**06**

# STANDING COMMITTEE ON FINANCE

**(2024-25)**

**EIGHTEENTH LOK SABHA**

# MINISTRY OF FINANCE

## (DEPARTMENT OF FINANCIAL SERVICES)

## MINISTRY OF HOME AFFAIRS
## AND
## MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

***[Action taken by the Government on the Observations/Recommendations contained in Fifty-Ninth Report (17th Lok Sabha) on the subject 'Cyber Security and Rising Incidence of Cyber/White Collar Crimes']***

## SIXTH REPORT


**LOK SABHA SECRETARIAT**
**NEW DELHI**

***December, 2024/ Agrahayana, 1946 (Saka)***

# SIXTH REPORT

## STANDING COMMITTEE ON FINANCE
## (2024-25)

## (EIGHTEENTH LOK SABHA)

## MINISTRY OF FINANCE

## (DEPARTMENT OF FINANCIAL SERVICES)

## MINISTRY OF HOME AFFAIRS
## AND
## MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOG

***Presented to Lok Sabha on 06 December, 2024***

***Laid in Rajya Sabha on 06 December, 2024***


**LOK SABHA SECRETARIAT**
**NEW DELHI**

*December, 2024/ Agrahayana, 1946 (Saka)*

| CONTENT | | |
|---|---|---|
| **REPORT** | | |
| Composition of the Committee | | (iv) |
| Introduction | | (v) |
| | | **Page No.** |
| **Chapter - I** | Report | 01 |
| **Chapter – II** | Observations/Recommendations which have been accepted by the Government | 16 |
| **Chapter- III** | Observations/Recommendations which the Committee do not desire to pursue in view of the Government's replies | 52 |
| **Chapter- IV** | Observations/Recommendations in respect of which replies of the Government have not been accepted by the Committee | 53 |
| **Chapter- V** | Observations/Recommendations in respect of which final reply of the Government is still awaited | 94 |
| | **ANNEXURE** | |
| | Minutes of the Sitting of the Committee held on 04.12.2024 | 95 |
| | **APPENDIX** | |
| | Analysis of Action Taken by the Government on the Recommendations contained in the Fifty-Ninth Report (Seventeenth Lok Sabha) of the Standing Committee on Finance on 'Cyber Security and Rising Incidence of Cyber/White Collar Crimes' of the Ministry of Finance (Department of Financial Services), Ministry of Home Affairs and Ministry of Electronics and Information Technology. | 97 |

## COMPOSITION OF STANDING COMMITTEE ON FINANCE (2024-25)

### Shri Bhartruhari Mahtab - Chairperson

### MEMBERS

**LOK SABHA**

2. Shri Arun Bharti
3. Shri P. P. Chaudhary
4. Shri Lavu Sri Krishna Devarayalu
5. Shri Gaurav Gogoi
6. Shri K. Gopinath
7. Shri Suresh Kumar Kashyap
8. Shri Kishori Lal
9. Shri Harendra Singh Malik
10. Shri Chudasama Rajeshbhai Naranbhai
11. Thiru Arun Nehru
12. Shri N. K. Premachandran
13. Dr. C. M. Ramesh
14. Smt. Sandhya Ray
15. Prof. Sougata Ray
16. Shri P. V. Midhun Reddy
17. Dr. Jayanta Kumar Roy
18. Dr. K. Sudhakar
19. Shri Manish Tewari
20. Shri Balashowry Vallabhaneni
21. Shri Prabhakar Reddy Vemireddy

**RAJYA SABHA**

22. Shri P. Chidambaram
23. Shri Milind Murli Deora
24. Dr. Ashok Kumar Mittal
25. Shri Yerram Venkata Subba Reddy
26. Shri S. Selvaganabathy
27. Shri Sanjay Seth
28. Dr. Dinesh Sharma
29. Smt. Darshana Singh
30. Dr. M. Thambidurai
31. Shri Pramod Tiwari

### SECRETARIAT

| | | |
|---|---|---|
| 1. | Shri Gaurav Goyal | Joint Secretary |
| 2. | Shri Vinay Pradeep Barwa | Director |
| 3. | Shri Kuldeep Singh Rana | Deputy Secretary |
| 4. | Ms. Abhiruchi Srivastava | Assistant Executive Officer |

# INTRODUCTION

I, the Chairperson, of the Standing Committee on Finance, having been authorised by the Committee, present this Sixth Report (Eighteenth Lok Sabha) on action taken by Government on the Observations / Recommendations contained in the Fifty-Ninth Report of the Committee (Seventeenth Lok Sabha) on 'Cyber Security and Rising Incidence of Cyber/White Collar Crimes'.

2. The Fifty-Ninth Report was presented to Lok Sabha / laid on the table of Rajya Sabha on 27 July, 2023. The updated Action Taken Notes on the Observations/Recommendations were received from the Government *vide* their communication dated 18 October, 2024.

3. The Committee considered and adopted this Report at their sitting held on 4 December, 2024.

4. An analysis of the action taken by the Government on the Recommendations contained in the Fifty-Ninth Report of the Committee is given in the Appendix.

5. For facility of reference, the Observations/Recommendations of the Committee have been printed in bold in the body of the Report.

6. The Committee would also like to place on record their deep sense of appreciation for the invaluable assistance rendered to them by the officials of Lok Sabha Secretariat attached to the Committee.

**New Delhi;**
**4 December, 2024**
**13 Agrahayana, 1946 (Saka)**

**Bhartruhari Mahtab,**
**Chairperson**
**Standing Committee on Finance**

# REPORT

## CHAPTER I

This Report of the Standing Committee on Finance deals with the action taken by the Government on the Observations/Recommendations contained in their Fifty-Ninth Report on 'Cyber Security and Rising Incidence of Cyber/White Collar Crimes' pertaining to the Ministry of Finance (Department of Financial Services), Ministry of Home Affairs and Ministry of Electronics and Information Technology, which was presented to Lok Sabha and laid in Rajya Sabha on 27th July, 2023.

2. Updated Action taken notes (consolidated) have been received from Ministry of Finance (Department of Financial Services) on 18th October, 2024 in respect of all the 05 Observations/Recommendations contained in the Report. The replies have been analyzed and categorized as follows:

(i) Observations/Recommendations that have been accepted by the Government:

Recommendation No. 1, 4 and 5

(Total 03)
(Chapter- II)

(ii) Observations/Recommendations which the Committee do not desire to pursue in view of the Government's replies:

Recommendation No. NIL

(Total NIL)
(Chapter- III)

(iii) Observations/Recommendations in respect of which replies of Government have not been accepted by the Committee:

Recommendation No. 02 and 03.

(Total 02)
(Chapter -IV)

(iv) Observations/Recommendations in respect of which final replies by the Government are still awaited:

Recommendation No. NIL

(Total - NIL)
(Chapter- V)

3. The Committee desire that the replies to the observations / recommendations contained in Chapter-I of this Report may be furnished to them expeditiously.

4. The Committee will now deal with and comment upon the action taken by the Government on some of their observations / recommendations that require reiteration or merit comments.

**Recommendation [Serial No. 2 (i)]**

**(Paragraph No.1)**

5. The Committee had recommended as under:

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.

6. In their Action Taken Reply the Ministry of Finance (Department of Financial Services) have submitted as follows:-

*"Ministry of Home Affairs (MHA) has informed that there are various Ministries and agencies in the country for strengthening the Cyber security apparatus and securing the cyber space of the country.MHA is responsible for information security policy formulation and administers the Official Secrets Act. MHA currently performs coordination activities on regular basis related to identifying cyber security and cybercrime related issues.*

*National Cyber Security Coordinator (NCSC), Ministry of Electronics and Information Technology (MeitY), Indian Computer Emergency Response Team (CERT-In), National Critical Information Infrastructure Protection Centre (NCIIPC), I4C Department of Financial Services (DFS), Reserve Bank of India (RBI), etc., are the major stakeholders responsible for monitoring regulation compliance.*

*The cyber space is vast and warrants a differentiated approach based on the digital depth of an entity, its interconnectedness with the payment systems and the systemic risk each entity poses. RBI is of the view that intensity and scope of regulations would vary depending upon the nature of business of the entities under each of the regulators and there may be a need for a differentiated approach from the perspective of their systemic importance. Some of the cyber risks for the entities in financial sector may, however, be common and a mechanism for coordination and cooperation among the financial sector regulators is already put in place as part of Inter Regulatory forum under FSDC where RBI engages with other financial regulators for sharing of best practices in this regard.*

*In order to provide focussed attention on IT related matters, RBI had set up a Cyber Security and IT Risk (CSITE) Group within its Department of Supervision in 2015. Cyber Security framework was put in place by RBI for banks in June 2016 and appropriate regulatory and supervisory mechanism has been in place since then to take care of regulation and supervision of the REs from cyber security perspective. The banking sector entities have achieved reasonable level of cyber maturity now.*

*While progressive measures were being taken to enhance cyber security posture of the UCB sector, they have not been able to enhance their cyber preparedness commensurately with the growth in digital payments during covid period. Appropriate steps are being taken to address cyber risks for the UCB sector in a non-disruptive manner and with a risk-based approach.*

*In a similar manner, dedicated divisions have been set up in other financial sector regulators such as SEBI, IRDAI, and PFRDA as well for regulating and supervising the entities in their respective jurisdiction.*

*MHA is of the view that existing authorities may be empowered with legal powers for better regulation and protection of cyber space and for acting on cybercrime. National Cyber Coordination Centre (NCCC) has been established with an aim 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. The domain of NCCC is to monitor internet traffic data as well as proactive monitoring and analysis of cyber security threats*."

**7. Cyber Security Protection Authority**

**The Committee note that while the Government has established multiple agencies and initiatives to address cyber security concerns, including the National Cyber Security Coordinator (NCSC), Ministry of Electronics and Information Technology (MeitY), Computer Emergency Response Team —India (CERT-In), National Critical Information and Infrastructure Protection Centre (NCIIPC), and Indian Cyber Crime Coordination Centre (I4C), the current decentralized approach appears to be inadequate in providing a unified and coordinated response to the growing scale of cyber threats. The Committee is concerned that the fragmented structure, with several agencies handling different aspects of cyber security, may lead to inefficiencies, regulatory overlaps, and delays in response to emerging cyber risks.**

**The Committee note that Government has highlighted the roles of various stakeholders, such as the Reserve Bank of India (RBI), Securities and Exchange Board of India (SEBI), and other financial regulators in improving cyber security measures within their respective domains, the Committee believe that this approach may not be sufficiently comprehensive or proactive in addressing systemic risks to the nation's critical infrastructure and digital economy as a whole. The current mechanism, despite the best efforts of individual agencies, lacks a centralized authority that could provide cohesive leadership, coordination, and enforceability of cyber security policies across all sectors.**

**The Committee, therefore, strongly reiterates its recommendation for the establishment of Cyber Security Protection Authority - a centralized, overarching regulatory authority dedicated specifically to cyber security, similar to the role of the Directorate General of Civil Aviation (DGCA) in the aviation sector. Such an authority would have a clear mandate to oversee the protection of the nation's critical IT infrastructure, promote best practices, and ensure coordinated responses to cyber incidents. This centralized body would work in close collaboration with existing stakeholders like MeitY, RBI, NCIIPC, and other sectoral regulators, but would have the mandate to enforce compliance and ensure timely, proactive action across all sectors, especially in critical areas like banking, finance, and telecom.**

**Furthermore, the Committee stress that while the National Cyber Coordination Centre (NCCC) has been set up to generate situational awareness and monitor internet traffic for cyber security threats, its current scope and authority appear limited to threat analysis and information sharing. The Committee believe that NCCC, or a similar body under the proposed centralized authority, should be empowered with greater oversight and enforcement powers, enabling it to act decisively real time on identified cyber threats, incidents, and regulatory non-compliance. Additionally, it should be tasked with providing comprehensive cyber security frameworks and compliance guidelines, monitoring their implementation, and holding entities accountable for lapses in their cyber security practices.**

**Recommendation [(Serial No. 2) (vi)]**

**[Paragraph No.1 & 2]**

8. The Committee had recommended as under:

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.

