/ charges, mandatory disclosures to customers, and grievance redressal measures, to name a few.

Also, in a latest development in February 2023, MeitY issued ban on some of the DLAs as part of a whitelisting exercise. A Rajya Sabha response in this regard further unveiled that the names of such whitelisted apps was provided by RBI to MeitY. After this development, recently Google Play Store also tweaked its

policy for listing of DLAs in lines with the latest guidelines and progress in the sector".

3.9 Ministry of Home Affairs in their post evidence replies furnished the following with regard to Digital Loan Apps:

"Digital loan Apps related frauds for the year 2022 are 26844 and for year 2023 are 9926.National Cybercrime Reporting Portal has a repository of all these suspected accounts reported on the portal and banks/financial intermediaries have visibility to this repository to act on these accounts. Banks/financial intermediaries also get the complete trail of the movement of fraud money and they can act on these to identify mule accounts. There is a need on parts of the banks and financial institutions to use this to plug the gaps in their KYC mechanisms and confirm to the prescribed fraud prevention and AML requirements.

I4C, MHA has prepared various reports on malicious loan apps/digital lending platforms and shared these reports to concerned stakeholders. List of apps are being regularly shared with Google Play Store to remove theses malicious apps from Play Store and Google has started taking action in many cases. Similarly, number of malicious loan apps has been recommended for blocking and the concerned committee in MeitY took necessary action on these apps. These reports are also shared with RBI to take necessary action. To overcome the menace of rogue loan Apps, RBI will have to device mechanisms to identify entities which area not confirming to its regulations. While guidelines for Digital Lending have been published by RBI, a mechanism to ensure adherence to these guidelines is still work in progress.

3.10 Regarding the key issues faced while dealing with fraudsters the representatives from Paytm submitted as under:

(i) Easy movement of fraudster from one payment operator to another - It is very easy for a fraudulent merchant to move from one payment operator to another if he / she is blocked at one place for fraud.

(ii) Lack of a central list of fraudulent merchants at a pan India level - There is no such list of fraudulent merchants which can be identified by a common identifier(e.g., GST Number, PAN Card, Aadhaar Card) which can be shared with all PAs to ensure that merchants from that list are not allowed to operate on any PA service provider.

(iii) Lack of Industry Forum to exchange best practices and latest fraud trends -There is no formal industry and government forum to exchange best practices and share latest trends of fraud being experienced in the market.

3.11 As regards to cyber security for Banks, M.D, Yes Bank stated as under:

"Regular audit of the entire bank system is very necessary, especially in terms of D-DOS attack, today it is more in terms of what is the resilience of the banks to immediately able to come back with the systems"

3.12 Highlighting the regulatory gaps with regard to cyber security, the representative from Reserve Bank of India during the oral evidence proposed as under:

"The first area which I feel is the extent of involvement of third-party service providers. Now, our reach of the third-party service providers is limited whereas the banks and the other regulated entities are relying more and more on the third-party service providers and some of the third-party service providers become very, very critical and systemically very important which include some of the Big Techs also. We have a list of top 25 systemically important third-party service providers. Now, we have started engaging with them directly with the help of banks to see what control they lack and how we enforce the controls through the commercial banks. That is the first important gap. Many of the countries' central banks are armed with statutory powers to regulate third-party service providers to the extent they provide services to banks. This could be one way including the Big Techs and the other fin techs.

The second gap where we need to improve is the cooperative banks and the non-banking finance companies. Our reach over them is not as much as in the case of banks. So, while banks have attained a certain level of cyber security maturity, that is not the case with these cooperative banks and the NBFCs and we have seen some types of attacks for example, ransomware attack.

The third area where we feel that there is need for improvement is downtime critical payments. People do not visit a branch any longer. They are so much dependent on channels like internet banking etc. Any major downtime in the services on account of either a cyber security attack or any other reasons can have an impact on customer services. We do find despite of best efforts that there are banks where this happens and that is an area where we are closely working with banks to improve this area.

The fourth is global issues. The regulation in this area is mostly reactive. It is unlike any other area. We probably cannot be so proactive because we find a certain type of act, we react to it".

3.13 Regarding regulatory gap, Director-General, CERT-In Shri Sanjay Bahl stated as under:

"Under the current framework it is observed that the SMS template is required to be registered by the entity. But the SMS template contains both fixed characters and variable characters. We have observed that this variable part of the SMS template is being misused by the threat actors for sending malicious links. Such things we have already highlighted. Also, the telemarketer after receiving three unique IDs from the entity does not verify whether the IDs provided to it belongs to the genuine entity or not. These are some of the gaps which we have seen. You have seen in terms of the maker-checker process, it is not being completely followed while modifying user rights in internal applications. This can lead to insider threats. Implementation of NEFT, RTGS, IMPS etc. by banks requires much more stringent security controls. These are some lapses. Last year, there have been about 16 per cent ransomware cases out of the overall ransomware cases here in the financial sector. In terms of challenges at ATMs, we have seen that the end-to-end encryption has not been implemented at ATM channel communication. We have also seen that the network cables and the ports within the ATM premises have not been concealed properly and are accessible to threat actors."

Chapter - IV

Enforcement Capacity and Regulation

4.1 Ministry of Electronics and Information Technology (MeitY).

The Indian Computer Emergency Response Team (CERT-In) has taken following actions for enhancing the cyber security posture and preventing cyber attacks:

(i) CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers and networks on regular basis.

(ii) CERT-In is operating 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.

(iii) CERT-In has set up the National Cyber Coordination Centre (NCCC) to generate necessary situational awareness of existing and potential cyber security threats and enable timely information sharing for proactive, preventive, and protective actions by individual entities.

(iv) CERT-In has formulated a Cyber Crisis Management Plan for countering cyber attacks and cyber terrorism for implementation by all Ministries/ Departments of Central Government, State Governments and their organizations and critical sectors.

(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 75 such exercises & drills and tabletop exercises have been conducted by CERT-In, where 1015 organisations from different States and sectors have participated.

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

(vii) CERT-In is operating the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre). The centre provides detection of malicious programs and free tools to remove the same for citizens and organisations. Currently alerts regarding malware infections and vulnerable services along with remedial measures are being sent to 755 organisations across sectors on daily basis.

(viii) CERT-In operates Responsible Vulnerability Disclosure and Coordination program to promote identification and disclosure of vulnerabilities by security researchers to enable timely remediable measures by OEMs/vendors/entities.

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

4.2 Security capabilities of banking sector and cooperative banks

(i) CERT-In, through RBI, has advised all authorised entities and banks issuing pre-paid payment instruments (wallets) in the country to carry out special audit by CERT-In-empanelled auditors, close the non-compliances identified in the audit report and ensure implementation of security best practices.

(ii) As per analysis audits by CERT-In empanelled auditors during the year 2022, the following are key trends.

(a) All Public and Private sector banks and Payment banks have conducted audits.

(b) Out of 1886 Cooperative banks, around 206 cooperative banks have conducted audits, which is 10.92 %.

(c) 91% Small Finance banks have conducted audits

(d) 39% of Gramin banks have conducted audits

(e) Major factors of vulnerabilities found during the audits are usage of vulnerable software versions and configuration errors.

4.3 Budget

A budget of Rs. 383 crores, 475 crores and 585 crores was allocated for CERT-In and its projects during the Financial year 2021-22, 2022-23 and 2023-24 respectively.

4.4 Manpower:

CERT-In currently has 126 sanctioned technical manpower. Proposal for enhancement of manpower at various levels has been submitted to MeitY and is being processed.

As informed by RBI, the supervisory strategy for cyber security is given as below:

(i) A robust supervisory mechanism is essential to enable RBI to evaluate the risk and compliance measures adopted by REs (commensurate with their risk exposure) along with their sustenance on an ongoing basis.

(ii) Onsite IT Examination: The compliance with extant instructions and IT/ cyber risks are assessed through IT Examinations. Focus of such examinations include a) IT Governance b) maintenance of basic cyber hygiene, c) Oversight over third-party service providers, d) effectiveness of business continuity and disaster recovery processes, e) robustness of IT Assurance mechanism.

(iii) Offsite Surveillance: The cyber security posture of supervised entities is monitored through collection and analysis of varied data/ information on a periodic and ad hoc basis, supplementing IT examinations as under:

(a) The cyber security posture is captured through a set of quantifiable indicators (Key Risk Indicators) which is collected on a quarterly basis. A composite score is arrived at based on these data points which provides an indication of the relative cyber security posture of the banks. The scoring model is revised from time to time to capture the emerging risks.

(b) Other periodic data which are collected include data on public facing applications and their databases, data on downtime of digital banking channels, cyber incident summary, DR testing etc. The compliance with extant advisories, circulars/ Master Directions are also assessed through offsite monitoring which are further validated in the onsite IT examination.

(iv) In cases where persistent issues of non-compliance are observed in the entities, appropriate supervisory actions are initiated. These range from engagement with the bank's Senior Management/ concerned members of the Board through letters and meetings to more severe measures such as imposing restriction on business activities and enforcement action through imposition of penalty.

(v) Adoption of advanced tools to assess cyber security posture of Regulated Entities Supplementing the on-site IT examinations and off-site surveillance, other supervisory tools are recently employed to assess the cyber security posture of the REs as under:

(a) Phishing Simulation Exercise: The objective of this exercise is to conduct phishing simulation across selected REs and assess their awareness in handling phishing emails.

(b) Cyber Reconnaissance: The Cyber Reconnaissance (Cyber Recon) initiative aims to enhance offsite surveillance by providing an insight into external view of the cybersecurity risk posture of REs. The proactive monitoring of cyber space initiative endeavours to find and collate sensitive data on REs available in public domain and analyse the same to provide pre-emptive information on the cybersecurity risk vectors of REs.

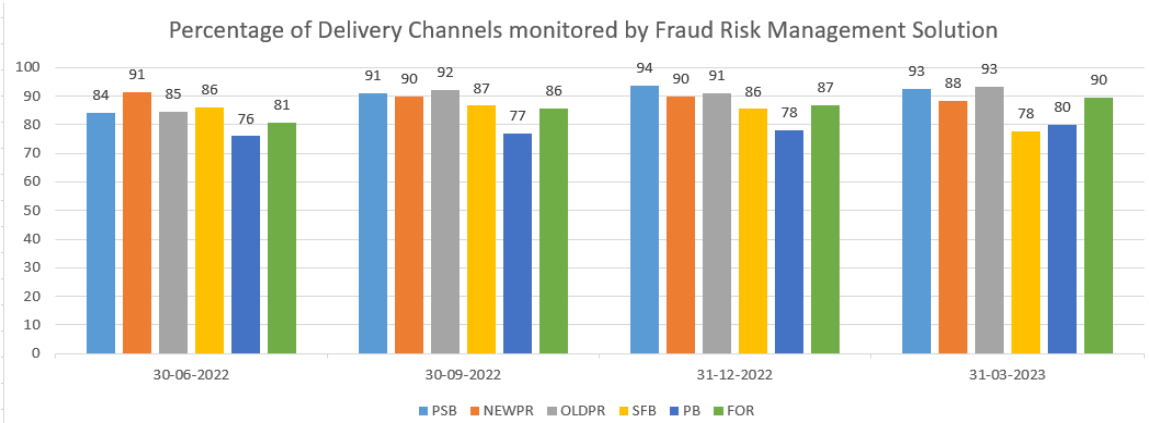
(c) Tabletop Exercises: Table-top cyber security exercises are scenario-based, open forum discussions which are conducted to test entities' preparedness and response in mitigating the consequences of cyber security incidents and crisis. RBI regularly conducts table-top cyber exercises for banks, UCBs and NBFCs. Till date, 11 such exercises have been conducted.

4.5 On the question to provide data on the level of preparedness and response time in handling cybercrime incidents, Ministry of Electronics and Information Technology the Department of financial Services submitted as follow:

"CERT-In notifies the affected organisations along with remedial actions to be taken, and coordinates incident response measures with affected organisations, service providers, respective sector regulators and law enforcement agencies.

Typically, in 85% of incidents reported, initial response is sent within 4 hours of receiving the security incident. Depending upon the type and scale of cyber attack and assets affected, containment of cyber security incident, remedial measures and detailed analysis take few hours to few months.