9. In their Action Taken Reply the Ministry of Finance (Department of Financial Services) have submitted as follows:-

*"In this connection, it is stated that Financial intelligence Unit (FIU-IND) was set up as the central national agency responsible for receiving, processing, analysing and disseminating information relating to suspect financial transactions. Further, FIU-IND is responsible for coordinating and strengthening efforts of national and international intelligence, investigation and enforcement agencies in pursuing the global efforts against money laundering, terrorist financing and related crimes. With respect to the establishment of a Central Negative Registry (CNR), FIU-IND would be able to share inputs for creation and updating of CNR on the basis of information received.*

*MHA has informed that based on the complaint reported on the National Cybercrime Reporting Portal and information received from various stakeholders, I4C compiles and maintains a negative repository of suspected Bank account numbers, Mobile numbers, UPI IDs, etc., and share them with concerned entities to take necessary action. Such information needs to be taken in to account while performing due diligence of customers by the banks and financial institutions. I4C also maintains the repository of suspected URLs, websites and applications and shares it with all concerned stakeholders. The National Cybercrime Reporting Portal also facilitates LEAs to upload the mobile numbers for blocking by the concerned Telecom Service Providers (TSPs). So far 1.96 lakh mobile numbers have been blocked. I4C, MHA has requested RBI to take proactive steps for the integration of NCRP database with that maintained by RBI of fraud and attempted fraud cases.*

*Further, The Reserve Bank has put in place Central Payments Fraud Information Registry(CPFIR) in March 2020. All payment frauds reported by customers or detected by banks and PPI Issuers are reported to CPFIR by supervised entities (banks, non-bank Prepaid Payment Instrument Issuers and non-bank Credit Card issuers). Under the Payments Vision 2025, an enhancement in CPFIR envisaged was creating a negative database of fraudulent beneficiaries. The negative registry is envisaged to be created*

*using the suspect / beneficiary information reported to CPFIR. Once the negative database is created it is envisaged to share the same with supervised entities that may use the information for appropriate risk management checks at their end.*

*Further, the honourable Supreme Court passed a judgement on Civil Appeal No. 7300 of 2022 in connection with "no opportunity of being heard is envisaged to borrowers before classifying their accounts as fraudulent". In view of the same, the legal aspects of sharing / using the information in negative registry may also need to be examined, as the same is proposed to be created based on information reported by the customer / detected by the reporting bank with no opportunity provided to the beneficiary.*

*Every customer on identification of a payment fraud reports the same to their bank / non-bank entity whose payment system / payment instrument was used to undertake the transaction. As CPFIR mandates reporting from banks / non-bank entities based on customer reported frauds in all payment systems, the information available in CPFIR is comprehensive and should be leveraged in the fight against cyber-crimes.*

*Further, MHA's Citizen Financial Cyber Frauds Reporting and Management System (Helpline), developed as part of National Cybercrime Reporting Portal, provides an integrated platform where all concerned stakeholders like Law Enforcement Agencies (LEAs), Banks, Financial intermediaries, Payment wallets, etc., work in tandem to ensure that quick, decisive, and system-based effective action is taken to prevent the flow of money from innocent citizens to the fraudsters. However, not all frauds are reported in the Helpline.*

*Incidentally, RBI's Payment Vision 2025 provides that the Reserve Bank shall engage with the industry and Government to examine the feasibility of integrating CPFIR with other fraud reporting solutions to ensure that a single comprehensive platform is made available for real-time reporting and resolution of payment frauds in the country.*

*RBI has informed that while the payment ecosystem (banks, NPCI, card networks, payment aggregators, and payment apps) take various measures on an ongoing basis to protect customers from such frauds, a need was felt for network-level intelligence and real-time data sharing across payment systems. Hence, RBI had recently proposed to set up a Digital Payments Intelligence Platform which will harness advanced technologies to mitigate payment fraud risks. To take this initiative forward, a committee was constituted to examine the various aspects of setting up this Platform. The committee's recommendations are under examination by RBI."*

**10. Central Negative Registry (CNR)**

**The Committee acknowledge the various initiatives by the Government, such as the Financial Intelligence Unit (FIU-IND), the National Cybercrime Reporting Portal (NCRP), and the Central Payments Fraud Information Registry (CPFIR), aimed at tackling fraud and enhancing cyber security in the banking and financial sector. However, despite these efforts, the Committee remain concerned that the current systems remain fragmented and do not fully integrate the information across different agencies, which could result in delays or gaps in fraud detection and prevention.**

**The Committee strongly believe that the establishment of a centralized Central Negative Registry (CNR), as initially recommended, would significantly enhance the ability to proactively prevent fraud by consolidating data from FIU-IND, MHA, NCRP, RBI, and CPFIR into one unified repository. This would not only streamline the identification of fraudulent entities but also ensure better risk management by enabling more effective due diligence by financial institutions.**

**While the Government has taken steps to create separate repositories and registries, the Committee urge the Government to expedite the integration of these databases, including the proposed negative database from CPFIR, with the broader ecosystem of fraud management systems. The Committee also emphasize that legal challenges around the sharing of fraud information, as highlighted by the Supreme Court's ruling, (civil appeal no 7300 0f 2022) must be addressed swiftly to avoid delays in the implementation of such a system.**

**Furthermore, the Committee commend the development of the Digital Payments Intelligence Platform by the RBI and urge that its findings be aligned with the broader framework of fraud detection and prevention systems. The Committee urge that the Government prioritize the integration of these various initiatives into a single, comprehensive, and real-time fraud reporting and resolution platform, thereby enhancing both the speed and efficiency of the response to financial frauds in the country. This integrated approach would not only bolster the effectiveness of fraud prevention measures but also provide a robust mechanism for safeguarding the financial ecosystem and protecting innocent consumers from fraud.**

**Recommendation (Serial No. 3 (i))**

**[Paragraph No. 1 &2 ]**

11. The Committee had recommended as under:

*Consumer Grievance Redressal and Compensation Mechanisms*

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.

12. In their Action Taken Reply the Ministry of Finance (Department of Financial Services) have submitted as follows:-

*"RBI, vide circular dated July 06, 2017 on 'Limited liability of customers in unauthorized electronic banking transactions' addressed to SCBs, Small finance banks and Payment banks and circular dated December 14, 2017 on 'Limiting Liability of Customers of Co-operative Banks in Unauthorised Electronic Banking Transactions' addressed to all cooperative banks has issued the following guidelines:*

*Reporting of unauthorised transactions by customers to banks: Banks must ask their customers to mandatorily register for SMS alerts and wherever available register for e-mail alerts, for electronic banking transactions. The SMS alerts shall mandatorily be sent to the customers, while email alerts may be sent, wherever registered. The customers must be advised to notify their bank of any unauthorised electronic banking transaction at the earliest after the occurrence of such transaction, and informed that the longer the time taken to notify the bank, the higher will be the risk of loss to the bank/ customer. To facilitate this, banks must 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 unauthorised transactions that have taken place and/ or loss or theft of payment instrument such as card, etc. Banks shall also enable customers to instantly respond by "Reply" to the SMS and e-mail alerts and the customers should not be required to search for a web page or an e-mail address to notify the objection, if any. Further, a direct link for lodging the complaints, with specific option to report unauthorised electronic transactions shall be provided by banks on home page of their website. The loss/ fraud reporting system shall also ensure that immediate response (including auto response) is sent to the customers acknowledging the complaint along with the registered complaint number. The communication systems used by banks to send alerts and receive their responses thereto must record the time and date of delivery of the message and receipt of customer's response, if any, to them. This shall be important in determining the extent of a customer's liability. The banks may not offer facility of electronic transactions, other than ATM cash withdrawals, to customers who do not provide mobile numbers to the bank. On receipt of report of an unauthorised transaction from the customer, banks must take immediate steps to prevent further unauthorised transactions in the account".*

*Reversal timeline for Zero Liability/ Limited Liability of customer: 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 off any customer liability in case of unauthorised electronic banking transactions even in cases of customer negligence. The credit shall be value dated to be as of the date of the unauthorised transaction. Further, banks shall ensure that:*

*(i) 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 from the date of receipt of the complaint, and the customer is compensated as per provisions of paragraph 6 to 9 of the circular;*

*(ii) where it is unable to resolve the complaint or determine the customer liability, if any, within 90 days, the compensation as prescribed in paragraphs 6 to 9 is paid to the customer; and*

*(iii) in case of debit card/ bank account, the customer does not suffer loss of interest, and in case of credit card, the customer does not bear any additional burden of interest.*

*Burden of Proof : The burden of proving customer liability in case of unauthorised electronic banking transactions shall lie on the bank." The Reserve Bank has, vide circular dated September 20, 2019, put in place a framework on Turn Around Time (TAT) for resolution of failed transactions and compensation framework across all authorised payment systems. This was expected to increase customer confidence and bring in uniformity in processing of the failed transactions. The operators and participants of authorised payment systems have been advised that the TAT prescribed in the circular is the outer limit for resolution of failed transactions; and they shall endeavour towards quicker resolution of such failed transactions. Further, 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. Customers who do not get the benefit of redress of the failure as defined in the TAT, can register a complaint with the Reserve Bank - Integrated Ombudsman Scheme, 2021 (as amended from time to time).*

*RBI has issued directions vide email dated September 30, 2022 to Regulated Entities to put in place a dedicated team with enough nodal officers available to respond to LEAs on a 24*7 basis to provide near zero delay and reiterated the importance of having sufficient number of empowered and skilled resources, also at state level vide advisory by email dated February 9, 2024. Directions for deployment of dedicated personnel from the RE at the Financial Crime Command Centre of I4C, New Delhi was also issued to select REs vide advisory of even date, emphasizing the supportive role that Regulated Entities must play in cybercrime incidents.*

*To understand the needs of the Law Enforcement Agencies (LEAs) and to exchange ideas on the subject, a Workshop with LEAs was held at RBI on April 16, 2024.*

*RBI is in the final stages of issuing a circular on 'Prevention of financial frauds perpetrated using voice calls and SMS' to all its Regulated Entities to comply with TRAI guidelines on making marketing / transaction calls for particular series of numbers, register their SMS headers and templates etc. The circular also emphasises the Regulated Entities clean their customer database based on Mobile Number Revocation List (MNRL) published by DoT.*

*In relation to reported cases of alleged cybercrime frauds, it is observed that despite the efforts of stakeholders, the recovery rate of defrauded amount is not very encouraging. Considering the same, the Reserve Bank's Payments Vision 2025 provides for conducting a study on scope / feasibility of creation of Digital Payments Protection Fund (DPPF). Immediately reimbursing a customer without following due process as laid out in the payment system's guideline may create perverse incentives wherein the customer may report even a genuine transaction as fraudulent and claim the amount."*

**13. The Committee appreciate the efforts made by the Reserve Bank of India (RBI) to implement frameworks such as the Zero Liability / Limited Liability policy, Turnaround Time (TAT) for resolution of failed transactions, and the Compensation Framework for unauthorized electronic banking transactions. These measures are a step in the right direction in protecting customers and ensuring swift redressal of complaints.**

**However, the Committee remain concerned that the current system, despite its provisions, still relies on a reactive approach, Customers are obligated to report unauthorized transactions, with compensation dependent on the completion of further investigations and the traceability of funds. This process has often been made overly complex and time-consuming. This approach not only delays the resolution process but also leaves customers vulnerable during the interim period. The delays in resolving cases may not fully protect consumers from the immediate financial impact of cybercrime. The Committee reiterates its recommendation that the compensation process be automated, with financial institutions initiating compensation promptly, without unnecessary delays pending investigation or final traceability of fraud.**

**Recommendation [Serial No.3(ii)]**

**(Paragraph No.1)**

*14. The committee had recommended as under:*

*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.*

*15. In their Action Taken Reply the Ministry of Finance (Department of Financial Services) have submitted as follows:-*

*"RBI vide Master Direction on Digital Payment Security Controls of RBI, banks have been advised that alerts (like SMS, e-mail, etc.) should be applied in respect of all payment transactions (including debits and credits), creation of new account linkages (addition/ modification/ deletion of beneficiaries), changing account details or revision to fund transfer limits.*

*It is also submitted that under the provisions of the Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions, banks must ask their customers to mandatorily register for SMS alerts and wherever available register for e-mail alerts, for electronic banking transactions. The SMS alerts shall mandatorily be sent to the customers, while email alerts may be sent, wherever registered. In addition, the time period for determining customer liability in case of unauthorised transaction starts from the time the customer receives the SMS notification, to account for telecom network related issues.*

*Reserve Bank of India has also issued instructions vide its circulars dated February 18, 2009, March 29, 2011 and August 27, 2021 that Payment System Providers shall 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.*

*TRAI has apprised that Access Service Providers have built resilient and stable systems that ensure that all SMSs are delivered to the consumers. Under TCCCPR-2018, there is flexibility available with the Senders that for sending the commercial communications over the networks of Access Service Providers, the Senders can either deal directly with the Access Service Providers or opt to outsource this exercise to registered telemarketers (RTMs) and use their communication platform. RBI may encourage Banks/ other financial institutions to reduce number of RTMs in the chain between the Banks/ other financial institutions and Access Service Providers or preferably establish direct connectivity with the Access Service Providers.*

*DOT has launched an online Digital Intelligence Platform (DIP) for sharing of telecom misuse related information and list of disconnected numbers along with reasons with the stakeholders for prevention of cyber-crime and financial frauds. At present TSPs, DOT field Units, 460 banks and financial institutions, RBI, 30 State/UT Police, MHA 14C, NIA, FIU, UIDAI, GSTN etc. have on-boarded the platform."*

**16. Irregularities in SMS alerts, where customers do not receive notifications for credits or debits of a transaction, have been identified as a significant vulnerability in the financial system. The Committee acknowledge the measures taken by the Reserve Bank of India (RBI) to mandate Additional Factor of Authentication (AFA) for various payment methods, including UPI, mobile payments, and card payments. In response to the ever evolving tactics of fraudsters, the Committee strongly reiterate the recommendation that financial institutions ensure consistent and timely SMS notifications for all transactions.**

**Furthermore, the Committee stresses the importance of implementing a dual display of transaction amounts — both in numeric and written word format — during online payments across platforms like Google Pay (GPay), UPI, BHIM, and**

**others. This simple yet highly effective measure would mitigate errors such as inadvertently adding extra zeros or misinterpreting the amount, thereby enhancing the accuracy of transactions. This dual confirmation would significantly improve**

**user experience, increase confidence in the system, and reduce the potential for costly errors.**

**The Committee urge that the RBI and relevant financial authorities urgently adopt these measures to strengthen consumer protection, enhance transaction accuracy, and ensure greater accountability within the digital payments ecosystem.**

**NEW DELHI**
**4 December, 2024**
**13 Agrahayana, 1946 (Saka)**

**BHARTRUHARI MAHTAB,**
**Chairperson,**
**Standing Committee on Finance**

## CHAPTER II

## OBSERVATIONS/RECOMMENDATIONS WHICH HAVE BEEN ACCEPTED BY THE GOVERNMENT

### Recommendation Serial No.1(i) Paragraph No.1

**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, better KYC 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.

### Reply of the Government

The Government is cognizant of various emerging issues in the cyberspace and making continuous efforts to have in place appropriate regulation. The Information Technology Act, 2000 (“IT Act”) provides provisions for regulatory powers for dealing with internet service providers (ISPs).

Section 79(1) of IT Act provides for exemption to the intermediaries from the liabilities for third party user information, and to claim such exemption, the intermediaries have to observe certain due diligence prescribed through intermediary guidelines under section 79(2)(c) of the IT Act. Such due diligence to be followed by the intermediaries includes making reasonable efforts by themselves and causing their users not to transmit or share any unlawful information.