CERT-In has taken measures to enable organisations to prevent and respond to cyber security incidents in timely manner, by sending proactive threat intelligence alerts, providing situational awareness, conducting mock drills and training programs".



**PSB – Public Sector Banks, NEWPR – New Private Sector Banks, OLDPR – Old Private Sector Banks, SFB – Small Finance Banks, PB – Payment Banks, FOR – Foreign Banks.*

(All in Lakh)

Sample data of 24 banks	Total number of alerts generated by the bank's FRM System in FY 2021-22	Total number of alerts generated by the bank's FRM System in FY 2022-23	Number of alerts that prevented/ mitigated the loss at customer end in FY 2021-22	Number of alerts that prevented/ mitigated the loss at customer end in FY 2022-23	Amount (approx.) of loss that was prevented FY 2021-22	Amount (approx.) of loss that was prevented FY 2022-23
	361	407	1	4	13900	22500
Yo-Y Improvement		13%		300%		62%

On a sample assessment of 24 banks, it is seen that the number of alerts generated by the banks' fraud risk monitoring system has increased 13% on a year-on-year basis (in FY 2022-23 as compared to FY 2021-22) and approx. ₹225 crore of

fraudulent transactions were prevented in FY 2022-23 as compared to ₹ 139 crore in FY 2021-22 (a Y-o-Y increase of 62%).

4.6 Regarding cyber crime hotspots, the ministry of Home Affairs deposed as under:

> "There is a massive lack of awareness in cyber attacks among the users. These are the hotspots which the hon. Members have already mentioned. The top ten districts of the country are accounting for 81 per cent of the cybercrimes. The very basic problem is that 1930, the landing place, many places are not integrated with the main control room. In fact, we have had many meetings and most of them are sensitised now that 1930 should not be just put away in some SP's room, it should be there in the control room which is 24X7 monitored, that is manpower available always. Many of the banks have still not given for this 1930 helpline a kind of importance that has to be given. Likewise, the banks also must really get their act together and give some allocation to 24X7 to quick redressal of the problem. We are only able to save some Rs. 8 or Rs. 10 out of the Rs. 100 because of the time taken to complete the process and by that the time that much of money has flown out of the banks. So, this is an important issue."

4.7 When asked about the situation of law enforcement in cybercrime hotspots region, Ministry of Home Affairs in their post evidence replies stated as under:

> "There are issues of inadequate enforcement in the areas where hotspots exist. There have been several arrests made from these areas by various police agencies in the hotspot areas. Most of the offences under IT Act 2000 are bailable in nature. In many cases the same individual and gang have been found to be involved in many cases across the country. I4C's JMIS platform has identified that in 233 cases where 872 arrests were made, the arrested person were involved in 267170 cases. Stricter penal provisions and making bail condition stricter and making provision for local sureties would be necessary."

4.8 Regarding FIRs registered across the states, the Ministry of Home Affairs stated as under:

> "About the number of FIRs filed throughout the country, there is a variation. Overall, the national average is about 1.7 per cent. For every 100 complaints that come to the NCRP, the States are registering 17 FIRs."

4.9 On being asked as to why specific action has not been taken to crush the cybercrime gangs in cybercrime hotspots, the Ministry of Home Affairs their post evidence replies furnished as under:

"'Police' and 'Public Order' are State subjects as per the Seventh Schedule of the Constitution of India. States/UTs are primarily responsible for the prevention, detection, investigation, and prosecution of crimes through their Law Enforcement Agencies (LEAs). MHA largely play the role of a coordinator and facilitator. The Ministry of Home Affairs has set up Indian Cyber Crime Coordination Centre (I4C) to handle all the issues related to prevention, detection, and prosecution of cybercrime in a comprehensive and coordinated manner. I4C has seven verticals to play this role.

One of the verticals, Joint Cybercrime Coordination Team (JCCT), is tasked to achieve an effective coordination among State/UTs for inter-state investigation assistance, intelligence-led operation, criminal profiling, and data sharing, and cooperating on all other aspects of cybercrime and cyber threats. I4C, MHA has constituted seven JCCTs comprising various States/UTs vide references cited above".

4.10 With regard to regulatory gaps, capability gaps and institutional gaps in the existing cyber security framework, Ministry of Home Affairs stated as under:

"Misuse of SIM cards has been a matter of recurrent concern for all Law Enforcement Agencies. DoT has introduced new facial recognition technology-based methods to reduce instances of fake KYC based SIM cards. I4C along with DoT has also created a web portal for near real time blocking of SIM cards involved in cyber frauds. Since its launch in May 2023 this portal has helped block 1,19,732 SIM cards. The scope of this portal would be increased to include blocking of mobile devices involved in cyber frauds.

INTERPOL's Global Rapid Intervention of Payments (IGRIP) is a system being implemented by INTERPOL to block fraud related transaction across the world. CBI & I4C, MHA may be integrated with this system in future to track and block fraudulent transactions.

As per data published by NCRB in Crime in India 2021, the conviction rate was 3.6%. As per data available with I4C, in the year 2022 out of 694424 complaints related to financial frauds, in 2.6% cases FIR were issued.

Continuous education of investigating officers is being done by the State Police Forces. I4C has also been conducting training and orientation program through CyTrain portal of NCTC (cytrain.ncrb.gov.in), periodic sponsored trainings and weekly program call "Peer Learning".

4.11 Elaborating further on the issue Ministry of Home Affairs submitted as under:

"Legal powers under IT Act, 2000

Cyber Security powers with MeitY:

Section 70 of IT Act, 2000- Protected system:- The appropriate Government may, by notification in the Official Gazette, declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system.

i. Under Section 70B of the IT Act, 2000 Government of India has appointed Indian Computer Emergency Response Team (CERT-In) under MeitY as the National Nodal Agency for performing the functions described under the Information Technology (The Indian Computer Emergency Response Team and manner of performing functions and duties) Rules, 2013.

ii. Under Section 70A of the IT Act, 2000 the Government of India has designated "National Critical Information Infrastructure Protection Centre (NCIIPC)" under NTRO as the National Nodal Agency in respect of Critical Information Infrastructure Protection for performing the functions described under the Information Technology (National Critical Information Infrastructure Protection Centre and manner of performing functionsand duties) Rules, 2013.

However, MHA has not been given any mandate on Cyber Security which comes under the domain of Ministry of Electronics and Information Technology and NTRO. However, since MHA regularly coordinates with States and UTs for multifarious responsibilities on issues related to cyber security, MHA needs to be given a legal mandate of cyber security too.

Regulatory framework for Cyber Security in context of MHA

<u>Administrative arrangements</u>:

i. The proposal of National Security Council Secretariat (NSCS) on Framework for Enhancing Cyber Security of Indian Cyberspace was approved by the Cabinet Committee on Security on 08.05.2013 by assigning various responsibilities among following Ministries and Departments/Agencies, securing cyberspace. MHA was given the responsibility for framing policies related to classification, handling and security of information relating to Government. Accordingly, in the year 2014, "National Information Security Policy and Guidelines (NISPG)" was issued by the MHA to all Ministries and Departments for its implementation.

Further, a version of NISPG on `information security' was also issued by MHA in 2019.

ii. In pursuance of Cabinet Secretariat's direction dated on 11.07.2022, a Monitoring Committee under the chairmanship of Special Secretary (CIS), MHA was constituted on 26th July, 2022 to follow up the compliance regarding the implementation of shared Advisories, Indicator of Compromises (IoCs), TTPs (Tactics, Techniques, and Procedures), Alerts, etc., related to cyber and information security. Till date, six meetings of the Monitoring Committee have been convened.

iii. As per Government of India (Allocation of Business) Rules, 1961, Ministry of Home Affairs (MHA) is tasked to administration the Official Secrets Act, 1923. However, the MHA does not have legal mandate in the matter of cyber security.

Proposed amendments in IT Act:

i. MHA needs to designated as one of the National Nodal Agency in respect of CriticalInformation Infrastructure Protection.

ii. MHA needs to be empowered to notify Cyber Forensic labs as 'Examiner of ElectronicEvidence' under Section 79A of the Information Technology Act 2000

MHA to be made the nodal agency for negotiation of international treaties with respectto cyber crime and cyber security, on various forums/ Conventions.

4.12 Institutional Gaps

RBI's working group on Digital Lending in its report dated 18th November 2021 has recommended setting up of a Digital Trust Agency (DIGITA) which would ensure that only authorized and trusted Digital Apps are used by consumer. A multi-disciplinary DIGITA with enlarged mandate covering other public concerns like Digital Advertisement, investments, Trading, Gaming, and e-Sports is necessary. This agency can serve as a watch dog against fraudulent activities and fill in the regulatory gaps currently being experienced.

4.13 The Committee further enquired if any specific study has been conducted to further classify each of these categories of fraud, the Ministry of Home Affairs in its post evidence replies submitted that as under:

"I4C studies the complaints reported on National Cybercrime Reporting Portal and prepare analysis reports to share with all the concerned stakeholders with a view to sensitize them and help them in taking necessary preventive action and investigation of the complaints. These analysis reports are shared with State/UT

Law Enforcement Agencies, banks and other financial intermediaries, service providers like Google, GoDaddy etc. to take necessary action. Many of these analysis reports has led to immediate action by the LEAs, banks, and other concerned stakeholders.

Apart from the categories defined on National Cybercrime Reporting Portal (NCRP), I4C also analyzes the complaints according to the modus operandi and technology used by the fraudsters; digital lending applications, loan apps, investment apps, .apk files, use of social media, phishing, vishing etc. I4C also figure out the keywords of cybercrime and working to provide facility to tag the cybercrimes as per the new modus operandi. Options for tagging to categorize these complaints by the police officials taking complaints on helpline number 1930 are being created.

The ontology of cybercrime as used in the NCRP needs regular updating in view of evolving nature of threat vectors and modus operandi. Efforts will be made to reach global classification protocols to make the categories more specific and amenable to analysis."

4.14 When enquired about the functioning of National Cyber Crime Helpline number 1930 and whether the Government has adopted any worldwide best practices for controlling cybercrime, Ministry of Home Affairs submitted as under:

"National Cybercrime Helpline number 1930 has been established for ease of reporting of cybercrime complaints by citizen. The call made on helpline number lands in the respective states from where call has been made and that is responded by the State Law Enforcement Agency which is further escalated through an automated system to the concerned bank/financial intermediaries in case of financial fraud. Action on these complaints is taken by the concerned State/UT LEAs and bank/financial intermediaries. MHA has provided financial assistance to States to strengthen 1930 Call Centers under Hon'ble Home Minister's discretionary funds in March 2023.

MHA analyzes the work being done in the other countries in the area of cybercrime and tries to learn from the best practices used there. MHA with the help of MEA is making efforts for exchange of best practices with foreign countries. A MoU is under consideration between I4C, MHA and IC3 of FBI, USA for sharing of best practices in the area of cybercrime investigation.

CBI is the National Central Bureau for India for cooperation with INTERPOL. IGRIP system of Interpol can also be integrated with Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS) in future. All Law Enforcement Agencies submit their request for information and any other request to CBI which is further processed and sent to INTERPOL for their response. Reponses are received at CBI and forwarded to concerned LEAs of States/UTs."

4.15 On being asked how many cyber security police staff are present in police stations, the Ministry of Home Affairs furnished the following:

"Different States have different levels of capabilities to handle cybercrime investigations at Police Station Levels. MHA has been conducting regular training courses to equip police staff with requisite skillsets through its National Cybercrime Training Centre (NCTC) and National Cybercrime Forensic Laboratory (NCFL) verticals. The list of cyber Police Stations across the states is mentioned below."

Cyber Police Station in all States/UTs

State/UTs	Total Cyber Police Station
Andaman and Nicobar Islands	1
Andhra Pradesh	17
Arunachal Pradesh	1
Bihar	1
Chandigarh	1
Chhattisgarh	1
Dadra & Nagar Haveli and Daman & Diu	1
Delhi	15
Goa	1
Gujarat	23
Haryana	29
Himachal Pradesh	3
Jammu and Kashmir	2
Jharkhand	7
Kerala	19
Ladakh	2
Lakshadweep	1
Madhya Pradesh	1
Maharashtra	55
Manipur	1
Meghalaya	1
Mizoram	1
Nagaland	1
Odisha	15
Puducherry	2
Punjab	1

Rajasthan	1
Sikkim	3
Telangana	3
Tripura	1
Uttar Pradesh	18
Uttarakhand	2
West Bengal	35
Assam	1
Karnataka	45
Total	**312**

4.16 With regard to the programme on security awareness and training to the bankers and police officers, the Ministry of Home Affairs furnished the following:

"Most criminal gangs operating from the hotspots have evolved from some other physical world criminal modus operandi and these areas were having criminal gangs operating in physical space earlier. They have now migrated to cyberspace and have rapidly increased in numbers and spread due to various reasons. Proactive policing in such places ensures that hotspots do not develop.