Section 85 of IT Act (offences by companies) and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (“IT Rules, 2021”), provide for deterrent provisions to any negligence or failure in preventing transmission of any unlawful information/activity on the intermediary platforms. The rule 3 (applicable for all intermediaries) and rule 4 (applicable for significant social media intermediaries) of the IT Rules, 2021 cast obligations on the intermediaries, including social media intermediaries, to observe certain due diligence. The rule 7 of the IT Rules, 2021 prescribes that in case of failure to follow diligence as provided in the IT Rules, 2021, by intermediaries, they shall lose their safe harbour protection under section 79 of the IT Act and shall be liable for consequential action as provided in such law.

Further, in case, an intermediary is a significant social media intermediary ("SSMI") (an intermediary having more than 50 lakh registered users in India), it has to additionally observe due diligence in terms of appointing, in India, a Grievance Officer, a Chief Compliance Officer and a nodal contact person for 24x7 coordination with law enforcement agencies.

The rule 3(1)(d) of the IT Rules, 2021 empowers the respective appropriate Government such as the Ministry of Finance or its relevant Departments or its authorised agency(ies) including their regulating agencies to deal with any violation of the extant laws including KYC related directions being administered by them and direct the intermediary concerned to remove any information which violates such laws.

Section 69A of the IT Act provides power to the Central Government to issue directions to block any information if it is necessary or expedient to do so in the interest of sovereignty and integrity, defence of India, security of the State, friendly relations with foreign States or public order or for inciting cognizable offence relating to above.

The rule 8(4) of Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, provides provision for carrying out the audit of reasonable security practices and procedures at least once a year, or, as and when the body corporate or a person on its behalf undertakes significant upgradation of its process and computer resource.

The Indian Computer Emergency Response Team (CERT-In) issued directions relating to information security practices, on 28.04.2022 in exercise of powers under section 70B(6) of the Information Technology Act, 2000. These directions aim to enhance overall cyber security posture and ensure Safe & Trusted Internet in the country. Thereafter, in response to general queries received by CERT-In, a set of Frequently Asked Questions (FAQs) document was also issued on 18.05.2022, to enable better understanding of the various stakeholders.

CERT-In has issued “guidelines on information security practices for Government entities” in June 2023. These guidelines, issued under the powers conferred by clause (e) of sub-section (4) of section 70B of the Information Technology Act, 2000 (21 of 2000), apply to all Ministries, Departments, Secretariats, and Offices specified in the First Schedule to the Government of India (Allocation of Business) Rules, 1961, along with their attached and subordinate offices. The purpose of these guidelines is to establish a prioritized baseline for cyber security measures and controls within government organisations and their associated organisations. The guideline shall assist security teams to implement baseline and essential controls and procedures to protect their Cyber infrastructure from prominent threats.

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

With the advancement of technologies and increasing online users, cyberspace is facing many challenging issues. Ministry of Electronics and Information Technology (MeitY) is considering review of the existing regulatory landscape, including the IT Act with an attempt to overhaul them to address many present-day and emerging challenges in the cyberspace. However, to effectively address the issue of emerging cyber incidents and cybercrimes relating to financial frauds, money-laundering and economic security of the country, the IT Act and any other Digital law/ regulatory framework for administering the emerging issues in the cyber space as a whole, can consider introducing necessary obligations on the digital intermediaries including the Big Techs for making reasonable efforts to prevent economic cybercrimes and comply with the extant laws and thereby ensure safe & trusted Internet for the Indian users.

With regards to regulation of service providers in financial sector, RBI has informed that with the increased use of technology in provision of financial services, traditional entities such as banks and NBFCs are now deeply engaged in availing services from Third party service providers including Big Tech firms.

As regards the big-tech firms, they currently operate in specific financial service activity such as payment services, based on applicable regulatory framework. However, they have been expanding their footprint in partnership with traditional financial sector players in other areas of operations to leverage the network effects of their large customer base. In view of the complex business structure of Big Techs, approaches to regulate them by different regulators including the competition authority and to be set up data protection board is still evolving across the world and financial regulators would need to coordinate on a national level to create an enabling regulatory framework.

As regards Fin Techs and other third-party IT service providers, RBI has been seized of the risks posed to the financial sector ecosystem due to their linkages with

supervised entities and has been continuously taking steps, including adjusting its regulatory/supervisory processes in line with the emerging risks.

Importance of vendor risk management was recognised and broad guidelines in this area were laid down as part of the Cyber Security Framework issued to banks in June, 2016.Further, in order to enable effective management of attendant risks in outsourcing of payment and settlement-related activities by Payment System Operators, a regulatory framework was issued by RBI in August 2021 which requires the Payment System Operators to ensure, among other things, that cyber security risk – where breach in IT systems may lead to potential loss of data, information, reputation, money, etc. - is addressed by them.

RBI issued regulations on Digital Lending, in September 2022, which requires, among other things, that the supervised entities and the Lending Service Providers (LSPs) engaged by them comply with various technology standards/ requirements on cyber security stipulated by RBI and other agencies.

Master Directions on IT Governance, Risk, Controls and Assurance Practices issued in November 2023 advised REs to implement appropriate vendor risk assessment process and controls proportionate to the assessed risk and materiality to mitigate concentration risks, address conflict of interests and manage supply chain effectively. These guidelines apply where third-party arrangements in the Information Technology/ Cyber Security ecosystem are not within the applicability of the Reserve Bank of India (Outsourcing of Information Technology Services) Directions, April 2023.

Several third-party IT service providers have been providing similar services to multiple banks and hence cyber security posture of these common third-party IT service providers will have impact on the sector. To assess cyber security risks posed by these common third-party service providers, banks have been conducting pooled audits (as per

our Master Direction on Outsourcing of IT services). This involves multiple banks using a single service provider forming a group to conduct a joint audit. A comprehensive audit scope is created, and the audit is performed by a CERT-In-empanelled auditor. This approach aims to improve the overall cyber security posture of the banking sector by ensuring that third-party service providers meet necessary security standards. Pooled audit exercise has been carried out for a few third-party service providers.

RBI along with MHA held discussions with Google to discuss measures for protection of customers from frauds via online third-party apps. Google in its android platform had implemented controls such as Google Messages obfuscation when screen recording is detected, warning the users when they click on suspicious links/links from unknown sources, real-time analysis of apps before installation, detection of unsafe environments (presence of malware, sensitive permissions by other apps etc) for banking/financial applications to improve security.

DoT has informed that following measures have been taken to curb the misuse of telecom resources in cybercrime, financial frauds:

I. ASTR (अस्त्र) is an AI powered facial recognition solution developed by DoT to detect mobile connections taken on fake/forged KYC documents and get them disconnected failing reverification. The information of these disconnected mobile connections is shared with MHA, Police, RBI, Banks & social media platforms for freezing/ blocking accounts linked to these numbers.

II. Sanchar Saathi Portal https://sancharsaathi.gov.in: Sanchar Saathi portal is a citizen centric initiative to empower mobile subscribers, strengthen their security and increase awareness about citizen centric initiatives of the Government. Sanchar Saathi empowers citizens by allowing them to know the mobile connections issued in their name, get disconnected the connections not

required by them, block/trace lost mobile phones and check genuineness of devices while buying a new/old mobile phone. Sanchar Saathi contains various modules like CEIR, TAFCOP etc.

III. Using ASTR and sancharSaathi portal, 114 crore mobile connections have been analysed out of which 83.26 lakh suspicious connections were detected and 59.06 lakh mobile connections have been disconnected failing reverification.

IV. 68,255 Point of Sale (SIM agents) involved in selling such mobile connections on fake/forged documents have been blacklisted and 316 FIRs registered against such Point of Sale (PoS) across the country.

V. DoT has amended the existing KYC instructions vide F.No. 800-09/2023-AS.II dated 31.08.2023 and introduced guidelines for regulation of PoS vide F.No. 800-09/2022-AS.II dated 31.08.2023. These are steps towards improving the KYC process and making the processes of SIM issuance more robust.

Further, DoT has launched a Digital Intelligence Portal which is an integrated platform for DoT, Telecom Service Providers, Law Enforcement Agencies (LEAs), Financial Institutions (FIs), banks, On The Top (OTT), Proof of identity (PoI) issuing authority and other stakeholders for information exchange and coordination for curbing cyber-crime, and financial frauds committed through misuse of telecom resources.

In view of the above, it could be concluded that joint efforts to enhance regulatory controls in their respective domains have already been initiated by the respective ministries/organizations on an ongoing and continued basis. MeitY underscored the established frameworks under the IT Act to regulate internet service providers and intermediaries, while also indicating a potential overhaul of the existing regulatory landscape. The RBI acknowledged the increased engagement with third-party service providers, emphasizing their continuous adjustments to regulatory processes to address

evolving risks, especially in the areas of digital lending and IT outsourcing. Similarly, DoT/TRAI, has implemented AI-powered solutions like ASTR and the Sanchar Saathi portal to address misuse of telecom resources and improve KYC processes. Collectively, these responses signify a dynamic and proactive approach by all stakeholders in addressing the complexities of the digital and financial ecosystem, ensuring that regulatory processes remain robust and responsive to the evolving landscape.

**[Ministry of Finance (Department of Financial Services), O.M. No. e.F.no.CSFT-01/4/2023, Dated 18th October, 2024]**

**Recommendation Serial No.1(ii) Paragraph No.1**

**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.

**Reply of the Government**

RBI has informed that RTGS and CCIL (a Central Counter Party) have been declared as Financial Market Infrastructure (FMI) under Principles for Financial Market Infrastructure (PFMI) guidelines issued by Committee on Payments and Market Infrastructures of Bank for International Settlements (BIS). FMIs are required to have the cyber resilience framework put in place as per the standards stipulated by RBI from time to time and guided in the CPMI document. The above mentioned FMIs are also regularly accessed based on the benchmark criteria in the PFMI guidelines. In the case of CCIL, apart from offsite monitoring of availability of its systems, CCIL is also subject to a rigorous onsite inspection of its IT infrastructure, including security assessments, by experts from the Reserve Bank Information Technology Private Limited. In the case of RTGS, close monitoring of system uptime is being monitored by Department of Payment

and Settlement Systems (DPSS), RBI through a dashboard that gives regular updates on the system's functioning. NEFT, though not classified as an FMI, being a critical infrastructure, is also subject to same process as RTGS.

The regulated entities are required to proactively report any abnormal events, aberrations, delays, incidents, downtime, etc. to the RBI at the earliest possible time. This system of alerts is designed to track and mitigate risks in a timely manner, as well as prevent disruptions to the entities and the payment system as a whole. Necessary follow-up actions are taken to ensure that corrective actions are being implemented properly. In addition, regulated entities must submit a System Audit Report (SAR) conducted by a Certified Information Systems Auditor (CISA), on an annual basis within two months of the close of their respective financial year, which covers incident management, robustness, vulnerability assessment, penetration testing, security controls, and disaster recovery plans. Further, any cyber security incident or threat, is to be examined on a priority basis and necessary preventive steps are to be implemented.

Further, all authorised non-bank Payment System Operators are required to proactively report any unusual incidents like cyber attacks, outage of critical system/ infrastructure, internal fraud, settlement delay, downtime etc. to the RBI within 6 hours of detection. This system of alerts is designed to track and mitigate risks in a timely manner, as well as prevent disruptions to the entities and the payment system as a whole. Necessary follow-up actions are taken to ensure that corrective actions are being implemented properly. In addition, regulated entities must submit a System Audit Report (SAR) conducted by a Certified Information Systems Auditor (CISA), on an annual basis within two months of the close of their respective financial year, which covers incident management, robustness, vulnerability assessment, penetration testing, security controls, and disaster recovery plans. Further, for any cyber security incident or threat, it is to be examined on a priority basis and necessary preventive steps are to be implemented.

Keeping in view the importance of NPCI operated systems in retail payments, special emphasis is laid on monitoring of system downtimes. There is an established system of daily reporting of downtime at NPCI as well as member banks' levels. The incidents are examined and taken up with NPCI and the member banks on need basis. NPCI downtime is regularly discussed in the quarterly business review meetings.

**[Ministry of Finance (Department of Financial Services), O.M. No. e.F.no.CSFT-01/4/2023, Dated 18th October, 2024]**

**Recommendation Serial No.1(iii) Paragraph No.1**

**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.

**Reply of the Government**

RBI has put in place the IT/ cyber security regulatory framework, which is based on updated global standards such as National Institute of Standards and Technology (NIST) standards and appropriately tuned to the requirements of the Indian banking sector. An Inter-disciplinary Standing Committee on Cyber Security was formed in 2017 with external members from the CERT-In, Academia, Professionals in the field, forensic auditor, inter alia, to review the threats inherent in the existing/emerging technology; study adoption of various security standards/protocols; interface with stakeholders; and suggest appropriate policy interventions to strengthen cyber security and resilience. The Standing Committee meets on a quarterly basis. Threat intelligence and learnings from cyber security incidents from specific entity is promptly shared with rest of the entities.

RBI is regularly holding discussions with counterparts in various Central Banks such as ECB (Europe) as well as with various policy institutions such as BIS (Basel) and

Financial Stability Board (FSB) on the area of Cyber and IT risks. RBI is a member of various Working groups constituted by FSB relating to Cyber Lexicon, effective practices for cyber incident response and recovery and cyber incident reporting. RBI is also associated with BRICS Rapid Information Security Channel.

**[Ministry of Finance (Department of Financial Services), O.M. No. e.F.no.CSFT-01/4/2023, Dated 18th October, 2024]**

**Recommendation Serial No.1(iv) Paragraph No.1**

**Regularly audit** the entire financial system especially cyber security and eKYC safeguards.

**Reply of the Government**

RBI has informed that banks are assessed periodically for their compliance to its instructions/regulation including cyber security and eKYC. RBI also conducts risk based on site IT Examinations of its supervised entities (SEs) periodically to ensure compliance with relevant instructions on Cyber security. RBI has prescribed third party audit by CERT-In empanelled auditors where appropriate, for assurance on IT/ cyber risk in supervised entities. Further, various periodic offsite data are collated and analysed to ensure continuous monitoring of the supervised entities.

In addition, in order to ensure that the technology deployed by Payment System Operators is being operated in a safe, secure, sound, and efficient manner, the authorized entities participating in payment systems are required to submit a System Audit Report (SAR) conducted by a Certified Information Systems Auditor (CISA), on an annual basis within two months of the close of their respective financial year. The scope of the System Audit should include the evaluation of the hardware structure, operating systems, and critical applications; security and controls in place, access controls on key applications,

disaster recovery plans, training of personnel managing systems and applications and documentation.

RBI has informed that Master Directions on Cyber Resilience and Digital Payment Security Controls for non-bank Payment System Operators was also issued by RBI in July 2024. The Directions cover baseline security measures for ensuring system resiliency as well as safe and secure digital payment transactions. These Directions aim to improve safety and security of the payment systems operated by PSOs by providing a framework for overall information security preparedness with an emphasis on cyber resilience.

KYC/eKYC aspect is also monitored by the Risk Based Supervision performed by RBI on its SEs through various onsite/ offsite mechanism. Internal assurance mechanism through periodic audits by qualified internal/ external auditors has been prescribed for SEs to ensure adherence to extant instructions. Further RBI is working with SEs to strengthen their internal Information System Audit function to serve as an effective third line of defence.

**[Ministry of Finance (Department of Financial Services),**
**O.M. No. e.F.no.CSFT-01/4/2023, Dated 18th October, 2024]**

**Recommendation Serial No.1(v) Paragraph No. (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.

**Reply of the Government**

Department of Telecom (DoT) has carried out analysis of 2.37 lakh Principal Entities (PEs)(- registered for sending bulk SMSs), 6.4 lakh SMS headers and 35 lakh SMS content templates and generated intelligence for suspected PEs, SMS Headers and

SMS templates. 20000 PEs, 30000 SMS Headers and 1.95 lakh SMS content templates have been removed from DLT Platform which allows to send such bulk SMSs.

Based on digital intelligence for misuse of SMS Headers, TRAI has issued multiple directions to Access Providers to stop misuse of Headers and Message Templates, and to curb unauthorized promotions using telecom resources under Telecom Commercial Communications Customer Preference Regulations, 2018 (TCCCPR-2018) dated 16.02.2023, 12.05.2023, 25.05.2023

Telecom Regulatory Authority of India (TRAI) through TCCCPR-2018 and various Directions issued thereunder from time to time, has taken several measures to curb the Unsolicited Commercial Communications (UCC) through text messages.

TRAI observed that some PEs, i.e. the senders of commercial messages, have registered a large number of Headers and Content Templates and, at times, some of these are misused by some Telemarketers. Therefore, through its Direction dated 16.02.2023,Access Service Providers were directed to reverify all registered Headers and Message Templates on DLT platform and block all unverified Headers and Message Templates within 30 days and 60 days respectively.

PEs are required to get Content Templates registered with the Access Service Providers. These templates typically have fixed and variable components. It has been observed that, at times, variable part of the message template is misused and the promotional content is being passed in the variable portions of Content Templates. Therefore, through its Direction dated 12.05.2023, TRAI has directed all the Access Service Providers that the use of more than three variable parts in the contents shall be permitted only with proper justification and additional checks. TRAI has mandated that Access Service Providers shall have to designate a separate approving authority for such Content Templates. Each variable part needs to be pre-tagged for the purpose it is

proposed to be used and minimum thirty percentage of message should comprise of fixed part so that intent of the original message, for which the content template was approved, is not changed by the intermediaries. It has also been decided that only white listed URLs/Apks/OTT links / call back numbers shall be allowed in the Content Template.

Further, DOT has launched an online Digital Intelligence Platform (DIP) for sharing of telecom misuse related information and list of disconnected numbers along with reasons with the stakeholders for prevention of cyber-crime and financial frauds. At present TSPs, DOT field Units, 460 banks and financial institutions, RBI, 30 State/UT Police, MHA 14C, NIA, FIU, UIDAI, GSTN etc. have on-boarded the platform.

**[Ministry of Finance (Department of Financial Services), O.M. No. e.F.no.CSFT-01/4/2023, Dated 18th October, 2024]**

**Recommendation Serial No.1(v) Paragraph No.(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.

**Reply of the Government**

TRAI has informed that following provisions have been made in the TCCCPR-20I8 to ensure that only messages sent by Senders (Principal Entities) are transmitted:

(i) An individual, business or legal entity that sends commercial communication is referred to as Sender or Principal Entity (PE). Under the TCCCPR-2018, as a first step, Senders are mandatorily required to register themselves with any of the Access Service Providers to become a registered Sender. Sender, once registered, is assigned a unique ID i.e. "Principal Entity ID".

(ii) For sending commercial communications over the networks of Access Service Providers, the Senders (PEs) can either deal directly with the Access

Service Providers or opt to outsource this exercise to Registered Telemarketers (RTMs) and use their communication platform. Telemarketers are thus engaged by Senders for the purpose of transmitting commercial communications on behalf of the Senders to the intended subscribers/ customers, for which purpose the networks of the Access Service Providers are utilized as conduit.

(iii) Once a Sender has been registered, it is required to register with any Access Service Provider the "headers" that it is desirous of using for sending commercial communications. 'Header' means an alphanumeric string of maximum eleven characters or numbers assigned to Senders under these regulations to send commercial communications. Headers once registered are also assigned unique IDs, i.e., "Header IDs".

(iv) Thereafter, the Sender is required to also register with any Access Service Provider, the Content Templates for its commercial communications. Content Templates are templates of content registered by any Sender with any Access Service Provider for sending commercial message(s). These templates typically have fixed and variable components. Fixed part of the content is pre-declared at the time of registration of Content Template which is common across all commercial communications sent to different recipients for same or similar subject. Content Templates once registered are also assigned unique iDs, i.e., "Template IDs".

(v) Any commercial communication coming from PE, via RTM route or directly, is subjected to scrubbing in DLT against Unique PE Id, Header, and Content Templates and, if it fails, then it is not allowed to be delivered.

Further, no commercial communication can be sent except from a registered header/ number. This has been achieved by the Access Service Providers by developing a state-of-the-art blockchain registry.

Further, for effective implementation of TRAI's regulation TCCCPR 2018 and the various directions issued under these regulations, all entities/ institutions such as banks, credit card companies, insurance companies, regulators, etc were requested to strictly adhere to the prescribed instructions and send commercial communication using telecom resources through voice calls or SMS using only '140/ 160' numbering series (or any other Numbering series allocated/ assigned by DoT/ TRAI in future).

**[Ministry of Finance (Department of Financial Services), O.M. No. e.F.no.CSFT-01/4/2023, Dated 18th October, 2024]**

**Recommendation Serial No.1(v) Paragraph No.(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.

**Reply of the Government**

RBI has informed that as per extant cyber security framework, banks have been advised to implement centralised authentication and authorisation system for accessing and administering applications, operating systems, databases, network and security devices/systems, point of connectivity (local/remote, etc.) including enforcement of strong password policy, two-factor/multi-factor authentication depending on risk assessment and following the principle of least privileges and separation of duties. Compliance to the regulations in this regard is required to be monitored by the SEs as part of their periodical internal IS Audit process and is also closely assessed during periodic onsite assessment of cyber/IT risks in the supervised entities by the RBI.

**[Ministry of Finance (Department of Financial Services), O.M. No. e.F.no.CSFT-01/4/2023, Dated 18th October, 2024]**

**Recommendation Serial No.1(v) Paragraph No.(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.

**Reply of the Government**

RBI has informed that multiple security controls including additional factor of Authentication, tokenisation, device binding for mobile banking applications, etc. have been mandated in this regard. Master Direction on Digital Payment Security Controls has been prescribed by RBI in 2021 which requires the Regulated Entities (REs) to ensure that they implement, except where explicitly permitted/ relaxed, multi-factor authentication for payments through electronic modes and fund transfers, including cash withdrawals from ATMs/ micro-ATMs/ business correspondents, through digital payment applications. At least one of the authentication methodologies should be generally dynamic or non-replicable. Besides educating customers on safe banking behaviour, the banks are also required to implement transaction monitoring system to alert the customers of potential fraudulent transactions.

**[Ministry of Finance (Department of Financial Services), O.M. No. e.F.no.CSFT-01/4/2023, Dated 18th October, 2024]**

**Recommendation Serial No.1(v) Paragraph No.(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.

**Reply of the Government**

Regulated Entities were advised by RBI in 2021 that communication between the ATM terminal/PC and the ATM Switch should be encrypted end-to-end. Further, it has been

advised that Network cables, I/O ports within the ATM premise should be concealed and physically secured/protected. These instructions have been implemented by the banks and sustenance of compliance to the same is being monitored by RBI.

**[Ministry of Finance (Department of Financial Services), O.M. No. e.F.no.CSFT-01/4/2023, Dated 18th October, 2024]**

**Recommendation Serial No.1(vi) Paragraph No.1**

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.

**Reply of the Government**

Ministry of Electronics and Information Technology (MeitY) has informed that the policies of the Government are aimed at ensuring an Open, Safe & Trusted and Accountable Internet for its users. Government is fully cognizant and aware of the growing cyber security threats and attacks.

The Appstore may be treated as intermediary between the App-developer and the user of such App, and hence they are excluded from the liability for the third-party content as per the provisions of the Information Technology Act, 2000. However, the Appstore, in addition to the meta-data and other data of the user and App-developer, also stores the personal information of the App-developer and the user. As these Appstore are storing the personal data, they are obligated to be a data fiduciary as per the definition given in the Digital Personal Data Protection Act, 2023 (DPDPA). The said Act has obligation entrusted on the data fiduciary and rights granted to the data principals. The data stored with the Appstore, other than the personal data, gets covered by the Information

Technology Act, 2000. Further, as per rule 3(1)(j) of the IT Rules, 2021, the prescribed timeline to be observed by an intermediary and an online gaming intermediary enabling access to online real money game to provide information under its control or possession, or assistance to the lawfully authorised agencies upon request for investigative or protective or cyber security activities are 72 hours and 24 hours respectively. Accordingly, any information about any app may be sought by the lawfully authorised agencies from the app stores concerned for the purpose of investigative or protective or cyber security activities.

(i). Obligations of the data fiduciaries:

a) Personal data processing based on consented, lawful, and transparent manner
b) Upholding the principle of purpose limitation, using data only for specified purposes
c) Embracing data minimization, collecting only necessary data for the purpose
d) Ensuring data accuracy and updates
e) Ensuring storage limitation, retaining data only as long as necessary
f) Requiring reasonable security safeguards for preventing data breaches
g) Requiring notification of affected Data Principals and the Data Protection Board about breaches
h) Erasing personal data upon withdrawal of consent
i) Establishing grievance redressal systems and responsive officers
j) Complying with the additional obligations of Significant Data Fiduciaries like data protection impact assessment and data audits.

(ii). Rights of the data principal (individual):

a) To access processed personal data
b) To correct and erasure of data
c) To get their grievance redressed

d) To nominate a representative in case of incapacity or death.

(iii). Data Protection Board

In case of violation of the Act, the Data Protection Board can impose penalties on the data fiduciaries depending on the gravity of the breach or the complaint.The DPDPA provides for the processing of digital personal data that recognizes both the rights of the individuals to protect their personal data and for the data fiduciaries the need to process such personal data for lawful specific purposes. Its comprehensive provisions safeguard individual data rights, enable legitimate data processing, and promote India's digital progress within a framework of principles, regulation, and accountability.

**[Ministry of Finance (Department of Financial Services), O.M. No. e.F.no.CSFT-01/4/2023, Dated 18th October, 2024]**

**Recommendation Serial No.1(vii) Paragraph No.1**

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”.

**Reply of the Government**

Ministry of Home Affairs (MHA) has informed that ‘Police’ & ‘Public Order’ are State subjects and states are primarily responsible for dealing with cybercrime. To strengthen the mechanism for dealing with cybercrime in a comprehensive and coordinated manner, the Central Government has made efforts to identify the gaps in States/UTs capacity and fill them through support and coordination.

MHA has established the ‘Indian Cyber Crime Coordination Centre’ (I4C) to deal with all types of cybercrime in a coordinated and comprehensive manner. The scheme is envisaged to act as a nodal point to curb cybercrime, ensure ease of filing cybercrime related complaints, identifying cybercrime trends/ patterns, focus on public awareness about cybercrime modus operandi and patterns and creating national ecosystem to combat all types of cybercrime.

MHA has prepared National Information Security Policy and Guidelines (NISPG) in March, 2019 in order to prevent information security breaches/ Cyber intrusions in ICT infrastructure. The NISPG has been shared with the Central Ministries as well as the State Governments/ Union Territories. They have been advised to take appropriate steps to strengthen information security controls as per NISPG for strengthening Information Security and preventing information security breaches. In order to meet the challenges posed due to current technological & threat landscape NISPG is being revised.

Further, Ministry of Electronics and Information Technology (MeitY) has informed that as per rule 3 of the Information Technology (National Critical Information Infrastructure Protection Centre and Manners of Performing Functions and Duties) Rules, 2013 ("NCIIPC Rules"), the National Critical Information Infrastructure Protection Centre

("NCIIPC") is the national nodal agency designated under section 70A of the Information Technology Act, 2000 ("IT Act") in respect of Critical Information Infrastructure (CIIs) Protection. Further, as per rule 4 of the NCIIPC Rules, the NCIIPC is empowered to evolve protection strategy, policies, etc. for protection of CIIs including the issuance of necessary guidelines to protect them.

Banking, Financial Services and Insurance(BFSI) sector is one of the seven identified critical sectors. As per Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Functions and Duties) Rules,2013, constituency of NCIIPC is the notified CIIs.

NCIIPC, in consultation with Ministry of Finance, has taken-up the case for CII identification with concerned entities and till date CIIs of GSTN,RBI, NPCI, 15 Banks, 10Market Infrastructure Institutions and LIC have been identified and notified as Protected Systems in the BFSI Sector.