(i) Under Cyber Crime Prevention against Women & Children (CCPWC) Scheme, MHA has provided financial assistance to the tune of Rs.122.24 crores to States/UTs for setting up of Cyber Forensic-cum-Training Labs, training of LEAs and hiring of Jr. Cyber Forensic Consultant.

(ii) Cyber Forensic-cum-Training Laboratories have been commissioned in 33 States/UTs namely Andhra Pradesh, Arunachal Pradesh, Assam, Bihar, Chhattisgarh, Gujarat, Haryana, Himachal Pradesh, Kerala, Karnataka, Madhya Pradesh, Maharashtra, Mizoram, Odisha, Sikkim, Telangana, Uttarakhand, Uttar Pradesh, Goa, Meghalaya, Nagaland, Dadra and Nagar Haveli & Daman and Diu, Punjab, Tripura, Puducherry, Chandigarh, J&K, Rajasthan, West Bengal, Jharkhand, Manipur, Andaman& Nicobar Islands and Delhi.

(iii) Training curriculum has been prepared for LEA personnel, Public Prosecutors and Judicial officers for better handling of investigation and prosecution. States/UTs have been requested to organize training programmes.

(iv) Workshop and hands-on-training for Law Enforcement Authorities on functioning of Cybercrime Reporting Portal (www.cybercrime.gov.in) are being organized.

(v) Under I4C Scheme, National Crime Records Bureau has developed a Massive Open Online Courses (MOOC) platform called 'CyTrain' portal. CyTrain portal helps in the capacity building of police officers/judicial officers through online course on critical aspects of cybercrime investigation, forensics, prosecution etc. along with certification. More than 37,700 Police Officers from States/UTs are registered for training and more than 18,700 Certificates issued through the portal.

(vi) 36118 LEAs, 2022 Judicial Officer and 2240 Public Prosecutors have been trained by MHA, State Government and Bureau of Police Research and Development (BPR&D).

(vii) Under I4C Scheme, a state-of-the-art Cyber Lab has been established through C-DAC at NCRB HQ, New Delhi. The Lab is equipped with more than 25 latest Digital Forensics tools from industry and more than 50 open source cybercrime detection and forensics tools. The Cyber Lab is also integrated with the MOOC platform (CyTrain portal) and called as e-Cyber Lab which was launched on 13.10.2020 for providing virtual experience on experimentation on the latest modus operandi on cybercrime. The officers can log into e-Cyber Lab and learn about and use any tool on pre-arranged use cases or by importing their own problem statement.

(viii) National Cyber Forensic Laboratory (Evidence) {NCFL(E)} has been set up at Hyderabad. Establishment of this laboratory provides the necessary forensic support in cases of evidence related to cyber crime, preserving the evidence and its analysis in line with the provisions of IT Act and Evidence Act; and turnaround time is reduced to 50%."

4.17 The Committee further enquired whether any concerted efforts have been done in the cyber crime hotspots Districts along with their cooperation with the Interpol, the Ministry of Home Affairs furnished the following:

"CBI is the National Central Bureau for India for cooperation with Interpol and all the correspondence with Interpol is being done through CBI. All Law Enforcement Agencies submit their request for information and any other request to CBI which is further processed and sent to Interpol for their response. Reponses are received at CBI and further sent to concern LEAs.

An online module has been developed for immediate blocking of SIM Cards reported by State/UT LEAs. It is hosted on National Cybercrime Reporting Portal and All State/UT LEAs can raise their request for blocking of SIM cards.

The authorized officer can send the request in a prescribed format and that will be escalated to concerned Telecom Service Providers (TSPs) for blocking of number. So far more than 1 lakh SIM card has been blocked using this module.

National Cybercrime Reporting Portal (cyberpolice.nic.in) not only works as a platform to take action on the complaints reported on National Cybercrime Reporting Portal (cybercrime.gov.in) and through National Cyber Crime Helpline Number 1930 but also works as an effective coordination mechanism. It has been developed in such a manner that all the State/UT Law Enforcement Agencies, Department of Telecommunication, Banks, wallets, merchants, and other financial intermediaries, TSPs, etc. are integrated and work in collaboration with each other. Not only the information related to complaints is being shared through this platform but also analysis reports, advisories, SOPs etc. are being shared.

Joint Cybercrime Coordination Team (JCCT) are also an effective mechanism for coordination among State/UTs for inter-state investigation assistance, intelligence-led operation, criminal profiling, and data sharing, and cooperating on all other aspects of cybercrime and cyber threats. I4C, MHA has constituted seven JCCTs comprising various States/UTs so far which covers all the States/UTs of the country.

To effectively neutralize the hotspots, apart from effective police action on the ground, the communication and financial channel used by the fraudsters also need to be blocked. This would involve working in close coordination with DoT, MeitY, DFS, RBI and other stakeholder ministries and departments."

Chapter – V

Impact of Artificial Intelligence / Chatbot on Cyber Security

5.1 When asked about the Impact of AI and Chatbot on cyber security, during the committee sitting on 15th June, 2023 representative of RBI deposed as under:

> "The volume, value and velocity of each transaction are getting monitored by AI. Even the fraud risk monitoring solutions are becoming AI-enabled, to make them practically identify such patterns which are not put through a manual transaction, and they are able to detect it. Of course, the maturity level of these FRM solutions across the banking sector or within banks is also different, but we are monitoring it continuously and trying to improve it."

5.2 Ministry of Electronics and Information Technology (MeitY) in its post evidence reply stated as under:

> "AI and chatbot technology have significantly influenced the landscape of cyber security and have improved threat detection, enhanced automation, advanced analytics, Intelligent authentication, threat intelligence and prediction, efficient incident response, behaviour-based anomaly detection and in adaptive and self-learning systems. AI-based security solutions can be used for enhancing cyber security as it offers continuous learning from historic and real-time data, quick response to cyber incidents and proactive identifying cyber-attacks and prevention. MeitY has initiated the National Program on AI (NPAI) – 'India AI', to make India the global leader in the AI space and ensure responsible and transformational use of AI for All. The objective of NPAI is to adopt a whole-of-governmentapproachforleveragingdisruptivetechnologiestofosterinclusion, innovation, and adoption for social impact."

5.3 During the course of oral evidence on 4th July 2023, Flipkart further elaborated on the impact of AI and Chatbot as under:

> "We do believe that new generative models, the large language models that are now on the rage in the AI community and around the world, do have the element of making it more accessible by writing code, setting up fake websites, etc., at least some level of technical know-how that people could buy in the past. Now, it makes it a little bit easier to do so. We do expect that there will be more escalation of these kinds of threats with the further prevalence of AI."

Chapter - VI

Grievance Redressal Mechanism and Compensatory Mechanism for the Victims of Cyber Crimes

6.1 RBI has advised its regulated entities (REs)to implement customer grievance redressal mechanisms at their end:

(i) Limiting Liability of Customers in Unauthorized Electronic Banking Transactions: RBI has issued instructions to banks regarding limiting customer liabilities in unauthorised/fraudulent electronic transactions. The salient features of the framework are as under:

(a) The burden of proving customer liability in case of unauthorised electronic banking transactions lies on the bank.

(b) Zero Liability: A customer need not bear any loss if the deficiency is on the part of the bank and in cases where the fault lies neither with the bank nor with the customer but lies elsewhere in the system and the customer notifies the bank within three working days of receiving the communication about the unauthorised transaction.

(c) Limited Liability: Where the loss is due to the customer's negligence, the customer has to bear the entire loss until he reports the unauthorised transaction to the bank; and where the fault lies neither with the customer nor with the bank and lies elsewhere in the system and the customer reports between four to seven working days of the unauthorised transaction, the maximum liability of the customer ranges from ₹5,000 to ₹25,000, depending on the type of account/ instrument.

(d) Liability as per Board approved policy: If the unauthorised transaction is reported beyond seven working days, the customer liability shall be determined as per the bank's Board approved policy.

(e) Providing shadow credit for Zero Liability/ Limited Liability of customer:

i. On being notified by the customer, the bank shall credit (shadow reversal) the amount involved in the unauthorised electronic transaction to the customer's account within 10 working days from the date of such notification by the customer (without waiting for settlement of insurance claim, if any). Banks may also at their discretion decide to waive any customer liability in case of unauthorised electronic banking transactions even in cases of customer negligence.

ii. Banks have been advised to ensure that a complaint is resolved and liability of the customer, if any, established within such time, as may be specified in the bank's Board approved policy, but not exceeding 90 days and the customer is compensated as given above. Where banks are unable to resolve the complaint or determine the customer liability, if any, within 90 days, the compensation as prescribed is paid to the customer.

iii. Thus, the burden of proving customer liability in case of unauthorised electronic banking transactions lies on the bank. The circular, in addition to laying down the liability of customers, also prescribes guidelines for strengthening systems and procedures to be put in place by banks/PPI issuers for preventing such frauds.

(f) Limiting Liability of Customers in Unauthorised Electronic Payment Transactions in Prepaid Payment Instruments (PPIs) issued by Authorised Non-banks – similar criteria, like those for banks above, have also been formulated for determining the customers' liability in unauthorised electronic payment transactions resulting in debit to their PPIs issued by non-bank PPI Issuers. Accordingly, zero liability of customer exists where the unauthorized transactions has occurred due to contributory fraud/negligence/ deficiency on the part of PPI Issuer (irrespective of whether the transactions is reported by the customer or not) and in case of third-party breach where the deficiency lies neither with the PPI Issuer nor with the customer but lies elsewhere in the system, and the customer notifies the PPI Issuer within three working days of transactions.

(g) Harmonizing Turn Around Time (TAT) for resolution of customer complaints and compensation for failed payment transactions - In order to bring uniformity and discipline in reversal of unsuccessful or 'failed' transactions, RBI has put in place a framework harmonising the Turn Around Time for resolution of customer complaints and customer compensation for failed transactions in some payment systems, i.e. ATMs, Unified Payments Interface (UPI), Immediate Payment Service (IMPS), PPIs and card payments. The framework has come into effect from October 15, 2019. The framework prescribes the TAT for failed transactions as also a compensation framework providing suo moto compensation to customers for delay in execution or reversal of such transactions beyond the prescribed TAT. Wherever financial compensation

is involved, the same shall be affected to the customer's account suo moto, without waiting for a complaint or claim from the customer.

(ii) Vide RBI circular dated September 20, 2019, instructions have been issued to all operators and participants of authorised payment systems for time-bound resolution (harmonisation of turn-around-time) of failed transactions; failure to do so may lead to payment of compensation (as prescribed in the circular) to customers.

(iii) Online Dispute Resolution (ODR) System for Digital Payments was introduced on August 06 2020 for resolving customer disputes and grievances pertaining to digital payments, using a system-driven and rule-based mechanism with zero or minimal manual intervention.

(iv) Vide Master Direction on Digital Payment Security Controls issued on February 18, 2021, REs has been advised to:

(a) incorporate secure, safe, and responsible usage guidelines and training materials for end users within the digital payment applications.

(b) provide digital payment products and services to a customer only at her/ his option based on specific written or authenticated electronic requisition along with a positive acknowledgement of the terms and conditions.

(c) provide a mechanism on their mobile and internet banking application for their customers to, with necessary authentication, identify/ mark a transaction as fraudulent for seamless and immediate notification to the RE.

(v) RBI has put in place following mechanisms for effective redressal of grievances and consumer protection:

<u>Integrated Ombudsman Scheme</u>

(a) RBI had introduced the Banking Ombudsman Scheme, 2006 (BOS, 2006) with the objective of enabling resolution of complaints relating to services rendered by banks. On similar lines, the Ombudsman Scheme for Non-Banking Financial Companies (OSNBFC), 2018 was setup for complaints against NBFCs and Ombudsman Scheme for Digital Transactions (OSDT), 2019 for complaints pertaining to digital transactions.