All organisations having Protected Systems need to follow Information Technology (Information Security Practices and Procedures for Protected Systems) Rules, 2018.NCIIPC from time to time issues various guidelines, standard operating procedures(SOPs), best practices, alerts and advisories to be followed by organisations having Protected Systems to enhance their Cyber Security Posture.

In view of the above, it could be concluded that the Government has implemented a comprehensive approach to address cyber security concerns and protect critical financial infrastructure. It has established the Indian Cyber Crime Coordination Centre (I4C) as a nodal point for curbing cybercrime and enhancing public awareness. Additionally, the National Information Security Policy and Guidelines (NISPG) have been developed to prevent information security breaches and are currently being revised to address evolving threats.

For Critical Information Infrastructure Protection, the National Critical Information Infrastructure Protection Centre (NCIIPC) is designated as the national nodal agency. NCIIPC formulates protection strategies, policies, and guidelines and has identified and notified several Critical Information Infrastructures (CIIs), including entities within the Banking, Financial Services, and Insurance (BFSI) sector.

The Cabinet Secretariat, through gazetted notification no. CG-DL-E-27092024-257563, dated 27.09.2024 has recently amended the Government of India (Allocation of Business) Rules, 1961. As per the notification, National Security Council Secretariat (Rashtriya Suraksha Parishad Sachivalaya) has been assigned the responsibility of providing overall coordination and strategic direction for cyber security. Further, the notification also states "*matters relating to security of telecom networks"* has been assigned to Department of Telecommunications under Ministry of communications. *"Matters relating to Cyber Security as assigned in the Information Technology Act, 2000 (21 of 2000) and support to other Ministries / Departments on Cyber Security*" have been assigned to Ministry of Electronics and Information Technology. "*Matters relating to Cyber Crime"* has been assigned to Ministry of Home Affairs.

**[Ministry of Finance (Department of Financial Services), O.M. No. e.F.no.CSFT-01/4/2023, Dated 18th October, 2024]**

**Recommendation Serial No.4(i) Paragraph No.1**

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.

**Reply of the Government**

Cybercrime being a state subject, the action on cybercrime complaints, hotspots of cybercrime etc. have to be taken by concerned States/UTs. However, cybercrime hotspots have been identified and periodic advisories are shared with concerned stakeholders.

Joint Cybercrime Coordination Team (JCCT) is one of the verticals of I4C 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 Joint Cybercrime Coordination Teams comprising various States/UTs based on the hotspots in the country. Seven workshops & discussion session of JCCT were held at Hyderabad, Ahmedabad, Guwahati, Vishakhapatnam, Lucknow, Chandigarh and Ranchi recently in Oct-Nov 2023 on the agenda/topics of CFCFRMS, Helpline No. 1930, cybercrime hotspots, cyber commandos, cyber volunteer and awareness programmes.7 Joint Cyber Coordination Teams have been formed at Mewat, Jamtara, Ahmedabad, Hyderabad, Chandigarh, Visakhapatnam and Guwahati. I4C has also appointed nodal officers for each States. To have effective coordination among JCCTs, following key responsibilities have been assigned to JCCTs:

i. Identify emerging cybercrime hotspots and modus operandi to take pre-emptive action and share with all stake holders.
ii. Facilitate the joint identification, prioritization, preparation and initiation of multi-jurisdictional action against cybercrime.
iii. Coordinate with all State/Central Nodal agencies, IT, Telecom and Financial Intermediaries and banks for improving response to cybercrime
iv. Share information related to arrests made in cases of cybercrime for identifying and acting upon interstate linkages.

v. Review and update the status of action taken on interstate linkages and crime alerts shared by I4C, MHA and other States/UTs.

vi. Sharing of forensic resources and exchange best practices on countering cybercrime amongst the members of JCCT.

Further, Cyber Fraud Mitigation Centre (CFMC) has been established at Indian cybercrime Coordination Centre (14C) in New Delhi with representatives of major banks, Financial Intermediaries, Payment Aggregators, Telecom Service Providers, IT Intermediaries and States/UTs Law Enforcement Agencies (LEAs). They will work together for immediate action and seamless cooperation to tackle online financial crimes. CFMC will serve as an example of "Cooperative Federalism" in law enforcement.

Samanvay Platform (Joint Cybercrime Investigation Facilitation System), which is a web-based module that will act as a one stop portal for data repository of cybercrime, data sharing, crime mapping, data analytics, cooperation and coordination platform for Law Enforcement Agencies across the country has also been launched.

The government has also designed a 'Cyber Commandos' Program. Under this program a special wing of trained 'Cyber Commandos' in States/UTs and Central Police Organizations (CPOs) will be established to counter threats of cyber security landscape in the country. Trained Cyber Commandos will assist States/UTs and Central Agencies in securing the digital space.

Further, a Suspect Registry of various identifiers is being created based on National Cybercrime Reporting Portal (NCRP), in collaboration with banks and financial intermediaries for strengthening fraud risk management capabilities of financial ecosystem

**[Ministry of Finance (Department of Financial Services), O.M. No. e.F.no.CSFT-01/4/2023, Dated 18th October, 2024]**

## Recommendation Serial No.4(ii) Paragraph No.1

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.

## Reply of the Government

Ministry of Home affairs has received recommendations from the States proposing amendments in the IT Act, 2000 which have been shared with MeitY, the administrative Ministryfor taking appropriate action.

**[Ministry of Finance (Department of Financial Services),**
**O.M. No. e.F.no.CSFT-01/4/2023, Dated 18th October, 2024]**

## Recommendation Serial No.4(iii) Paragraph No.1

The Committee note a significant variation in the number of cybercrime 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:

a) *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.

b) *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.

c) *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.

d) *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.

e) *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.

f) *Time-bound Redressal/Resolution:* The designated cybercrime 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.

g) 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**.**

**Reply of the Government**

Ministry of Home Affairs has established a National Cybercrime Helpline number 1930 for immediate reporting of cybercrimes. This Helpline number is operational in all the States/UTs of the country and is mostly used for reporting of financial cybercrimes. So far, in 27 States/UTs helpline number call centre are functional 24x7. The complaints reported through helpline number 1930 lands on the Citizen Financial Cyber Frauds Reporting and Management System of National Cybercrime Reporting Portal. More than 250 banks, wallets and other financial intermediaries are on boarded on the platform to take immediate action on the complaints related to financial cyber frauds reported on the portal.

Efforts are being made to popularize this helpline number amongst the citizen for immediate reporting of cybercrime and awareness campaign are being run by various stakeholders in this regard. Due to awareness amongst the citizen, daily complaints on portal has raised up to 4,500 complaints per day in August 2023 in comparison of 1,500 complaints per day in January 2022. So far, traffic of 14.15 crore views has been received on the portal.I4C is also working in capacity building of State/UT LEAs, Public Prosecutors, Judicial Officers through workshops and peer learning sessions every week. CyTrain portal has also been developed for online training of LEAs in various aspects of cybercrime. National Cyber Crime Threat Analytics Unit (TAU) of I4C is working to achieve the following objectives:

i. Developing actionable intelligence for Cybercrime Investigation Units of various LEAs

i. Identifying cyber threats – who is involved and where are they located?

ii. Mitigating the threats through disruptive and proactive law enforcement action

iii. Aid in investigation through aid in seizing evidence/assets/funds, dismantling cyber criminal's infrastructure and making arrests

iv. Identify usage of cyber space by organized criminal groups and terrorists and to develop actionable information about them.

Further following actions are being proposed to be taken

i. Instructions are to be issued to all major commercial banks for stationing an appropriate bank representative at I4C in New Delhi for proper appreciation of the issues involved and carry out real time interventions and required coordination. (Several countries including China, USA and Singapore have similar arrangements).

ii. Mechanism to improve the delayed/lack response of banks on lawful Notices/ requests from LEAs and achieve a Service Level Agreement between Banks and LEAs for responding to lawful Notices

iii. Developing a mechanism to "give temporary custody of the money" marked as lien to original owner under Section 102 (3) CrPC without a court order.

iv. Put in place State level coordinators for each major Bank, so that expeditious action is taken on customer complaints and all coordination issues are addressed locally.

v. Strengthen the campaign on prevention of cybercrime through various banks and financial intermediaries.

I4C, MHA has constituted seven Joint Cybercrime Coordination Teams comprising various States/UTs based on the hotspots in the country. 7 Joint Cyber Coordination Teams have been formed at Mewat, Jamtara, Ahmedabad, Hyderabad, Chandigarh, Visakhapatnam and Guwahati. I4C has also appointed nodal officers for each States. To have effective coordination among JCCTs, following key responsibilities have been assigned to JCCTs:

i. Identify emerging cybercrime hotspots and modus operandi to take pre-emptive action and share with all stake holders.

ii. Facilitate the joint identification, prioritization, preparation and initiation of multi-jurisdictional action against cybercrime.

iii. Coordinate with all State/Central Nodal agencies, IT, Telecom and Financial Intermediaries and banks for improving response to cybercrime

iv. Share information related to arrests made in cases of cybercrime for identifying and acting upon interstate linkages.

v. Review and update the status of action taken on interstate linkages and crime alerts shared by I4C, MHA and other States/UTs.

vi. Sharing of forensic resources and exchange best practices on countering cybercrime amongst the members of JCCT.

Further, Cyber Fraud Mitigation Centre (CFMC) has been established at Indian cybercrime Coordination Centre (14C) in New Delhi with representatives of major banks, Financial Intermediaries, Payment Aggregators, Telecom Service Providers, IT Intermediaries and States/UTs Law Enforcement Agencies (LEAs). They will work together for immediate action and seamless cooperation to tackle online financial crimes. CFMC will serve as an example of "Cooperative Federalism" in law enforcement.

Samanvay Platform (Joint Cybercrime Investigation Facilitation System), which is a web-based module that will act as a one stop portal for data repository of cybercrime, data sharing, crime mapping, data analytics, cooperation and coordination platform for Law Enforcement Agencies across the country has also been launched.

The government has also designed a 'Cyber Commandos' Program. Under this program a special wing of trained 'Cyber Commandos' in States/UTs and Central Police Organizations (CPOs) will be established to counter threats of cyber security landscape in

the country. Trained Cyber Commandos will assist States/UTs and Central Agencies in securing the digital space.

Further, a Suspect Registry of various identifiers is being created based on National Cybercrime Reporting Portal (NCRP), in collaboration with banks and financial intermediaries for strengthening fraud risk management capabilities of financial ecosystem

**[Ministry of Finance (Department of Financial Services), O.M. No. e.F.no.CSFT-01/4/2023, Dated 18th October, 2024]**

## Recommendation Serial No.4(iv) Paragraph No.1

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.

## Reply of the Government

Citizen Financial Cyber Frauds Report and Management System has integrated LEAs and financial intermediaries such as banks, wallets, Payment Aggregators, Payment Gateways, ecommerce platforms etc. to work in tandem on the complaints reported by

citizen. Efforts are being made to develop the module as a centralized mechanism for information sharing related to financial cybercrime by the all concerned stakeholders.

We concur with the need to have a centralised mechanism for information exchange on cyber frauds. Currently, there is a Standing Committee being convened by I4C (under MHA) which is undertaking this task in an effective manner. As regards streamlined investigations, it is understood that the proposed Digital India Act will holistically look at this aspect.

An "Omnibus Framework for recognising Self-Regulatory Organisations (SROs) for Regulated Entities (REs) of the Reserve Bank of India" was issued by RBI on March 21, 2024. Subsequently, an application has been received from one entity for operating as SRO of Payment System Operators and the same is under scrutiny.

a. Reserve Bank has issued an “Omnibus Framework for recognition of Self-Regulatory Organisations for Regulated Entities of the Bank” vide notification dated March 21, 2024, after undertaking necessary public consultation. The omnibus framework contains broad parameters viz., objectives, responsibilities, eligibility criteria, governance standards, application process and other basic conditions for grant of recognition, which will be common for any SRO proposed to be recognized by the Reserve Bank. Other sector-specific guidelines like number of SROs, membership, etc., shall be issued separately by the respective departments of the Reserve Bank wherever a sectoral SRO is intended to be set up. The recognised SROs for Regulated Entities (REs) of the Reserve Bank are expected to develop necessary standards/ code of conduct to improve the compliance culture in the REs to which they are catering and provide necessary inputs to the regulator for appropriate policy intervention.

b. To encourage self-regulation in the FinTech sector, RBI released a Framework for Recognising Self-Regulatory Organisation(s) for FinTech Sector' (SRO-FT framework) in May 2024.The framework covers the operational characteristics of the SROs, their eligibility and membership criteria, functions and responsibilities, Governance and Management

**[Ministry of Finance (Department of Financial Services), O.M. No. e.F.no.CSFT-01/4/2023, Dated 18th October, 2024]**

**Recommendation Serial No.5(i) Paragraph No.1**

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.

**Reply of the Government**

Government has taken the following measures to strengthen cyber security defences: Some of Cyber Security Certification activities performed by STQC, attached office of MeitY:

(a) *Common Criteria Certification* – Common Criteria for Information Technology Security Evaluation (referred to as Common Criteria or CC) is an international standard (ISO/IEC 15408) for IT security. STQC being a certification body have common criteria recognition arrangement with other countries including Japan, Australia, France, Canada, US etc. Standardization Testing and Quality

Certification (STQC) Directorate, MeitY has setup Common Criteria Evaluation and Certification Lab at Kolkata, Delhi and Bangalore for security testing & validation of IT products up to Evaluation Assurance Level (EAL) 4.

(b) *Trusted Supply Chain Security Certification* - This scheme formulated as perNational Electronics Policy 2019 for Securing National Critical Information Infrastructure to evaluate supply chain risks, may include insertion of counterfeits, unauthorized production, tampering, theft, insertion of malicious software and hardware, poor manufacturing and development practices in the ICT supply chain.