(b) To make the Ombudsman mechanism simpler, more efficient and more responsive, RBI rolled out Reserve Bank - Integrated Ombudsman Scheme, 2021 (RB-IOS) by integrating the above existing three ombudsman schemes with effect from November 12, 2021.

(c) The ambit of the RB-IOS has been extended to cover Primary Urban Co-operative Banks holding deposits of ₹50 crore and above as well as Credit Information Companies, in addition to the entities (banks, non-banking finance companies and non-bank providers of Prepaid Payment Instruments) that were already covered under the Ombudsman mechanism through the three schemes.

(d) A centralised receipt and processing of complaints has been introduced following the 'One Nation One Ombudsman' approach under which there is no limitation of territorial jurisdiction for the customer. The scheme provides a single reference point for customers to file complaints, submit documents, track status, and provide feedback against RBI regulated entities specified therein. A toll-free number is also available for customers to seek assistance in filing complaints and information on grievance redress, with multi-lingual support.

(e) The new scheme has also done away with the restrictive grounds of complaints and now includes all complaints against the Regulated Entities (REs) relating to 'deficiency in service', other than the grounds explicitly excluded under the Scheme.

(f) The Complaint Management System (CMS) launched in 2019 is a one-stop web-based application for 24x7 lodging of complaints by customers of all the entities regulated by RBI and their redressal by the RBI. The complainant can track the status of the complaint and share feedback on CMS. The system is also enabled for online filing of appeal.

Internal Ombudsman Scheme for non-bank System Participants, 2019 -The Internal Ombudsman (IO) scheme for the large non-bank system participants, with more than one crore PPIs outstanding, institutionalised in 2019, facilitates a swift, efficient, and effective complaint redressal mechanism within the entity to ensure that customer complaints are adequately addressed at the level of non-bank System Participant itself.

(vi) Regarding amount of compensation provided to customers by REs, RBI do not have the requisite data.

6.2 Regarding consumer's liability in case of misuse of OTP, the representative of NASSCOM stated as under:

"The number or volume of a transactions that an end-user is specially processing, there is a tremendous amount of cognitive burden in terms of taking the decision,

basically because he has to get the OTP and fill that OTP in the system. He has to authorise the transaction. But even as an advanced user, he has to do so many transactions. So many OTPs are coming in basically. Sometimes that becomes very difficult. You may not have the security frame of mind or privacy frame of mind. Every time you are doing transactions basically. So, there is definitely some over-reliance on the OTP and because of that, user is exposed to vishing and phishing kind of a fraud. So, that is one of the important parts. That is also related to the kind of a liability equation that we see which has been designed. For example, if you are authorising the transaction, then you are liable. Banks and institutions are not liable, basically. It is because of OTP ecosystem the user actions are getting into the place and users are getting defrauded for that. That is why liabilities are setting on them."

Chapter - VII

Global Best Practices in Cyber Security

India's position with respect to cybercrime in relation to global best practices.

7.1 On asking as to how India is doing with respect to cybercrime in relation to global best practices, Indian Bank's Association submitted as under:

> "There is 38% increase in global cyber-attacks in 2022 vs. previous year. Source (Check Point Research). Check Point Research Report´s findings are based on data drawn from the Check Point Threat Cloud AI Cyber-Threat Map, which looks at the key tactics' cybercriminals are using to carry out their attacks. The data is based on estimates. As per Government Data India witnessed 13.91 Lakh cyber security incidents in 2022, down from 14.02 Lakhs in 2021.
>
> India ranks among top 10 in ITU's Global Cybersecurity Index
>
> As per the ranking, India has moved up by 37 places to rank as the tenth best country in the world in the Global Cybersecurity Index 2020 launched by the International Telecommunication Union on June 29, 2021. India has made it to the top 10 in Global Cyber security Index (GCI) 2020 by ITU, moving up 37 places to rank as the tenth best country in the world on key cyber safety parameters.
>
> As per the ranking, India has moved up by 37 places to rank as the tenth best country in the world in the Global Cyber security Index (GCI) 2020 launched by the International Telecommunication Union (ITU) on June 29, 2021. India has also secured the fourth position in the Asia Pacific region, underlining its commitment to cybersecurity.
>
> GCI assessment is done based on performance on five parameters of cyber security including legal measures, technical measures, organisational measures, capacity development, and cooperation. The performance is then aggregated into an overall score."

7.2 Global Best Practices for tackling Fraud (Regulations)

(i) The UK has introduced a Contingent Reimbursement Model Code for Authorized Push Payment (APP) Scams to reimburse the victims of scams in any case where the bank or payment service provider is considered at fault where the customer has met the standards expected of them under the Code. Currently, in other parts

of world customer education is widely resorted to avert such frauds and no code exists. This may be another area where "codes" for customers may be formed by regulators.

(ii) European Commercial Bank's (Euro Area Central Bank) Single Supervisory Mechanism (SSM) includes a dedicated section in its methodology for on-site inspections, has analytical tools for off-site supervisors, and produces a cyber-risk profile for each bank within its remit.

(iii) Supervisors are converging towards a threat-informed or intelligence-led testing framework for assessing cyber-risk vulnerability and resilience. An intelligence-led framework goes beyond a simulated cyber-attack to test a bank's cyber-risk vulnerability and resilience. Banks are then assessed on the quality of the intelligence gathered, and their detection and response capabilities, to establish whether their level of cyber-security is commensurate to the cyber-risk faced. For eg, UK's CBEST Threat Intelligence-Led Assessments, the Hong Kong Monetary Authority's iCAST (intelligence-led Cyber-attack Simulation Testing) Framework and Netherland Bank's TIBER (Threat Intelligence-Based Ethical Red Teaming) Framework.

(iv) Supervisory tools to assess cyber-risk vulnerability and resilience can be either voluntary or mandatory, for all or selected banks. The US National Institute of Standards and Technology (NIST) Cyber-security Framework (CSF) and the Federal Financial Institutions Examination Council (FFIEC) Cyber-security Assessment Tool (CAT) are both voluntary tools that banks can use to assess cyber-risk.

(v) Supervisors in different jurisdictions appear to be actively exchanging practices, but there is scope for more supervisory cooperation and collaboration.

Global Best Practices	Indian Context
Contingent Reimbursement Model Code for Authorized Push Payment (APP) Scams in UK: Reimbursement of victims of scams in any case where bank or payment service provider is considered at fault where the customer has met standards as per code.	UK is one of the few countries to adopt such code.
European Commercial Bank's (Euro Area Central Bank) Single Supervisory Mechanism (SSM) includes a dedicated section in its methodology for on-site inspections for cyber risk profiling of banks.	The Single Supervisory Mechanism (SSM) is the first pillar of the European banking union and is the legislative and institutional framework that grants the European Central

	Bank (ECB) a leading supervisory role over banks in the EU. RBI has a comprehensive Cyber Security Framework for Banks. However, “cyber risk profiling” is not categorically mentioned in that framework.
Supervisors are converging towards a threat-informed or intelligence-led testing framework for assessing cyber-risk vulnerability and resilience. eg. UK’s CBEST Threat Intelligence-Led Assessments, the Hong Kong Monetary Authority’s iCAST (intelligence-led Cyber-attack Simulation Testing) Framework	Though RBI’s Cyber Security Framework for Banks dated 2nd June 2016 have provision for only testing.
Supervisory tools to assess cyber-risk vulnerability and resilience can be either voluntary or mandatory, for all or selected banks.eg., The US National Institute of Standards and Technology (NIST) Cyber-security Framework (CSF)	As per RBI’s Cyber Security Framework for Banks dated 2nd June 2016, there is need for a Board approved Cyber-security Policy

OBSERVATIONS/RECOMMENDATIONS

The Committee put on record its appreciation of the many proactive and decisive steps taken to deal with cyber security and cyber crime by various Ministries, agencies of the Central Government, and many State Governments. India is indisputably one of the best regulated and safest digital financial ecosystems in the world. Yet, the Committee note with concern the mushrooming of cyber crimes and increasing data vulnerabilities even as digitisation has rapidly expanded across the country. Within a few years, it is likely that a billion Indian citizens will be conducting hundreds of billions transactions online mediated entirely through large-scale, pervasive computer networks, systems, and algorithms. Simultaneously, criminals are getting more and more innovative and difficult to track since they can now utilise powerful new technologies and operate in lightly policed or hostile jurisdictions. These new and threatening technologies include generative artificial intelligence (AI), chatbots, and quantum computing, which raises the threat level exponentially.

To maintain its status as one of the world's best digital financial ecosystems, India should consider evolving its cyber security policy framework across five major dimensions to: (1) establish a more dynamic and proactive regulatory framework; (2) empower a centralized authority for cyber security which can work with all digital ecosystem participants in India and around the world; (3) formulate fairer and more responsive consumer grievance redressal and compensation mechanisms; (4) strengthen central and state cyber security enforcement capabilities; and (5) achieve closer global cooperation with other leading countries. Working simultaneously across all these five dimensions will ensure that India develops the world's most innovative, secure, and resilient digital financial ecosystem.

1. Overall Regulatory Framework

The Committee note that cyber security regulations will have to evolve rapidly to take into account various technological developments and to stay ahead of bad actors. Firstly, the Committee observe that there have been challenges in exerting sufficient control over third-party service providers, including Big Tech and Telecom companies on cyber security matters. Secondly, downtime in critical payment systems is able to disrupt customer services, which is not currently

regulated. Thirdly, there is no clear process to either continuously whitelist or blacklist apps and maintain a central registry of apps that have the ability to tap digital payment and settlement systems. Today's regulatory frameworks are focused mostly on fire-fighting, but they need to be much more dynamic in anticipating and dealing with emerging threats and vulnerabilities of the digital financial ecosystem. Specific threats today include misuse of SMS templates, telemarketer verification lapses, insufficient maker-checker processes, weak security controls in fund transfer systems, and vulnerabilities in ATM channel communication. The situation is exacerbated by limited coordination among different agencies and inadequate incident response as well as enforcement mechanisms. The Committee, therefore, to strengthen cyber security measures, mitigate vulnerabilities, and ensure the integrity of the financial sector's digital infrastructure recommend the following concrete measures:

(i) Regulation of Service Providers: Enhance regulatory powers to oversee and control third-party service providers, including Big Tech and Telecom companies, by implementing comprehensive guidelines and standards. This includes ensuring stringent security controls, thorough vetting processes, bettereKYC verification, and regular audits of their cyber security practices. During the Committee hearings, RBI provided evidence that Big Tech companies have refused to make various modifications to their mobile operating systems to make the OTP based two factor authentication protocol even more secure. Such invaluable input from key regulators should not be disregarded by Big Tech companies.

(ii) Downtime in Critical Payment Systems: Collaborate closely with financial institutions to improve uptime and address recurring downtime issues in critical payment systems. This can be achieved by investing in robust infrastructure, conducting regular security assessments and establishing effective incident response mechanisms.

(iii) Proactive Global Regulatory Frameworks: Move towards a more proactive approach in global cyber security regulations by fostering collaboration between regulatory bodies, financial institutions, and technology experts. Encourage information sharing, joint threat intelligence.

(iv) Regularly audit the entire financial system especially cyber security and eKYC safeguards.

(v) Addressing current threats:

(a) **Misuse of SMS Templates: Strengthen regulations by imposing stricter controls on the variable part of SMS templates, requiring verification and validation processes to prevent malicious links and content.**

(b) **Telemarketer Verification: Establish stricter procedures for telemarketers to verify the authenticity of provided unique IDs, ensuring they belong to genuine entities and reducing the risk of fraudulent activities.**

(c) **Maker-Checker Processes: Enforce strict adherence to maker-checker processes for modifying user rights in internal applications to minimize the risk of insider threats and unauthorized access.**

(d) **Security Controls for Fund Transfer Systems: Implement more stringent security controls for electronic fund transfer systems, such as NEFT, RTGS, and IMPS, to safeguard against potential vulnerabilities and ensure secure transactions.**

(e) **ATM Channel Security: Mandate the implementation of end-to-end encryption for ATM channel communication and ensure proper concealment of network cables and ports to prevent unauthorized access and tampering.**

The Committee further recommend that a regulatory directive should be implemented mandating app stores to share exhaustive metadata and pertinent information about all the apps they host on their platforms This data repository will empower regulators to conduct in-depth analysis, identify potential security vulnerabilities and institute appropriate measures to fortify the digital landscape.