(c) *Information Security Management System (ISMS) (ISO 27001)* - STQC operates third party ISMS certification scheme based on the ISO/IEC 27001 standard and offers ISMS Certification services since November 2001 to its valued clients in India and abroad.

(d) *Biometric Device Certification Scheme (BDCS)* - STQC is the only Conformity Assessment body to verify the compliances of Bio-metric Devices for Aadhar ecosystem for protection of citizen's Personal Identification i.e. Biometrics (Finger Print & Iris). STQC has certified Bio-metric Devices which are being used for Aadhar based Payments, Public Distribution System, eKYC, Authentication, Enrollment, applications like Jeevan Praman, Point of Sale, Aadhar based attendance etc. Presently, testing facilities are available at three locations in India at Delhi, Bangalore & Mohali. New facility for testing is being created at Kolkata.

Cyber Security testing/ evaluation/ audit activities performed by STQC

(a) Web Application Security as per Open Web application security project (OWASP) Top 10

(b) Mobile Application Security as per OWASP Mobile Application Security Verification Standard(MASVS)

(c) Vulnerability Assessment/Penetration Testing (VA/PT)

(d) End Point Devices Security (based on IoT checklist)

(e) Thick Client Security Testing

(f) Security Design Review

(g) Security Architecture Review

(h) Security Process Audit

(i) Cloud Security Audit

(j) Code Review

(k) Block chain-based system assessment

(l) Application programming interface(API) security

Further,RBI have advised banks to refer to globally accepted standards/ practices in various areas such as VA/ PT (OWASP), Business Continuity Plan/ Policy (ISO 22301), payment card security (applicable PCI Standards), etc. RBI have information exchange mechanism through MoUs with several central banks (MAS, ECB, PRA, HKMA, etc.). RBI exchange information on the regulatory/ supervisory initiatives on need basis.

RBI is a member of various Working groups constituted by FSB relating to Cyber Lexicon, effective practices for cyber incident response and recovery and cyber incident reporting. RBI is also associated with BRICS Rapid Information Security Channel (BRICS).I4C, MHA also shares information including negative repository collated from various sources with RBI to feed into cyber risk profiling for the benefit of banks and other financial institutions.

**[Ministry of Finance (Department of Financial Services), O.M. No. e.F.no.CSFT-01/4/2023, Dated 18th October, 2024]**

**Recommendation Serial No.5(ii) Paragraph No.1**

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.

**Reply of the Government**

The Indian Computer Emergency Response Team (CERT-In) has been issuing alerts, advisories and vulnerability Notes regarding latest cyber threats/vulnerabilities and countermeasures to protect computers, networks and data on an ongoing basis. CERT-In conducts detailed analysis of the incidents observed in the Indian financial sector and identifies the tactics, techniques and procedures used by the threat actors. IOCs (Indicator of Compromise) like Command and Control (C2) IP addresses, file types, DNS, hashes etc. thus identified are included in these CERT-In advisories. Advisories are also shared with regulators such as RBI, SEBI and IRDAI for coordinated dissemination to organizations in respective sectors.

CSIRT-Fin/CERT-In has also issued a structured report on the State of Cyber Landscape in the Indian Financial sector in December 2022 and communicated it to all regulators including RBI, DEA, DFS etc. This report presented an overview of the evolving cyber threats targeting the financial sector in India. It mentioned prominent cyber incidents having systemic risks like large scale phishing attacks, ransomware attacks, cyber frauds by malicious actors etc. and incidents related to cyber resiliency in the financial sector like ATM frauds, incidents targeting Payment Service Providers etc. It also discussed about recent trends and patterns in data breach and insider threat incidents. The report highlighted the gaps observed during analysis of these incidents and actions taken by CSIRT-Fin/CERT-In to strengthen cyber security in the financial sector. It also provided actionable recommendations and best / next practices for the financial regulators and its regulated entities.

**[Ministry of Finance (Department of Financial Services),**
**O.M. No. e.F.no.CSFT-01/4/2023, Dated 18th October, 2024]**

## CHAPTER III

## OBSERVATIONS/RECOMMENDATIONS WHICH THE COMMITTEE DO NOT DESIRE TO PURSUE IN VIEW OF THE GOVERNMENT'S REPLIES

**-NIL-**

## CHAPTER IV

## OBSERVATIONS/RECOMMENDATIONS IN RESPECT OF WHICH REPLIES OF THE GOVERNMENT HAVE NOT BEEN ACCEPTED BY THE COMMITTEE

### Recommendation Serial No.2(i) Paragraph No.1

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.

### Reply of the Government

Ministry of Home Affairs (MHA) has informed that there are various Ministries and agencies in the country for strengthening the Cyber security apparatus and securing the cyber space of the country.MHA is responsible for information security policy formulation and administers the Official Secrets Act. MHA currently performs coordination activities on regular basis related to identifying cyber security and cybercrime related issues.

National Cyber Security Coordinator (NCSC), Ministry of Electronics and Information Technology (MeitY), Indian Computer Emergency Response Team (CERT-

In), National Critical Information Infrastructure Protection Centre (NCIIPC), I4C Department of Financial Services (DFS), Reserve Bank of India (RBI), etc., are the major stakeholders responsible for monitoring regulation compliance.

The cyber space is vast and warrants a differentiated approach based on the digital depth of an entity, its interconnectedness with the payment systems and the systemic risk each entity poses. RBI is of the view that intensity and scope of regulations would vary depending upon the nature of business of the entities under each of the regulators and there may be a need for a differentiated approach from the perspective of their systemic importance. Some of the cyber risks for the entities in financial sector may, however, be common and a mechanism for coordination and cooperation among the financial sector regulators is already put in place as part of Inter Regulatory forum under FSDC where RBI engages with other financial regulators for sharing of best practices in this regard.

In order to provide focussed attention on IT related matters, RBI had set up a Cyber Security and IT Risk (CSITE) Group within its Department of Supervision in 2015. Cyber Security framework was put in place by RBI for banks in June 2016 and appropriate regulatory and supervisory mechanism has been in place since then to take care of regulation and supervision of the REs from cyber security perspective. The banking sector entities have achieved reasonable level of cyber maturity now.

While progressive measures were being taken to enhance cyber security posture of the UCB sector, they have not been able to enhance their cyber preparedness commensurately with the growth in digital payments during covid period. Appropriate steps are being taken to address cyber risks for the UCB sector in a non-disruptive manner and with a risk-based approach.

In a similar manner, dedicated divisions have been set up in other financial sector regulators such as SEBI, IRDAI, and PFRDA as well for regulating and supervising the entities in their respective jurisdiction.

MHA is of the view that existing authorities may be empowered with legal powers for better regulation and protection of cyber space and for acting on cybercrime. National Cyber Coordination Centre (NCCC) has been established with an aim 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. The domain of NCCC is to monitor internet traffic data as well as proactive monitoring and analysis of cyber security threats.

**[Ministry of Finance (Department of Financial Services),**
**O.M. No. e.F.no.CSFT-01/4/2023, Dated 18th October, 2024]**

***(For Comments of the Committee, please refer Para No. 7 of Chapter I)***

**Recommendation Serial No.2(ii) Paragraph No.1**

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 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).

a) Firstly, ecosystem participants should prioritize investments in robust cyber security infrastructure, including advanced threat detection systems and secure data storage practices.
b) Secondly, comprehensive training programs should be implemented to raise awareness among employees and customers regarding cyber threats, phishing attacks, and best security practices.
c) 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.

**Reply of the Government**

Given the large number of Urban Cooperative Banks (UCBs), their unique nature and constraints faced by them regarding availability of adequate financial resources and skilled manpower, implementation of cyber security controls was aimed to be achieved progressively, depending on their digital depth and their inter-connection with digital payment ecosystem. Graded Cyber Security framework issued in December 2019

required UCBs, among other things, to implement Anti-malware protection for Endpoints, Servers, Network Devices, etc.

To enhance the cyber security posture of the Urban Co-operative banking sector against evolving IT and cyber threat environment through a five-pillared strategic approach GUARD., viz., - Governance Oversight, Utilize Technology Investment, Appropriate Regulation and Supervision, Robust Collaboration and Developing necessary IT, cyber security skills set, a Technology Vision Document was issued in 2020.

Digitalisation of the payments systems gathered pace in the UCB sector during Covid period while this sector was still in the process of implementing baseline cyber security controls. The UCBs could not enhance IT controls commensurately during this period, leaving them vulnerable to cyber-attacks. Drawing from the learnings of regulating and supervising the banking sector, RBI has been progressively strengthening the regulatory and supervisory processes for the UCBs. Efforts are being made holistically to address the risks for this sector. The existing guidelines applicable to UCBs advise an annual IS audit for all UCBs. Further, the long form audit report (LFAR) applicable to UCBs also prescribe key areas related to IT to be observed by the Statutory auditors of the bank.

RBI has been progressively enhancing the coverage of IT Examinations of the UCBs, both directly and through CERT In empanelled auditors. RBI has also been engaged in capacity building efforts in this sector. A Handbook on controls critical for the CBS ecosystem in the UCBs was prepared and provided to them recently.

For handholding UCBs in improving their cyber security posture through capacity building, a comprehensive set of training programmes tailor-made for UCBs was designed in collaboration with College of Agricultural Banking (CAB), Pune. This initiative named Mission ‘AVTU’ (Awareness Vriddhi and Training for the UCBs) was rolled out in the

month of August 2021.The interests of this sector would be better served by setting up shared IT infrastructure services, like a community cloud with sound IT/Cyber security governance processes. The setting up of an Umbrella Organisation (UO) for UCBs is under process which, apart from extending liquidity and capital support to its member UCBs, is expected to set up Information and Technology (IT) infrastructure for shared use of members to enable them to widen their range of services in the wake of advances in information and communication technology at a relatively lower cost. Separately, RBI is also studying the feasibility of setting up shared cloud services for the banking sector with adequate security controls, which may be very useful for UCBs.

Further, NABARD has put forth a comprehensive cyber security framework for Rural Cooperative Banks (RCBs) as per the Ref. NO. NB. DoS. Pol. HO./3182 / J-1/2019-20, As per the framework, RCBs have been categorized into four levels based on their digital depth and interconnectedness to the payment systems landscape. RRBs are diligently following the cyber security framework issued by NABARD. They are also conducting the regular IS and cybersecurity audits through CERT In empanelled auditors to safeguard their information systems.

RBI has further informed that National Urban Co-operative Finance and Development Corporation Limited, a Non-Deposit taking NBFC has been set up as an Umbrella Organization (UO) for primary urban cooperative banks. The UO is expected to undertake, inter alia, the functions of consultancy services, capacity building, research, and development, setting up of IT infrastructure for use of UCBs to facilitate resource sharing. It is expected that the UO may also facilitate strengthening the cyber security posture of the UCBs.

A Gap Assessment Exercise by CERT-In empanelled auditors was conducted for a set of Level II (offering Internet and/or mobile banking) and Level III UCBs. Compliance status of these UCBs were closely monitored by RBI, and value based and time-based restrictions for

online fund transfer transactions (NEFT/RTGS) were placed on the outlier banks. Restrictions were relaxed based on the compliance status.

In order to ascertain the cyber security posture and readiness of Level-1 UCBs, a gap assessment exercise was initiated by RBI. Accordingly, '50' Level-1 UCBs were selected for this purpose and were advised to conduct a Gap assessment/ audit through an external CERT-In empanelled auditor. RBI circular on Cyber security framework for UCBs and relevant advisories issued by RBI form the scope of the audit. Post completion of audit, the reports submitted by UCBs will be reviewed for further action at bank's end to strengthen their cyber security controls.

**Recommendation Serial No.2(iii) Paragraph No.1**

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 defences 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.

**Reply of the Government**

The Cyber Security Framework issued by RBI in 2016 requires banks, among various other things, to periodically conduct vulnerability assessment and penetration testing exercises for all the critical systems (through professionally qualified teams), particularly those facing the internet. The vulnerabilities detected are required to be remedied promptly in terms of the bank's risk management/treatment framework so as to avoid exploitation of such vulnerabilities.

Given the sensitive nature of data held by banks and their systemic importance, Red Teaming exercise by security researchers/ companies engaged by SEs would be preferable to the open ethical hacking and this approach has been included in the Cyber Security Framework issued by RBI in 2016 to enable the banks to identify the vulnerabilities and the business risk and assess the efficacy of the defences and check the mitigating controls already in place by simulating the objectives and actions of an attacker.RBI has informed that Cyber Recon Phase 1 was taken up in 2022-2023. Phase 1 covered 40 entities. Comprehensive analytical reports highlighting vulnerabilities captured by the platform was put up to the top management periodically. Second phase of the project is being initiated to cover larger set of entities.

IDRBT (Institute for Development and Research in Banking Technology), an entity set up by the Reserve Bank of India, conducts cyber drill every quarters wherein all banks participate. Banks also actively participate in cyber drills conducted under the aegis of CERT-IN, etc.RBI conducts cyber reconnaissance, simulated phishing and table-top exercises which complement the supervisory processes in strengthening the cyber

security posture of the banks. CERT-In & RBI jointly conducted "G20 Cyber Security Exercise for Banking sector" on the 5th June 2023 in Mumbai for domestic & foreign banks to assess their preparedness and resilience in dealing with cyber security incidents & crisis.

The detailed After-Action Report (AAR) of the exercises was shared with all the financial sector regulators with a request to conduct sector-specific cyber security exercises & drills by themselves as well as by their REs with the support of CERT-In to enhance the preparedness of the sector to deal with cyber security incidents and crisis situations.

MHA has rolled out Cyber Crime Volunteer Framework as a part of cyber hygiene promotion to bring together citizens to contribute in the fight against cybercrime in the country and to assist State/UT LEAs in their endeavour to curb cyber crimes, as technical experts, and for reporting of content which is unlawful, as per provisions of law. Volunteers are registered in terms of due process (required to furnish ID proof, address proof, photograph etc) and their services are utilized by the respective State/UT Police Agencies, as per their requirement. The content reported by volunteers has to be verified and validated by the State/UT LEAs before/while taking appropriate action as per the existing provisions of law. Hon'ble Union Home Minister flagged off the 'Cyber Volunteer Squads' of seven Colleges/Universities during the G20 Conference "Crime and Security in the age of NFTs, AI and Metaverse" held on 13-14 July, 2023.