The Committee note that it is crucial to secure critical financial infrastructure against cyber threats as it ensures availability, reliability and integrity of financial services that directly impact public safety, national security, and the overall functioning of society. In light of this, the Committee emphasize the need for a strong and comprehensive legal framework that encompasses robust policies, procedures and guidelines along with advanced security technologies, regular risk assessments, employee training and incident response plan. Such a regulatory framework may be accomplished by (1) promulgating new rules; or(2) through amendments to the Digital India legal framework to explicitly address cyber security matters; or (3) by bringing in entirely new cyber security legislation. In fact, it may be necessary to evaluate all of these three actions. This

regulatory framework could enable closer supervision of digital ecosystem participants, strengthen investigative and enforcement powers, and provide better incident response capabilities. These amendments could also enable the establishment of a centralised "Cyber Protection Authority".

2. Centralised and Empowered "Cyber Protection Authority"

The Committee observe that the existing regulatory landscape for cyber security in India involves multiple agencies and bodies, each with distinct roles and responsibilities. This necessitates a high level of inter-ministerial coordination to effectively address the challenges and ensure a comprehensive approach to cyber security. The Committee note that the Ministry of Home Affairs (MHA) is responsible for cyber security policy formulation, while entities such as CERT-In and NCIIPC play vital roles in incident response, awareness creation, and protection of critical information infrastructure. In the financial sector, the Reserve Bank of India (RBI), along with IRDAI and PFRDA, ensures cyber security compliance. The Department of Financial Services (DFS) collaborates with regulators and the NCIIPC to identify critical financial IT infrastructure and designate them as protected systems under the IT Act, which falls under the Ministry of Electronics and Information Technology.

Thus, it is evident that there is a need for a centralized authority in ensuring cyber security, particularly for the financial services ecosystem. While the National Security Council Secretariat (NSCS) is responsible for coordinating, overseeing, and ensuring compliance of cyber security policies, there is no central authority or agency solely dedicated to cyber security. The Committee feel that the existing decentralized approach disperses regulation and control and thus hinders unified direction and a proactive approach to combating cyber threats. The Committee, therefore, strongly recommend establishment of a centralized overarching regulatory authority specifically focused on cyber security. Such a centralized authority would be analogous to the Directorate General of Civil Aviation (DGCA), which ensures a well-regulated and safe aviation system. This proposed authority would shoulder the responsibility of safeguarding the nation's critical IT infrastructure and networks from cyber threats. Collaborating with State Governments / district administration and private sector entities as well, it would develop and implement robust cyber security policies, guidelines, and best practices. Additionally, the Committee is of the view that it would serve as the

primary point of contact for cyber security information sharing and incident response coordination including effective enforcement at the ground level.

The Committee acknowledge the cyber security challenges faced by cooperative banks, non-banking financial companies (NBFCs), merchants, vendors, and other smaller participants in the digital financial ecosystem in India. It has been brought to the Committee's attention that these institutions experience a higher number of cyber security incidents compared to commercial banks. Furthermore, the Committee observe a significant disparity in the conduct of cyber security audits between cooperative banks and scheduled commercial banks. While all scheduled commercial banks have completed their audits, only a small percentage of cooperative banks, approximately 10.92 percent (206 out of 1886 banks), have undertaken such audits. The Committee have also observed that while commercial banks face more IT incidents such as functionality bugs and downtime, cooperative banks exhibit weaker cyber resilience, leading to a higher occurrence of cyber security incidents. The Committee have been informed that the banking sector is relatively advanced, whereas NBFCs, cooperative banks, merchants, and vendors encounter challenges due to limited manpower and technological capabilities.

The Committee are of the view that cyber security concerns surrounding all these various ecosystem participants demands immediate attention. The observed higher number of cyber security incidents in cooperative banks highlights the urgency to strengthen their cyber resilience. It is imperative that these entities enhance their technological capabilities and manpower to effectively mitigate cyber risks. To address the issue, the Committee recommend a multi-pronged approach led by the Cyber Protection Authority (CPA).

Firstly, ecosystem participants should prioritize investments in robust cyber security infrastructure, including advanced threat detection systems and secure data storage practices.

Secondly, comprehensive training programs should be implemented to raise awareness among employees and customers regarding cyber threats, phishing attacks, and best security practices.

Thirdly, regular audits and assessments should be conducted to identify vulnerabilities and ensure compliance with RBI's parameters for inclusion in the CBS and payments system.

The Committee strongly advocate that the CPA engage ethical hackers to test ecosystem participants. The Committee feel by integrating ethical hackers

into their cyber security strategies, ecosystem participants can considerably heighten their defenses against cyber threats. To fully capitalize on this collaboration, the Committee recommend that ecosystem participants adopt a comprehensive approach. Firstly, they should meticulously outline the scope of engagement with ethical hackers, explicitly delineating the authorized systems and networks for testing. Establishing well-defined rules of engagement becomes imperative to ensure a controlled and precisely targeted testing process. Rigorously verifying the credentials and expertise of ethical hackers assumes utmost importance, guaranteeing that only qualified professionals are entrusted with this crucial responsibility. Executing legal agreements, including non-disclosure agreements (NDAs) and liability waivers, serves to safeguard the interests of both parties. The Committee further suggest that the ethical hackers should diligently conduct penetration testing, painstakingly uncovering vulnerabilities and delivering a comprehensive report encompassing potential impact and recommended mitigation strategies. The Committee feel that instituting an enduring collaboration with ethical hackers facilitates periodic security assessments, ensuring a continuous and proactive approach towards countering emergent cyber threats.

To enhance the overall security posture of the institutions, safeguarding them against evolving cyber threats and potential breaches, the Committee recommend that the CPA require mandatory appointment of specified Cyber Security Officers within ecosystem participants, akin to chief risk officers. These cyber security officers will play a crucial role in mitigating cyber risks and safeguarding critical financial systems and customer data. The Committee emphasize the importance of these officers possessing strong technical expertise and extensive knowledge of cyber security threats. They should be capable of developing and implementing effective risk mitigation strategies to protect against cyber threats. The Committee further suggest that they must be responsible for formulating robust cyber security policies, conducting regular risk assessments, and fostering a culture of cyber security awareness within their organizations. Furthermore, they should ensure compliance with relevant regulations and industry standards while actively collaborating with internal stakeholders, regulatory bodies, and law enforcement agencies to enhance the resilience of financial institutions against cyber threats.

The Committee note that there are increasing instances of illegal Loan Apps offering loans/micro credits, especially to people from low-income groups at

exorbitantly high interest rates, and predatory recovery practices. The Committee also note that in February 2023, MeitY issued ban on some of the DLAs as part of a whitelisting exercise The Committee are of the view that while a favourable policy and regulatory infrastructure for digital lending services is in the pipeline, it is imperative to simultaneously look into and shape a framework for consumer-focused platforms to ensure consumer protection. The Committee, therefore, recommend establishment of a whitelisting framework by the CPA for Digital Lending Agencies (DLAs) and other "financial intermediaries" as a measure to combat illegal practices and promote a standardized code of conduct in the digital lending sector.

This framework would serve as a blueprint, outlining specific criteria that DLAs must meet to be recognized as legitimate entities. The Committee are of the view that by implementing a whitelisting framework, DLAs would undergo a thorough evaluation process to ensure compliance with regulations, transparency in operations, and adherence to ethical practices. This would help weed out fraudulent or unscrupulous DLAs from the market, protecting borrowers from predatory lending practices and other illegal activities. The standardized code of conduct within the whitelisting framework would establish clear guidelines and best practices for DLAs to follow. This includes fair and transparent lending practices, responsible data handling, appropriate disclosure of terms and conditions, and adherence to applicable laws and regulations.

The Committee would like to highlight that the expanding digital landscape, along with the presence of search engines and Big Tech companies, has increased the vulnerability of the digital ecosystem to cyber crime. The Committee feel that this susceptibility to cyber threats necessitates a clear delineation of responsibilities for search engines and global tech companies. As stated previously, the Committee strongly recommend that there should be a mandate that app stores, such as Apple's App Store or Google Play Store, adhere to specific guidelines and standards. This can include requirements for detailed app metadata, verification of developer identities, and the provision of traceability information, such as app ownership and origin. This can effectively enable the tracing of fraudulent apps' origins and prevent cybercriminals from engaging in repeated offenses. Thus, in the interest of safeguarding users and maintaining the integrity of the digital ecosystem, the Committee recommend that Tech companies should:

(i) Bear the responsibility of regularly updating and patching their operating systems (OS) to address vulnerabilities and incorporate robust security features.

(ii) They should also enforce a stringent vetting process for application approvals within their app stores, encompassing thorough malware detection and compliance with privacy and data security regulations.

Additionally, these companies should actively promote user education and awareness by providing guidance on safe practices and emphasizing the security features and controls available in their products.

To enhance the prevention and detection of fraud in the banking sector, the Committee strongly recommend the establishment of a Central Negative Registry. The CPA should maintain this Negative Registry. This registry should consolidate information on fraudsters' accounts and the official documents they have utilized. The Committee strongly believe that by making the registry accessible to all ecosystem participants, it would empower them to proactively deter and prevent the opening of accounts associated with fraudulent activities. The Committee acknowledge that the Reserve Bank of India (RBI) already maintains a comprehensive database of fraud and attempted fraud cases. To augment this database, the Committee suggest incorporating data from the Ministry of Home Affairs (Cyber Police), which contains end-to-end information on complaints. The Committee are of the view by consolidating these resources, the Central Negative Registry would serve as a powerful tool in combating fraud and protecting the integrity of the financial ecosystem.

The Committee note that technology advancement plays a crucial role in creating a resilient cyber landscape. To effectively prevent cybercrime, it is imperative for the CPA to prioritize the design of systems and technologies that simplify security and privacy decisions for users during transaction processing, minimizing their cognitive burden. The Committee are of the view that proactively addressing the security implications of quantum computing is essential. The Committee feel Investments in quantum cryptography, updating encryption standards, planning for quantum-resistant infrastructures, enhancing certificate and key management practices, and fostering collaboration among organizations can play a vital role in securing digital landscape.

The Committee note from the reply of MeitY that AI and chatbots are being used for strengthening cyber security. However, the Committee believe that the CPA should thoroughly assess potential pitfalls and negative impacts associated

with their implementation in the cyber security domain. The Committee, therefore, urge the Government to consistently evaluate the impact of AI tools along with periodic assessments to monitor the effectiveness of potential drawbacks of AI tools. Accountability standards should be set in this regard for all concerned entities.

3. <u>Consumer Grievance Redressal and Compensation Mechanisms</u>

The Committee note that the current compensatory mechanism for victims of cybercrime in the financial sector has limited scope and coverage. The process of filing a compensation claim is complex and time-consuming, placing the burden of proof on the victims to establish the connection between the cybercrime incident and the resulting financial loss, which is particularly challenging due to the traceability issues associated with cyber crimes. As there is a fiduciary relationship between financial institutions and their customers, the Committee emphasize that financial institutions must play a supportive role.

The Committee strongly believe there should be an automatic compensation system as devised by RBI and it should be the financial institution's sole responsibility to immediately compensate the hapless customer, pending further investigation and final traceability of funds. This proactive approach aligns with the principle of safeguarding customer interests and ensuring rapid resolution in cases of cybercrime in the financial sector. This would go a long way in demonstrating a steadfast commitment to consumer protection, which in turn strengthens their confidence in the financial system. Furthermore, this will propel financial institutions to bolster their security measures and adopt robust fraud prevention strategies. The Committee strongly believe that this will ensure that customers are shielded from the constantly evolving cyber threats and are provided with the necessary safeguards for their financial well-being.