Hackathons: Smart India Hackathon (SIH) 2020 was organized by I4C in collaboration with AICTE(MHRD). 17 problem statements were conceptualized. Finals were held on 1-3 August, 2020. I4C, MHA participated in SIH 2022 held by AICTE on the theme Culture, Heritage, Cyber Security and Blockchain. I4C submitted three Problem statements. SIH 2022- Software edition concluded on 25-26 August 2022 and Hardware edition concluded on 25-29 August, 2022. I4C, MHA in collaboration with AICTE launched

“KAVACHA Hackathon” on 16.02.2023 at National Media Centre, New Delhi. Idea submission was closed on 2nd May 2023. A total of 4240 ideas have been submitted across 20 Problem Statements of I4C and BPR&D. Ten winners Teams were declared on 10 August, 2023 at North Block, MHA, New Delhi through Video Conferencing in the Grand Finale.

The existing cybersecurity frameworks and initiatives, such as Red Teaming exercises,cyber drills, reconnaissance, simulated phishing, table-top exercisesand the Cyber Crime Volunteer Framework, reflect the proactive approach to countering cyber threats. Engaging ethical hackers by CPA for identifying vulnerabilities and enhancing cybersecurity defences requires further deliberations as stated at recommendationserial Nno.2(i) paragraph No. It is also felt that further deliberation would be needed to establish a secure framework and ensure close monitoring of ethical hackers engagedby security agencies.

**Recommendation Serial No.2(iii) Paragraph No.2**

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.

**Reply of the Government**

Banks have already been mandated to designate a sufficiently senior level executive as the Chief Information Security Officer (CISO). CISO shall be responsible for bringing to the notice of the Board/ IT sub-committee of the Board about the vulnerabilities and cyber security risk, the bank is exposed to. The role and functions of CISO including details of reporting structure, having requisite technical expertise, adequate staffing in CISO's office, etc. have also been clearly specified by RBI. Effectiveness of roles of CISOs are assessed during IT examinations conducted by the RBI. Under the aegis of IDRBT, a CISO forum has been created. The forum meets every quarter to discuss emerging areas of cyber risks and share new learnings.

National Informatics Center (NIC) has proposed to have a Cyber Security and IT cell in critical/sensitive ministries. The Cyber Security cell will consist of the Dy.CISO of that Ministry/Department assisted by 5-6 cyber security experts/consultant to cater the Cyber Security need of the Ministry/Departments concerns.

**Recommendation Serial No.2(iv) Paragraph No.1 & 2**

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.

**Reply of the Government**

Indian Cybercrime Coordination Centre (I4C)-MHA has been regularly analyzing the digital lending apps both proactively and also on the basis of complaints reported on the National Cybercrime Reporting Portal. Based on these complaints, I4C team analyzes Apps on various parameters, and report such Apps to MeitY for blocking which are found suspicious. I4C also receives list of spurious Apps from the other stakeholders and after analysis I4C recommends suspicious Apps for blocking. Sofar, on the recommendation of I4C, around 162 Loan Apps have been blocked by the MeitY.

MeitY has also blocked certain loan lending apps under section 69A of the IT Act 2000. These applications were blocked because they attract the provision of section 69A. Further, MeitY enquired and advised Google for appropriate policy establishment for

lending apps. Towards it, Google updated the policy and reviewed the processes and onboarded the Fintech Association for Consumer Empowerment (FACE) to the Google Priority Flagger Program (GPFP) for fighting against scams and fraud in the personal loans space. With the help of LEA and other industry bodies (like FACE), Google has removed over 2200 DLAs from play store (2nd Sep 2022 to 1st Aug 2023).

While whitelisting framework of Loan Apps by Government agency would help weed out fraudulent or unscrupulous DLAs from the market, RBI digital lending guidelines protect borrowers from predatory lending practices and other illegal activities.

Till such time, such nodal agency is setup, Ministry of Finance, I4C, MHA, RBI, Ministry of Corporate Affairs, MeitY and DFS are working together to identify legal/ illegal apps at regular intervals to address the issue of Illegal DLAs.

RBI in the August 2024 Statement on Development and Regulatory Policies, has announced the creation of a public repository of digital lending apps (DLAs) which will aid the customers in verifying the association of a DLA with a Bank/ NBFC. The repository will be based on data submitted by the REs (without any intervention by RBI) directly to the repository and will get updated as and when the REs reports the details, i.e., addition of new DLAs or deletion of any existing DLA. The same will be operationalized shortly.

The Master Direction on Responsible Lending Conduct is under preparation, which shall include instructions on conduct related aspects on lending activities and shall be applicable to all lenders, including those engaged in digital lending.

**Recommendation Serial No.2(v) Paragraph No.1**

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 cybercrime. 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 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:

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

(b) 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.

**Reply of the Government**

Government policies and regulations are aimed at ensuring an Open, Safe & Trusted and Accountable Internet for its users. Government is fully cognizant and aware of the growing cyber security threats and attacks.

As per Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (“IT Rules”), an intermediary including a social media intermediary shall observe due diligence and cause its users not to host misinformation and/or information that impersonates another person under section 3(1)(b). Under Rule 3(1)(d), an intermediary, on whose computer resource the information is stored, hosted or published, upon receiving actual knowledge in the form of an order by a court of competent jurisdiction or on being notified by the Appropriate Government or its agency under clause (b) of sub-section (3) of section 79 of the Act, shall not host, store or publish any unlawful information, which is prohibited under any law for the time being in force in relation to the interest of the sovereignty and integrity of India; security of the State; friendly relations with foreign States; public order; decency or morality; in relation to contempt of court; defamation; incitement to an offence relating to the above, or any information which is prohibited under any law for the time being in force.

Further, failure on the part of an intermediary/platform to observe due diligence and/or to comply with the provisions of the IT Act and Rules in case of misinformation and/or grievance redressal mechanism, will amount to non-compliance with the IT Rules and could result in the concerned intermediary/platform automatically losing the exemption provided under Section 79(1) of the IT Act, in accordance with Section 79(2)(c) of the IT Act. Moreover, Intermediaries have also been advised that users must be made aware of the various penal provisions of the Indian Penal Code, 1860, the IT Act and such other laws that may be attracted in case of violation of Rule 3(1)(b).

Furthermore, sub-section (1) of Section 69A of the IT Act, 2000, the Central Government may direct any agency of the Government or intermediary to block public access to any information generated, transmitted, received, stored or hosted in any computer resource only under following circumstances involving issues related to the interest of sovereignty and integrity of India, defence of India, security of the state, friendly

relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to the above. Sub-section (2) of Section 69A of the IT Act provides for a system of checks and balances in the form of procedures and safeguards concerning the blocking of online information/sources from access to the public. The detailed process for blocking websites/URLs under Section 69A of the IT Act has been provided under the Information Technology (Procedure and Safeguards for Blocking for Access of Information for Public) Rules, 2009 (hereinafter referred to as 'IT (Blocking) Rules, 2009/Blocking Rules').

Also, MeitY has issued recommendations and advisories from time to time on the efforts that intermediaries/platforms need to make to prevent hosting of misinformation.

**Recommendation Serial No.2(vi) Paragraph No.1 & 2**

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

**Reply of the Government**

In this connection, it is stated that Financial intelligence Unit (FIU-IND) was set up as the central national agency responsible for receiving, processing, analysing and disseminating information relating to suspect financial transactions. Further, FIU-IND is responsible for coordinating and strengthening efforts of national and international intelligence, investigation and enforcement agencies in pursuing the global efforts against money laundering, terrorist financing and related crimes. With respect to the establishment of a Central Negative Registry (CNR), FIU-IND would be able to share inputs for creation and updating of CNR on the basis of information received.

MHA has informed that based on the complaint reported on the National Cybercrime Reporting Portal and information received from various stakeholders, I4C compiles and maintains a negative repository of suspected Bank account numbers, Mobile numbers, UPI IDs, etc., and share them with concerned entities to take necessary action. Such information needs to be taken in to account while performing due diligence of customers by the banks and financial institutions. I4C also maintains the repository of suspected URLs, websites and applications and shares it with all concerned stakeholders. The National Cybercrime Reporting Portal also facilitates LEAs to upload the mobile numbers for blocking by the concerned Telecom Service Providers (TSPs). So far 1.96 lakh mobile numbers have been blocked. I4C, MHA has requested RBI to take proactive steps for the integration of NCRP database with that maintained by RBI of fraud and attempted fraud cases.

Further, The Reserve Bank has put in place Central Payments Fraud Information Registry(CPFIR) in March 2020. All payment frauds reported by customers or detected by banks and PPI Issuers are reported to CPFIR by supervised entities (banks, non-bank Prepaid Payment Instrument Issuers and non-bank Credit Card issuers). Under the Payments Vision 2025, an enhancement in CPFIR envisaged was creating a negative

database of fraudulent beneficiaries. The negative registry is envisaged to be created using the suspect / beneficiary information reported to CPFIR. Once the negative database is created it is envisaged to share the same with supervised entities that may use the information for appropriate risk management checks at their end.

Further, the honourable Supreme Court passed a judgement on Civil Appeal No. 7300 of 2022 in connection with "no opportunity of being heard is envisaged to borrowers before classifying their accounts as fraudulent". In view of the same, the legal aspects of sharing / using the information in negative registry may also need to be examined, as the same is proposed to be created based on information reported by the customer / detected by the reporting bank with no opportunity provided to the beneficiary.

Every customer on identification of a payment fraud reports the same to their bank / non-bank entity whose payment system / payment instrument was used to undertake the transaction. As CPFIR mandates reporting from banks / non-bank entities based on customer reported frauds in all payment systems, the information available in CPFIR is comprehensive and should be leveraged in the fight against cyber-crimes.

Further, MHA’s Citizen Financial Cyber Frauds Reporting and Management System (Helpline), developed as part of National Cybercrime Reporting Portal, provides an integrated platform where all concerned stakeholders like Law Enforcement Agencies (LEAs), Banks, Financial intermediaries, Payment wallets, etc., work in tandem to ensure that quick, decisive, and system-based effective action is taken to prevent the flow of money from innocent citizens to the fraudsters. However, not all frauds are reported in the Helpline.

Incidentally, RBI’s Payment Vision 2025 provides that the Reserve Bank shall engage with the industry and Government to examine the feasibility of integrating CPFIR

with other fraud reporting solutions to ensure that a single comprehensive platform is made available for real-time reporting and resolution of payment frauds in the country.

RBI has informed that While the payment ecosystem (banks, NPCI, card networks, payment aggregators, and payment apps) take various measures on an ongoing basis to protect customers from such frauds, a need was felt for network-level intelligence and real-time data sharing across payment systems. Hence, RBI had recently proposed to set up a Digital Payments Intelligence Platform which will harness advanced technologies to mitigate payment fraud risks. To take this initiative forward, a committee was constituted to examine the various aspects of setting up this Platform. The committee's recommendations are under examination by RBI.

**[Ministry of Finance (Department of Financial Services),**
**O.M. No. e.F.no.CSFT-01/4/2023, Dated 18th October, 2024]**

***(For Comments of the Committee, please refer Para No. 10 of Chapter I)***

**Recommendation Serial No.2(vii) Paragraph No.1& 2**

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.

**Reply of the Government**

Government is cognizant about the impact of emerging technologies such as Quantum Computing, AI/Chatbot, etc on cyber security. Government has taken the following initiatives:

(a) A project entitled “Development of Secure Post Quantum Public Key Infrastructure” has been initiated with the objective of developing Post Quantum Crypto Token by implementing CRYSTALS-Dilithium (for Digital Signature Scheme) and CRYSTALS-Kyber (for Key Encapsulation Mechanism) algorithms. These algorithms have been chosen by the National Institute of Standards and Technology (NIST) as winners in the competition for Post Quantum Cryptography (PQC) Standardization, and will be implemented on Hardware (FPGA) platforms and integrated with Post Quantum Crypto token. The Certificate Authority suite will be enabled with Post Quantum Crypto Token. The developed solution will enhance the security of the Public Key Infrastructure against both classical and quantum computers.

(b) *India AI:*Programme is envisioned as an umbrella programme by the Ministry of Electronics and Information Technology (MeitY) for leveraging transformative technologies to foster inclusion, innovation, and adoption for social impact. Pillars of India AI include Data for AI, Skilling, AI Ethics and Governance, Compute, AI Research and Development, National Centre for AI, among others.

(c) *National Program on Artificial Intelligence:*To actualize the vision of India AI, MeitY has undertaken the implementation of the "National Program on Artificial Intelligence" (NPAI). NPAI would encompass four broad pillars of the India AI program, which include Skilling in AI, Responsible AI, Data Management Office and the National Centre on AI.

Further, I4C had commissioned a study with IIT Kanpur on the possibilities of abuse of new and emerging technologies. The reports have flagged many related issues. Relevant extracts have been circulated to the stakeholders concerned. I4C is also running various programmes for cyber awareness & cyber hygiene amongst the citizen through Social Media platforms, FM/Radios, Railway stations, Airports, etc. Efforts are being made to reach the people at lowest level and at the remotest places in the country. With the help of law enforcement agencies across the country, I4C is trying to reach citizens in their regional languages to make them understand better and encourage general public to follow the guidelines. Cyber Volunteer Framework has also been developed to enable the participation of citizens in tackling of the menace of cybercrime.

**Recommendation Serial No.3(i) Paragraph No.1**

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.