The Committee have observed a serious anomaly in the financial transaction system, wherein customers are not necessarily receiving SMS notifications when amounts are credited to or debited from their accounts. This lack of information leaves room for potential crimes and fraudulent activities to go unnoticed. To address this critical issue, it is strongly recommended that financial institutions and service providers establish and implement robust SMS notification systems. These systems should promptly send SMS notifications to

customers whenever funds are credited or debited in their accounts. The Committee are of the view that by ensuring the timely and transparent dissemination of financial activity information through SMS, customers can stay informed and take necessary actions to protect themselves against fraudulent transactions. The Committee would also suggest that the financial institution should not debit any amount from the customer account without confirmation from the customer by way of an OTP or SMS or any other secure method. Considering the rising incidence of financial frauds, it is imperative that such fool-proof measures are taken to fully protect the customer from frauds (including UPI related) catching them unawares. Such firewalls are badly needed at this juncture when the fraudsters adopt new methods and try to stay a step ahead of the available safeguards.

The Committee note that although several consumer awareness initiatives and campaigns, such as "Stay Safe Online" by MeitY, "Cyber JagrukDiwas" by MHA, and "DigiSaathi," among others, have been implemented, there is still a notable lack of awareness among the general public. The Committee further observe that nascent customer awareness is not translating into widespread behavior change. The Committee, therefore, believe that there should be strong emphasis on comprehensive financial education programs that provide individuals with the necessary knowledge and skill to make informed decisions. Additionally, targeted communications strategies tailored to specific demographic groups should be developed to ensure relevance and effectiveness. Simplifying financial processes, leveraging technology for widespread dissemination of information, and introducing gamification and incentives can also encourage positive behavior change.

Additionally, the Committee recommend leveraging partnerships with private sector organizations, including banks, telecom operators, and e-commerce platforms, to integrate cyber security awareness messages into their customer communications. The Committee feel this would ensure that consumers receive consistent and timely information about online safety and best practices. Such communications should be mandatorily included with any consumer messages, such as monthly bank statements.

The Committee further recommend to regularly assess the effectiveness of the consumer campaign through comprehensive audits and evaluations. These assessments should gauge the level of awareness and understanding among the target audience, measure changes in behavior and online habits, and identify any

gaps or areas for improvement. The findings from these evaluations should be used to refine the campaign strategy and ensure its continued effectiveness.

The Committee understand the importance of an effective ombudsperson mechanism for resolving customer grievances. To further enhance its effectiveness, the Committee recommend that all financial institutions and service providers, regardless of the initial point of contact, should have a clear and standardized process to direct customers to the ombudsperson for grievance resolution. The Committee are of the view that there should be mechanism ensuring that customers are not turned away or redirected multiple times, but rather are consistently guided towards the appropriate avenue for resolution. The Committee, thus, recommend streamlining the process and promoting the ombudsperson as the central point for addressing customer complaints, to provide a more efficient and accessible system for customers to seek redressal. The redressal process should be completed within a stipulated time frame.

4. <u>Strengthening Enforcement Capabilities</u>

The Committee understand the importance of the enforcement system in addressing cyber fraud and stresses the importance of local police to take effective action against cybercrimes. It has come to the Committee's attention that certain geographic areas have persistently experienced high levels of cybercriminal activities, indicating a lack of proactive measures by local law enforcement agencies (LEAs). The Committee, therefore, strongly recommend immediate action to address the persistently high levels of cybercriminal activities in certain hotspots. The Committee have been informed about the inadequate enforcement and the bailable nature of most offenses under the IT Act 2000, which has enabled individuals and gangs to persist in their fraudulent activities across the country. This situation has resulted in repeated offenses and a lack of deterrence. The Committee feel to effectively combat cybercrime, two crucial elements should be considered: severity and certainty of punishment. To tackle this issue effectively, the Committee suggest implementing stricter penal provisions, imposing stricter bail conditions, and considering provisions for local surety.

The Committee note a significant variation in the number of cyber crime related FIRs filed across the country, with the national average being approximately 1.7 percent. This indicates a lack of awareness among users

regarding cyber attacks and the importance of reporting such incidents. The Committee further note that one of the key challenges identified is the integration of the 1930 helpline with the main police control rooms, as many places still lack this integration. The Committee recommend the following steps to address these issues:

(i) Awareness Campaigns: Launch comprehensive awareness campaigns to educate users about cyber attacks, their impact, and the importance of reporting such incidents to law enforcement agencies.

(ii) Strengthen Reporting Mechanisms: Establish a seamless and integrated system for reporting cybercrimes, ensuring that the 1930 helpline is centrally monitored and managed 24/7 in a dedicated control room.

(iii) Collaboration with financial institutions: Work closely with ecosystem participants to emphasize the significance of the 1930 helpline and encourage them to prioritize reporting cybercrimes to the designated helpline.

(iv) Capacity Building: Provide training and capacity building programs for law enforcement agencies and personnel involved in handling cybercrime cases, equipping them with the necessary skills and knowledge to effectively investigate and combat cybercrimes.

(v) Enhanced Data Analysis: Regularly analyse and assess data related to cybercrimes to identify emerging trends, hotspots, and modus operandi. This will enable law enforcement agencies to better allocate resources and implement targeted preventive measures.

(vi) Time-bound Redressal/Resolution: The designated cyber crime cell in various states should be mandated to file the case within a stipulated time frame. There should be a structured coordination mechanism between the cyber cell and the financial institution agency dealing with the customer.

(vii) The Committee recommend the establishment of a Single Point of Contact (SPOC) system within each district police department. This system may streamline the reporting process and facilitate efficient handling of cyber fraud cases. By designating a specific contact person dedicated to addressing cybercrime-related matters, affected individuals and organizations can easily report incidents and receive the necessary assistance and support.

In addition, the Committee are surprised to note that there is no self-regulating organisation/associations specifically dedicated to addressing cyber

security issues within the digital financial ecosystem. The Committee are of the view that SROs can play a vital role in setting sector-specific standards and collaborating closely with LEAs to proactively address cyber security challenges. The Committee feel by establishing SROs, there will be a unified and centralized mechanism for information exchange and streamlined investigations between law enforcement agencies, financial institutions, banks, and fintech companies. The Committee, therefore, strongly recommend the creation of SROs to promote best industry practices and ensure the effective implementation of cyber security frameworks. facilitate quicker response times, enhance coordination, and foster a more effective cyber security ecosystem.

5. Global Coordination and Best Practices Development

The Committee feel coordination and collaboration with other leading countries is imperative considering the increasing prevalence of cyber attacks worldwide. The Committee note India's ranking in the top 10 of the International Telecommunication Union's Global Security Index which has reflected progress, but continuous efforts are needed to streamline and upgrade our systems to remain alert, dynamic, and resilient. The Committee is of the view that by adopting practices like the European Commercial Bank's cyber risk profiling and intelligence-led testing frameworks among others, India can further strengthen its cyber security defences.

Countries worldwide have recognized the need to establish dedicated laws and regulations to address cyber security issues. For example, the United States implemented the Cyber security Information Sharing Act (CISA) in 2015, enabling private entities to proactively counter cyber threats, share vital information for vulnerability identification, and mitigate potential harm. CISA offers statutory protections and incentives, such as liability safeguards and non-waiver of privileges, to encourage entities to report cyber security incidents. In contrast, India's National Cyber Security Policy takes an incentive-based approach without specific incentives.

Additionally, the European cyber security skills framework focuses on building a competent workforce in this domain. Furthermore, Singapore has launched the SG Cyber Safe program, which assists organizations in bolstering their cyber security measures. This program provides valuable resources like toolkits for enhanced understanding of cyber security issues, facilitates the

implementation of quality measures, offers incident response simulations, and grants a cyber security trust mark to recognize enterprises with effective security measures. The Committee further believe that promoting supervisory cooperation and knowledge exchange with global regulators will facilitate a collective response to the exponentially growing cyber threats. The Committee, therefore, strongly urge the Government to adopt and go beyond global best practices – in short to develop "next practices" based on India's specific needs and requirements.

NEW DELHI;
20 July, 2023
29 Ashadha, 1945 (Saka)

SHRI JAYANT SINHA,
Chairperson,
Standing Committee on Finance

Minutes of the Ninth sitting of the Standing Committee on Finance (2022-23) The Committee sat on Monday, the 13th February, 2023 from 1500hrs. to 1745 hrs. in Main Committee Room, Parliament House Annexe, New Delhi.

PRESENT

Shri Jayant Sinha – Chairperson

LOK SABHA

2. Shri S.S. Ahluwalia
3. Shri Subhash Chandra Baheria
4. Dr. Subhash Ramrao Bhamre
5. Smt. Sunita Duggal
6. Shri Sudheer Gupta
7. Shri Manoj Kishorbhai Kotak
8. Shri Pinaki Misra
9. Shri Hemant Shriram Patil
10. Shri Gopal Chinayya Shetty
11. Shri Parvesh Sahib Singh
12. Dr. (Prof.) Kirit Premjibhai Solanki
13. Shri Manish Tewari
14. Shri Rajesh Verma

RAJYA SABHA

15. Dr. Radha Mohan Das Agarwal
16. Shri Raghav Chadha
17. Shri P. Chidambaram
18. Shri Sushil Kumar Modi
19. Dr. Amar Patnaik
20. Dr. C.M. Ramesh
21. Shri G.V.L Narasimha Rao

SECRETARIAT

1.	Shri Siddharth Mahajan	-	Joint Secretary
2.	Shri Ramkumar Suryanarayanan	-	Director
3.	Shri Kulmohan Singh Arora	-	Additional Director

WITNESSES

Ministry of Finance (Department of Financial Services)

1. Shri Vivek Joshi, Secretary
2. Shri Saurabh Mishra, Joint Secretary
3. Shri Srinivas Rao Sureddit, DMD, State Bank of India
4. Shri Murli Nambiar, CISO, State Bank of India

Ministry of Finance (Department of Revenue)

1. Shri Vivek Aggarwal, Additional Secretary

Ministry of Home Affairs

1. Ms. Sivagami Sundari Nanda, Special Secretary
2. Shri Chandraker Bharti, Additional Secretary (CIS)
3. Shri H.G.S Dhaliwal, Special Commissioner, Delhi Police
4. Shri Ashish Kumar, Joint Secretary (CIS)
5. Rajesh Kumar, CEO(I4C)
6. Shri Vivek Gogia, Director, National Crime Records Bureau
7. Shri Vineet Vinayak, Joint Director, Central Bureau of Investigation

Reserve Bank of India

1. Shri Rohit Jain, Executive Director
2. Shri P Vasudevan, Chief General Manager, Department of Payment and Settlement Systems
3. Shri T.K. Rajan, Chief General Manager, Department of Supervision (Cyber Security and IT Examination Group.

2. At the outset, the Chairperson welcomed the Members and the witnesses to the sitting of the Committee. After the customary introduction of the Witnesses the Chairperson initiated the discussion on the subject 'Cyber security and rising incidence of cyber/white collar crimes'. The major issues discussed include rising incidence of cybercrime; regulatory gaps in overall regulatory architecture; mechanisms within the Government to deal with inter-ministerial issues; education and awareness of consumers on an ongoing basis; quantitative data indicating the extent of cyber crimes as a threat to the financial system; increasing volume of cyber complaints; wide gap between number of complaints and number of FIRs registered; incident response; cybercrime hotspots;

activities of malicious loan Apps; e-cyber lab AI chatbot; reporting of suspicious transactions to Financial Intelligence Unit (FIU); need for adequate staff strength; use of crypto for money laundering and terror financing; mule accounts; bifurcation of frauds affecting common man and frauds related to online betting; status of connectivity of all police station via Crime and Criminal Tracking Network & Systems(CCTNS); idea of nodal agency to deal with cybercrime, simplifying co-ordination between various agencies; percentage of overall IT budget spent on investment in building a cyber security architecture and Software and sypwares to prevent incidence of money laundering as well as cyber security threats.

3. The witnesses responded to the queries raised by the Members and the Chairperson then directed the representatives to furnish written replies to the points raised by the Members, which could not be readily replied by them during the discussion to the Secretariat.

The witnesses then withdrew.

The Committee then adjourned.

A verbatim record of the proceedings has been kept.

Minutes of the Seventeenth sitting of the Standing Committee on Finance (2022-23) The Committee sat on Wednesday, the 3rd May, 2023 from 1500hrs. to 1700 hrs. in Main Committee Room, Parliament House Annexe, New Delhi.

PRESENT

Shri Jayant Sinha – Chairperson

LOK SABHA

2. Shri S.S. Ahluwalia
3. Shri Pinaki Misra
4. Shri Hemant Shriram Patil
5. Shri Nama Nageswara Rao
6. Shri Gopal Chinayya Shetty
7. Shri Manish Tewari

RAJYA SABHA

8. Dr. Radha Mohan Das Agarwal
9. Shri P. Chidambaram
10. Shri Ryaga Krishnaiah
11. Shri Sushil Kumar Modi
12. Dr. Amar Patnaik
13. Dr. C.M. Ramesh

SECRETARIAT

1. Shri Ramkumar Suryanarayanan - Director
2. Shri Kulmohan Singh Arora - Additional Director

WITNESSES

Reserve Bank of India

1. Shri. P Vasudevan, Chief General Manager, Department of Payment and Settlement Systems
2. Shri. T K Rajan, Chief General Manager, Department of Supervision
3. Shri. A G Giridharan, General Manager, Department of Supervision

Indian Banks' Association (IBA)

1. Shri Atul Kumar Goel, Chairman IBA and MD&CEO Punjab National Bank
2. Shri Sunil Mehta, Chief Executive, Indian Banks' Association
3. Shri S Srinivas Rao, DMD, State Bank of India
4. Shri Murlidhar Nambiar, Chief Information Security Officer, State Bank of India
5. Ms. Vijayalakshmi Muddu, GM, State Bank of India
6. Shri K Srinivasa Rao, Senior Advisor, Indian Banks' Association
7. Shri. Rajneesh Khanna - Head - FCPG Investigations, ICICI Bank
8. Shri. Samir Dani - Head – Information Security Risk Management, ICICI Bank

National Payments Corporation of India (NPCI)

1. Shri Viswanath Krishnamurthy, Chief Risk Officer
2. Shri Hardik Dixit, In-charge FRM Operns. Risk Management

Computer Emergency Response Team (CERT-In)

1. Shri Sanjay Behl, DG
2. Shir S. S. Sharma, Scientist 'G'

2. At the outset, the Chairperson welcomed the Members and the witnesses to the sitting of the Committee. After the customary introduction of the Witnesses the Chairperson initiated the discussion on the subject 'Cyber security and rising incidence of cyber/white collar crimes'. The major issues discussed include challenges associated with cybercrime; safeguarding of financial systems from hackers, thieves and other fraudulent activities; gaps in regulatory architecture; different agencies involved in dealing with cybercrime; education and protection of consumers; relative position of India in comparison with other countries and specific quantitative indicators to judge the same; regulation of entities who provide payment services; real time payment solutions; issue

of multi state co-operative societies; need for national level architecture for cyber security; systemic risk management framework for entire payment and settlement system; insider threat activity and improving intrusion detection; status of complaints received by RBI and their final outcome; strengthening of cyber security laws and regulations; innovative new methods to enhance training and awareness; cyber insurance; promotion of sandboxes for improving cyber security; defence mechanism against various sources of cybercrime; efficient enforcement of cyber laws; awareness to small vendors using UPI to make them aware of their rights and steps to follow in case of a cyber fraud; fact check mechanism to authenticate various advertisements and monetary news; ethical hackers; issue of regulation of loan apps and improved incident response mechanism and speed and efficiency of investigation.

3. The witnesses responded to the queries raised by the Members and the Chairperson then directed the representatives to furnish written replies to the points raised by the Members, which could not be readily replied by them during the discussion to the Secretariat.

The witnesses then withdrew.

The Committee then adjourned.

A verbatim record of the proceedings has been kept.

Minutes of the Eighteenth sitting of the Standing Committee on Finance (2022-23) The Committee sat on Thursday, the 1st June, 2023 from 1500hrs. to 1700 hrs. in Main Committee Room, Parliament House Annexe, New Delhi.

PRESENT

Shri Jayant Sinha – Chairperson

LOK SABHA

2. Shri Subhash Chandra Baheria
3. Smt. Sunita Duggal
4. Shri Pinaki Mishra
5. Shri Hemant Shriram Patil
6. Shri Ravi Shankar Prasad
7. Prof. Sougata Ray
8. Shri Gopal Chinayya Shetty

RAJYA SABHA

9. Dr. Radha Mohan Das Agarwal
10. Shri Sushil Kumar Modi
11. Dr. Amar Patnaik
12. Shri Pramod Tiwari

SECRETARIAT

1.	Shri Siddharth Mahajan	-	Joint Secretary
2.	Shri Ramkumar Suryanarayanan	-	Director
3.	Shri Puneet Bhatia	-	Deputy Secretary

WITNESSES

National Association of Software and Service Companies (NASSCOM)

1. Shri Vinayak Godse, CEO, Data Security Council of India (DSCI)
2. Shri Venkatesh Murthy, Senior Director, Data Security Council of India (DSCI)

Chase India

1. Shri Manash K Neog, Managing Director, Chase APAC
2. Shri Kaushal Mahan, Vice President -Public Policy, Chase India
3. Ms. Aishwarya Sharma, Associate, Chase India

Pine Labs

1. Shri Amrish Rau, CEO
2. Ms. Jagriti Bhattacharyya, General Counsel

Razorpay Software Private Limited

1. Shri Harshil Mathur, CEO
2. Ms. Saranya Gopinath, Director, Government Affairs and Public Policy

QNu Labs

1. Shri Sunil Gupta, CEO
2. Shri Gautam Kumar, AVP

PhonePe

1. Shri Rahul Chari, CTO
2. Shri Anuj Bhansali, Head of Trust & Safety

CRED

1. Shri Miten Sampat, Head, Corporate & Business Strategy
2. Shri Hardeep Singh, Head, Legal & Policy

2. At the outset, the Chairperson welcomed the Members and the witnesses to the sitting of the Committee. After the customary introduction of the Witnesses the Chairperson initiated the discussion on the subject 'Cyber security and rising incidence of cyber/white collar crimes'. The major issues discussed include rising incidence of cybercrime; types of cybercrimes/white-collars crimes in the financial sector such as

phishing, data theft, biometric fraud, stalking and so on; challenges of cognitive burden on users due to over reliance on OTPs; reporting of cyber crimes at police stations; need for timely access to information and support systems for cybercrime victim; collaboration between the telecom and banking sector to tackle issues like duplicate SIM cards; policy intervention to encourage security investments and enhance fraud management practices; systematic digital education and training for law enforcement agencies on payment fraud prevention and consumer awareness; efficient cybercrime reporting mechanism; decentralized nature of investigations; social engineering frauds; collaboration between private entities, banks and law enforcement agencies; standardization of practices across states to simplify information; technological advancements combating cybercrimes and frauds in digital payment; establishment of self-regulatory organization (SRO) in the digital lending sector; implementation of advanced encryption technology to counter quantum computers threat in data system; building of next generation encryption layer; common people's concerns with digital expansion in financial sector; regulating digital entrepreneurship effectively; delays in cybercrime investigation caused by multiple agencies involved; single investigation agency for cyber crimes, global best practices for securing digital payments, SARTHI portal initiatives, frauds targeting digitally illiterate low-income individuals; specific cyber crime police station; RBI's Har payment digital campaign; idea of single person ombudsman for cyber crimes; cyber safe initiative; idea of nodal agency to deal with cybercrime and constitution of formal or informal self regulating association for cyber crimes.

3. The witnesses responded to the queries raised by the Members and the Chairperson then directed the representatives to furnish written replies to the points raised by the Members, which could not be readily replied by them during the discussion to the Secretariat. Besides, Chairperson also directed the witnesses to provide further points and additional perspectives / recommendations on the subject.

The witnesses then withdrew.

The Committee then adjourned.

A verbatim record of the proceedings has been kept.

* * *

Minutes of the Nineteenth sitting of the Standing Committee on Finance (2022-23) The Committee sat on Thursday, the 15th June, 2023 from 1400hrs. to 1600 hrs. in Committee Room '2', Parliament House Annexe Extension Block A, New Delhi.

PRESENT

Shri Jayant Sinha – Chairperson

LOK SABHA

2. Shri S.S. Ahluwalia
3. Shri Subhash Chandra Baheria
4. Shri Gaurav Gogoi
5. Shri Manoj Kishorbhai Kotak
6. Shri Nama Nageswara Rao
7. Prof. Sougata Ray
8. Shri Gopal Chinayya Shetty
9. Shri Manish Tewari
10. Shri Rajesh Verma

RAJYA SABHA

11. Dr. Radha Mohan Das Agarwal
12. Shri Ryaga Krishnaiah
13. Shri Sushil Kumar Modi
14. Dr. Amar Patnaik
15. Shri G.V.L Narasimha Rao
16. Shri Pramod Tiwari

SECRETARIAT

1. Shri Siddharth Mahajan - Joint Secretary
2. Shri Ramkumar Suryanarayanan - Director
3. Shri Puneet Bhatia - Deputy Secretary

WITNESSES

Ministry of Finance (Department of Financial Services)

1. Shri Vivek Joshi, Secretary
2. Shri M.P Tangirala, Additional Secretary
3. Shri Abhijit Phukon, Economic Adviser
4. Shri T.K. Rajan, CGM, RBI
5. Shri Sudhanshu Prasad, CGM, RBI
6. Shri Lokesh Garg, DDG, National Critical Information Infrastructure Protection Centre (NCIIPC)
7. Shri Ashwini Kumar Tewari, MD, State Bank of India
8. Shri Murli Nambiar, CISO, State Bank of India

Ministry of Home Affairs

1. Ms. Sivagami Sundari Nanda, Special Secretary
2. Shri Chandraker Bharti, Additional Secretary (CIS)
3. Shri Ashish Kumar, Joint Secretary (CIS)
4. Shri Rajesh Kumar, CEO (Indian Cybercrime Coordination Centre)
5. Shri Vivek Gogia, Director, National Crime Records Bureau

MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY (MeitY)

1. Shri Alkesh Kumar Sharma, Secretary
2. Shri Amit Agrawal, Additional Secretary
3. Shri Kuntal Sensarma, Economic Adviser
4. Dr Sanjay Bahl, DG, CERT-In
5. Smt Savita Utreja, Scientist ‘G’ and Group Coordinator
6. Dr Sandip Chatterjee, Scientist ‘G’ and Group Coordinator
7. Ms. Tulika Pandey, Scientist 'G' and Group Coordinator
8. Shri S. S. Sarma, Director and Scientist ‘G’, CERT-In

National Payments Corporation of India (NPCI)

1. Shri Viswanath Krishnamurthy, Chief Risk Officer
2. Shri Hardik Dixit, In-charge FRM Operns. Risk Management

2. At the outset, the Chairperson welcomed the Members and the witnesses to the sitting of the Committee. After the customary introduction of the Witnesses the Chairperson initiated the discussion on the subject ‘Cyber security and rising incidence

of cyber/white collar crimes'. The major issues discussed include implementation of a strict two-factor authentication regime; surge in social engineering frauds; malware and cyber-attacks by state and non-state actors originating from foreign entities; vulnerabilities and weaknesses in the current cyber security framework; impact of Artificial Intelligence & chatbots on Cyber Security; Insufficient awareness of cyber hygiene practices; Chinese investment and loan apps, Dubai based betting apps fraudulent dating aps, gaming apps, investment apps and other vectors of cybercrime; lack of stringent KYC guidelines for domains and hosts beyond Indian borders; mechanism for filtering content in social media.; end-to-end encrypted chat applications; TRAI guidelines for AI-based fraud phishing links filtering; RBI advisory on mule accounts; Citizen Financial Cyber Fraud Reporting and Management System; Real-time SIM blocking mechanism; role of CERT-In in protecting financial institutions; financial Institutions with appropriate protection system; risk mitigation framework; AI enabled fraud risk monitoring solutions; customer limited liability framework, ransomware attack and data infiltration; Enterprise Fraud Risk Management Solutions; need for a study analyzing fraud classification and auditing safety/security in critical digital infrastructure; ethical hackers engagement policy; global best practices for controlling cyber crime; cyber crime vulnerability assessment; cyber crime incident response and forensic; global comparative analysis of fraud-to-sales ratios; Inter agency cooperation; compensatory policy for victims of cyber crime and current status of third-party service provider audits.

3. The witnesses responded to the queries raised by the Members and the Chairperson then directed the representatives to furnish written replies to the points raised by the Members, which could not be readily replied by them during the discussion to the Secretariat.

The witnesses then withdrew.

The Committee then adjourned.

A verbatim record of the proceedings has been kept.

Minutes of the Twentieth sitting of the Standing Committee on Finance (2022-23) The Committee sat on Tuesday, the 04th July, 2023 from 1400hrs. to 1640 hrs. in Committee Room '2', Parliament House Annexe Extension Block A, New Delhi.

PRESENT

Shri Jayant Sinha – Chairperson

LOK SABHA

2. Shri S.S. Ahluwalia
3. Shri Subhash Chandra Baheria
4. Dr. Subhash Ramrao Bhamre
5. Smt. Sunita Duggal
6. Shri Gaurav Gogoi
7. Shri Manoj Kishorbhai Kotak
8. Shri Pinaki Misra
9. Shri Ravi Shankar Prasad
10. Shri Nama Nageswara Rao
11. Shri Gopal Chinayya Shetty
12. Dr. (Prof.) Kirit Premjibhai Solanki
13. Shri Manish Tewari
14. Shri Balashowry Vallabhbhaneni
15. Shri Rajesh Verma

RAJYA SABHA

16. Dr. Radha Mohan Das Agarwal
17. Shri Raghav Chadha
18. Shri P. Chidambaram
19. Shri Ryaga Krishnaiah
20. Shri Sushil Kumar Modi
21. Dr. Amar Patnaik
22. Shri Pramod Tiwari

SECRETARIAT

1. Shri Siddharth Mahajan - Joint Secretary

PART I

1400 hrs to 1500 hrs

Punjab National Bank

1. Shri Atul Kumar Goel, MD & CEO
2. Shri Kalyan Kumar, Executive Director
3. Shri Ashwini Pandey, Chief Information Security Officer (CISO)

Bank of India

1. Shri Rajneesh Karnatak, MD & CEO
2. Shri Kuldeep Pal, Chief Information Security Officer

Yes Bank

1. Shri Prashant Kumar, MD & CEO
2. Shri Sumit Gupta, Chief Risk Officer
3. Shri Sandeep Mehra, Chief Vigilance Officer

Computer Emergency Response Team (CERT-In)

1. Dr Sanjay Bahl, DG, CERT-In
2. Shri S. S. Sarma, Director, Scientist 'G', CERT-In
3. Ms. Tulika Pandey, Scientist 'G' and Group Coordinator

2. At the outset, the Chairperson welcomed the Members and the witnesses to the sitting of the Committee. After the customary introduction of the Witnesses the Chairperson initiated the discussion on the subject 'Cyber security and rising incidence of cyber/white collar crimes'. The major issues discussed include comprehensive policy framework for cyber crime; centralized authority to deal with cyber crime; enforcement capability to deal with cyber crime; vulnerability audit of banking institutions; consumer awareness and grievance redressal mechanism; compensatory mechanism for victims of cyber security; impact of Artificial Intelligence and chat bots on cyber security; volume of digital transactions; cyber security instruments and solutions; Cyber Crime Monitoring Cells; Enterprise Fraud Reporting Management System (EFRMS); vulnerable financial institutions; cyber swachhta Kendra; engagement of ethical hackers; budget allocated and the amount spent by the banks for cyber security; steps taken by banks to create awareness among customers and staff and insurance policies to cover unauthorized banking transaction.

3. The witnesses responded to the queries raised by the Members and the Chairperson then directed the representatives to furnish written replies to the points raised by the Members, which could not be readily replied by them during the discussion to the Secretariat.

The witnesses then withdrew.

PART II

1500 hrs onwards

Apple India

1. Shri Virat Bhatia – Managing Director, Strategy & Policy - India
2. Shri Kulin Sanghvi - Head Public Policy - India
3. Shri Priyesh Poovanna - Country Counsel – India
4. Shri Prateek Hiremath – Senior Counsel - India

Flipkart

1. Shri Jeyandran Venugopal, Senior Vice President & Chief Product and Technology Officer
2. Dr Tafheem Siddiqui, Senior Director - Flipkart Group

One97 Communications Ltd. (Paytm)

1. Dr. Srinivas Yanamandra, Group Head - Regulatory Affairs & Policy
2. Shri Arun Shankar Chandrasekaran, Head - Fraud & Operations Risk
3. Shri Akshay Jain, Associate Vice President

3. After the customary introduction of the Witnesses the Chairperson initiated the discussion on the subject 'Cyber security and rising incidence of cyber/white collar crimes'. The major issues discussed include internal cyber security audits; adjudication mechanism for cyber crime; need of uniformity in the regulatory mechanism; inadequate auditing in cooperative banks; need for establishment of cyber courts; repeat offenders in cybercrime; global best practices in cyber security; Government investment in cyber security; coordination with state police; uniformity in technological standards in various banks; audit of entire bank system in terms of DDOS attacks; DAKSH Portal; Global Cyber Security Index; uniformity of standards and audits in Banks; SMS notification for credited or debited amounts in bank accounts, issue of targeted spyware attacks

identified in India; instances of data leaks resulted in cyber fraud incidents; National Security Policy Framework and lack of OTP system in Paytm transactions

The witnesses then withdrew.

The Committee then adjourned.

A verbatim record of the proceedings has been kept.

Minutes of the Twenty-first sitting of the Standing Committee on Finance (2022-23) The Committee sat on Thursday, the 20th July, 2023 from 1500hrs. to 1700 hrs. in Committee Room '2', Parliament House Annexe Extension Block A, New Delhi.

PRESENT

Shri Jayant Sinha – Chairperson

LOK SABHA

2. Shri S.S Ahluwalia
3. Shri Subhash Chandra Baheria
4. Dr. Subhash Ramrao Bhamre
5. Smt. Sunita Duggal
6. Shri Gaurav Gogoi
7. Shri Sudheer Gupta
8. Shri Manoj Kishorbhai Kotak
9. Shri Hemant Shriram Patil
10. Shri Nama Nageswara Rao
11. Shri Gopal Chinayya Shetty
12. Shri Parvesh Sahib Singh
13. Dr. (Prof.) Kirit Premjibhai Solanki
14. Shri Manish Tewari
15. Shri Balashowry Vallabbhaneni

RAJYA SABHA

16. Dr. Radha Mohan Das Agarwal
17. Shri Ryaga Krishnaiah
18. Shri Sushil Kumar Modi
19. Dr. Amar Patnaik
20. Shri G.V.L Narasimha Rao
21. Shri Pramod Tiwari

SECRETARIAT

1. Shri Siddharth Mahajan - Joint Secretary
2. Shri Ramkumar Suryanarayanan - Director
3. Shri Puneet Bhatia - Deputy Secretary

PART I

1500 hrs to 1600 hrs

WITNESSES

Google India

1. Shri Sanjay Gupta, Country Head and V.P
2. Shri Saikat Mitra, Vice President and Head of Trust and Safety
3. Ms. Gitanjli Duggal, Director and Head of Legal
4. Ms. Yolynd Lobo, Government Relations and Public Policy

2. At the outset, the Chairperson welcomed the Members and the witnesses to the sitting of the Committee. After the customary introduction of the Witnesses the Chairperson initiated the discussion on the subject 'Cyber security and rising incidence of cyber/white collar crimes'. The major issues discussed include increasing incidents of cyber threats, systemic lapses in cyber security policies; social engineering frauds; fraudulent digital lending apps; prevailing deficiencies in the system; challenges faced by big tech companies in cyber security ecosystem; number of fraudulent transactions detected; money spent on user awareness; risk mitigation and reduction mechanism and part of revenue spent on it by Big Tech companies; regulations in India in relation to other developed countries; verification policy for financial advertisements; built-in app benchmarks for detecting fraudulent transactions; mule accounts; weak e-kyc norms; policy and regulatory framework; better enforcement and quicker resolution of issues related to cyber security; reliable mechanisms ensuring OTP security; retention of financial data with tech companies; single unified blacklist of fraudulent apps; funds utilised by tech companies for consumer awareness; risk reduction strategy; malware and phishing incidents and global experiences with respect to cyber security and enhanced data maintenance and analysis.

3. The witnesses responded to the queries raised by the Members and the Chairperson then directed the representatives to furnish written replies to the points raised by the Members, which could not be readily replied by them during the discussion to the Secretariat.

(The witnesses then withdrew)

PART II

1600 hrs onwards

WITNESSES

Reserve Bank of India

1. Shri T K Rajan, Chief General Manager, Department of Supervision
2. Shri Sudhanshu Prasad, Chief General Manager, Department of Payment and Settlement System

Ministry of Electronics and Information Technology (MeitY)

1. Shri Alkesh Kumar Sharma, Secretary, MEITY
2. Shri Bhuvnesh Kumar, Additional Secretary, MEITY
3. Dr. Sanjay Bahl, DG, CERT-In
4. Smt. Savita Utreja, Scientist G & Group Coordinator (Cyber Security)
5. Dr. Sandip Chatterjee, Scientist G & Group Coordinator (Cyber Law Group)
6. Shri S.S. Sarma, Scientist G, CERT-In
7. Ms. Tulika Pandey, Scientist G & Group Coordinator

4. At the outset, the Chairperson welcomed the witnesses to the sitting of the Committee. After the customary introduction of the Witnesses the Chairperson initiated the discussion on the subject 'Cyber security and rising incidence of cyber/white collar crimes'. The major issues discussed include overall regulatory framework; better e-kyc verification; regular audit of entire financial system; security of OTP based digital banking; key improvements needed to enhance OTP security; changes in operating system to safeguard financial sector; enhancing monitoring mechanisms over apps; SMS forwarding apps; concept of passkeys in cyber security; regulatory gaps existing in cyber security; lack of central registry of bad actors; need for Centralized Regulatory Authority for cyber security; strong Grievance Redressal Mechanism; local law enforcement specially in cyber crime hotspot regions; Big Tech companies disregarding invaluable input from key regulators; compensation mechanism for victims of cyber crime; strengthening enforcement capabilities; weak e-kyc norms and whitelisting of apps; regulatory mechanism mandating app stores to share exhaustive data/information with regulators and app stores to be accountable for fraudulent apps hosted on their platforms.

5. The witnesses responded to the queries raised by the Members and the Chairperson then directed the representatives to furnish written replies to the points raised by the Members, which could not be readily replied by them during the discussion to the Secretariat.

(The witnesses then withdrew)

6. Thereafter, the Committee took up the following draft reports for consideration and adoption:

(i) Draft Report on the subject 'Cyber security and rising incidence of cyber/white collar crimes' of the Ministry of Finance (Department of Financial Services), Ministry of Electronics and Information Technology and Ministry of Home Affairs.

(ii) Draft Action Taken Report on the recommendations contained in the Fifty-Third Report on the subject 'Anti-Competitive Practices by Big-Tech Companies' of the Ministry of Corporate Affairs.

(iii) Draft Action Taken Report on the recommendations contained in the Fifty-Fourth Report on Demands for Grants (2023-24) of the Ministry of Finance (Departments of Economic Affairs, Expenditure, Financial Services, Investment & Public Asset Management and Public Enterprises).

(iv) Draft Action Taken Report on the recommendations contained in the Fifty-Fifth Report on Demands for Grants (2023-24) of the Ministry of Finance (Department of Revenue).

(v) Draft Action Taken Report on the recommendations contained in the Fifty-Sixth Report on Demands for Grants (2023-24) of the Ministry of Corporate Affairs.

(vi) Draft Action Taken Report on the recommendations contained in the Fifty-Seventh Report on Demands for Grants (2023-24) of the Ministry of Planning.

(vii) Draft Action Taken Report on the recommendations contained in the Fifty-Eighth Report on Demands for Grants (2023-24) of the Ministry of Statistics and Programme Implementation.

After some deliberations, the Committee adopted the above draft Reports and authorised the Chairperson to finalise them and present the Reports to the Parliament. The Chairperson also appreciated the Committee Secretariat for putting their sincere

efforts in drafting comprehensive reports within a short span of time. The Committee also decided to undertake a Study Tour during the third or fourth week of August, 2023.

The Committee then adjourned.

A verbatim record of the proceedings has been kept.