**Reply of the Government**

RBI, vide circular dated July 06, 2017 on 'Limited liability of customers in unauthorized electronic banking transactions' addressed to SCBs, Small finance banks and Payment banks and circular dated December 14, 2017 on 'Limiting Liability of Customers of Co-operative Banks in Unauthorised Electronic Banking Transactions' addressed to all cooperative banks has issued the following guidelines:

*Reporting of unauthorised transactions by customers to banks:* Banks must ask their customers to mandatorily register for SMS alerts and wherever available register for e-mail alerts, for electronic banking transactions. The SMS alerts shall mandatorily be sent to the customers, while email alerts may be sent, wherever registered. The customers must be advised to notify their bank of any unauthorised electronic banking transaction at the earliest after the occurrence of such transaction, and informed that the longer the time taken to notify the bank, the higher will be the risk of loss to the bank/ customer. To facilitate this, banks must 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 unauthorised transactions that have taken place and/ or loss or theft of payment instrument such as card, etc. Banks shall also enable customers to instantly respond by "Reply" to the SMS and e-mail alerts and the customers should not be required to search for a web page or an e-mail address to notify the objection, if any. Further, a direct link for lodging the complaints, with specific option to report unauthorised electronic transactions shall be provided by banks on home page of their website. The loss/ fraud reporting system shall also ensure that immediate response (including auto response) is sent to the customers acknowledging the complaint along with the registered complaint number. The

communication systems used by banks to send alerts and receive their responses thereto must record the time and date of delivery of the message and receipt of customer's response, if any, to them. This shall be important in determining the extent of a customer's liability. The banks may not offer facility of electronic transactions, other than ATM cash withdrawals, to customers who do not provide mobile numbers to the bank. On receipt of report of an unauthorised transaction from the customer, banks must take immediate steps to prevent further unauthorised transactions in the account".

*Reversal timeline for Zero Liability/ Limited Liability of customer:* 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 off any customer liability in case of unauthorised electronic banking transactions even in cases of customer negligence. The credit shall be value dated to be as of the date of the unauthorised transaction. Further, banks shall ensure that:

(i) 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 from the date of receipt of the complaint, and the customer is compensated as per provisions of paragraph 6 to 9 of the circular;

(ii) where it is unable to resolve the complaint or determine the customer liability, if any, within 90 days, the compensation as prescribed in paragraphs 6 to 9 is paid to the customer; and

(iii) in case of debit card/ bank account, the customer does not suffer loss of interest, and in case of credit card, the customer does not bear any additional burden of interest.

*Burden of Proof :*The burden of proving customer liability in case of unauthorised electronic banking transactions shall lie on the bank." The Reserve Bank has, vide circular dated September 20, 2019, put in place a framework on Turn Around Time (TAT) for resolution of failed transactions and compensation framework across all authorised payment systems. This was expected to increase customer confidence and bring in uniformity in processing of the failed transactions. The operators and participants of authorised payment systems have been advised that the TAT prescribed in the circular is the outer limit for resolution of failed transactions; and they shall endeavour towards quicker resolution of such failed transactions. Further, 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. Customers who do not get the benefit of redress of the failure as defined in the TAT, can register a complaint with the Reserve Bank - Integrated Ombudsman Scheme, 2021 (as amended from time to time).

RBI has issued directions vide email dated September 30, 2022 to Regulated Entities to put in place a dedicated team with enough nodal officers available to respond to LEAs on a 24*7 basis to provide near zero delay and reiterated the importance of having sufficient number of empowered and skilled resources, also at state level vide advisory by email dated February 9, 2024. Directions for deployment of dedicated personnel from the RE at the Financial Crime Command Centre of I4C, New Delhi was also issued to select REs vide advisory of even date, emphasizing the supportive role that Regulated Entities must play in cybercrime incidents.

To understand the needs of the Law Enforcement Agencies (LEAs) and to exchange ideas on the subject, a Workshop with LEAs was held at RBI on April 16, 2024.

RBI is in the final stages of issuing a circular on 'Prevention of financial frauds perpetrated using voice calls and SMS' to all its Regulated Entities to comply with TRAI guidelines on making marketing / transaction calls for particular series of numbers, register

their SMS headers and templates etc. The circular also emphasises the Regulated Entities clean their customer database based on Mobile Number Revocation List (MNRL) published by DoT.

In relation to reported cases of alleged cybercrime frauds, it is observed that despite the efforts of stakeholders, the recovery rate of defrauded amount is not very encouraging. Considering the same, the Reserve Bank's Payments Vision 2025 provides for conducting a study on scope / feasibility of creation of Digital Payments Protection Fund (DPPF). Immediately reimbursing a customer without following due process as laid out in the payment system's guideline may create perverse incentives wherein the customer may report even a genuine transaction as fraudulent and claim the amount.

**[Ministry of Finance (Department of Financial Services),**
**O.M. No. e.F.no.CSFT-01/4/2023, Dated 18th October, 2024]**

***(For Comments of the Committee, please refer Para No. 13 of Chapter I)***

**Recommendation Serial No.3(ii) Paragraph No.1**

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.

**Reply of the Government**

RBI *vide* Master Direction on Digital Payment Security Controls of RBI, banks have been advised that alerts (like SMS, e-mail, etc.) should be applied in respect of all payment transactions (including debits and credits), creation of new account linkages (addition/ modification/ deletion of beneficiaries), changing account details or revision to fund transfer limits.

It is also submitted that under the provisions of the Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions, banks must ask their customers to mandatorily register for SMS alerts and wherever available register for e-mail alerts, for electronic banking transactions. The SMS alerts shall mandatorily be sent to the customers, while email alerts may be sent, wherever registered. In addition, the time period for determining customer liability in case of unauthorised transaction starts from the time the customer receives the SMS notification, to account for telecom network related issues.

Reserve Bank of India has also issued instructions vide its circulars dated February 18, 2009, March 29, 2011 and August 27, 2021 that Payment System Providers shall 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.

TRAI has apprised that Access Service Providers have built resilient and stable systems that ensure that all SMSs are delivered to the consumers. Under TCCCPR-2018, there is flexibility available with the Senders that for sending the commercial communications over the networks of Access Service Providers, the Senders can either deal directly with the Access Service Providers or opt to outsource this exercise to registered telemarketers (RTMs)and use their communication platform. RBI may encourage Banks/ other financial institutions to reduce number of RTMs in the chain

between the Banks/ other financial institutions and Access Service Providers or preferably establish direct connectivity with the Access Service Providers.

DOT has launched an online Digital Intelligence Platform (DIP) for sharing of telecom misuse related information and list of disconnected numbers along with reasonswith the stakeholders for prevention of cyber-crime and financial frauds. At present TSPs, DOT field Units, 460 banks and financial institutions, RBI, 30 State/UT Police, MHA 14C, NIA, FIU, UIDAI, GSTN etc. have on-boarded the platform.

**[Ministry of Finance (Department of Financial Services),**
**O.M. No. e.F.no.CSFT-01/4/2023, Dated 18th October, 2024]**

***(For Comments of the Committee, please refer Para No. 16 of Chapter I)***

**Recommendation Serial No.3(iii) Paragraph No.1**

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.

**Reply of the Government**

It is submitted that for various payment methods including UPI, mobile payments, card payments, prepaid payment instrument, RBI has mandated the use of an Additional Factor of Authentication for every payment transaction irrespective of the value or mode or channel used. Separately, on successfully completing a transaction, a SMS is mandatorily sent informing the customer of the transaction undertaken.

**Recommendation Serial No.3(iv) Paragraph No.1, 2 & 3**

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 behaviour 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 behaviour 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 behaviour 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.

**Reply of the Government**

Government through MeitY is implementing Information Security Education and Awareness (ISEA) programme with the objective of capacity building in the area of Information Security, training and creation of mass Information Security awareness. The project is being implemented involving 52 academic and training institutions across the country through formal and non-formal courses.

MeitY conducts programmes to generate information security awareness. Specific books, videos and online materials are developed for children, parents and general users about information security, which are disseminated through portals such as www.infosecawareness.in and www.csk.gov.in.MeitY is running the 'Stay Safe Online' campaign as a part of India's G20 presidency to sensitize internet users about online cyber risk & safety measures and to promote safe online behaviour & best practices on cyber hygiene. MeitY is also observing 'Cyber JagrooktaDiwas' on the first Wednesday of every month since May 2022 onwards towards capacity building of Government employees and creating awareness for prevention of cybercrimes.

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

Further, following initiatives have been undertaken by RBI for creating public awareness such as:

A detailed framework for financial education has been formulated with a focus on consumer protection. The implementation of the framework is underway, including the intensified/ focused awareness campaigns 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.

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 and 2023, all 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 (RB-IOS), 2021, 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 and 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. These interactions have also been uploaded by media channels on social media platforms. The media briefings by Ombudsmen were rerun on October 02, 2022, for recall value.

A media interaction was addressed by the Executive Director and Chief General Manager of CEPD, RBI, at New Delhi Regional Office on August 29, 2022, covering various facilities of RBI under its Alternate Grievance Redress mechanism viz., RB-IOS, 2021, Centralised Receipt and Processing Centre (CRPC), Contact Centre (CC), the roles and responsibilities of the customers as well as measures (Do’s and Don’ts) for safeguarding them against digital/electronic frauds.

A "Nation-wide Intensive Awareness Programme" (NIAP) was carried out during November 1-30, 2022 by RBI in collaboration with the Regulated Entities (REs) of RBI. 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, 82,436 senior citizens participated in these activities. Focused drives were organised for around 22,125 recovery agents on fair practices and guidelines to be followed.

Financial Awareness booklets BE(A)WARE (available in English, Hindi and 11 regional languages) and Raju and the Forty Thieves (available in English, and seven regionallanguages) covering the modus operandi of frauds and the way to escape/ avoid getting trapped by fraudsters have been issued by RBI and placed on its Website for use by members of public and other stakeholders. These are also distributed in physical programmes conducted by Regional Offices of RBI Ombudsmen.

On a macro level various initiatives have been taken for creating public awareness 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;

(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;

(v) Nation-wide SMS campaigns on various consumer protection themes.

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.

Awareness is created by participation in major festivals/events such as Rath Yatra in Puri, Shining Maharashtra, etc. Regional offices were further advised to participate in similar campaigns in regional and state level.

To provide efficient and effective redress to victims of cyber frauds, common public are made aware of aspects such as Reserve Bank – Integrated Ombudsman Scheme, 2021 (RB-IOS), RBI’s circular on Limiting Liability of Customers in Unauthorised Electronic Banking Transactions through advertisements and campaigns.

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 RB-IOS, 2021. The RB-IOS, 2021 was launched by the Honourable Prime Minister on November 12, 2021. The launch ceremony was covered by national news and most media channels.

RBI set up the Centralised Receipt and Processing Centre (CRPC) on November 12, 2021 at RBI, Chandigarh, which also hosts 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 28, 2022 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. Also, the regulated entities covered under RB-IOS, 2021 are repeatedly sensitised on their roles & responsibilities towards customer education and awareness.

Reserve Bank of India (RBI) conducts, on an ongoing basis, 360-degree, multimedia channel / platform based public awareness campaigns under the tag of 'RBI Says' or 'RBI Kehta Hai' to create awareness among members of public about various digital payment initiatives that cover customer's safety, security and convenience.

Further, to create awareness about payment products and to disseminate information about safe digital banking, Regional Offices of RBI have also been conducting Electronic Banking Awareness and Training (e-BAAT) programmes across the country. The main thrust of a e-BAAT programme comprises i) Awareness about Digital Payment Products ii) Awareness about Frauds and Risk Mitigation iii) Awareness about grievance redressal. The target audience includes cross section of the society consisting of bank staff, customers, government officials, students, Self Help Groups, farmers, shopkeepers, traders, and the common man.

RBI has also launched a mission "Har Payment Digital" wherein various participants to ecosystem are contributing to create awareness about safe usage of digital payments under single campaign. Campaign such as "75 Digital Villages" and "Digital payment apnao, auron ko bhisikhao" were launched as part of it.

According to RBI's circular on Limited Liability of Customers in unauthorised electronic banking transactions, banks have been instructed to design systems and

procedures to make customers feel safe about such transactions. Moreover, banks have been instructed to put in place robust and dynamic fraud detection and prevention mechanism and a system of continually and repeatedly advising customers on how to protect themselves from electronic banking and payments related fraud.

In light of increasing instances of payment frauds, all authorised payment systems operators and participants were advised to undertake targeted multi-lingual campaigns by way of SMSs, advertisements in print and visual media, etc., to educate their users on safe and secure use of digital payments.

The importance of awareness on modus operandi of frauds and safety measures to be undertaken to the public in general and targeted awareness to Senior Citizens, differently abled in particular was emphasized to REs vide advisory dated September 30, 2022. The REs were also advised to organize Cyber Jaagrookta (Awareness) on the first Wednesday of every month.

A Press Release on RBI cautions against Fraudulent Activities in its name was issued on August 29, 2024 cautioning the members of public about impersonation frauds by unscrupulous elements using various methods to defraud members of the public by using the name of RBI.

RBI has further informed that “Digital Payment, Safe Payment” a new campaign through TV and print media has been included.

Consumer Education and Protection Department (CEPD), RBI is in the process of conducting a survey to assess the level of awareness on grievance redress mechanism in rural and semi urban centers. The survey would provide inputs on awareness gaps at the grass root level and the findings would help in customizing the awareness campaigns and conducting target / area specific awareness campaigns.

Regarding assessing the effectiveness of the consumer campaigns by RBI Regulated Entities, the Report of the Committee setup by RBI for Review of Customer ServiceStandards(https://www.rbi.org.in/Scripts/PublicationReportDetails.aspx?UrlPage=&ID=1232)in RBI Regulated Entities (REs) recommended that :

- The Reserve Bank may develop and publish a "Customer Service and Protection Index" with a view to capture, at the system level, the quality / standards of customer service and extent of customer protection in the REs through a single score. The Index may cover dimensions like adequacy of regulatory and institutional framework in place, customer experience, efficacy of grievance redress, under both Internal Grievance Redressal and Alternate Grievance Redressal, extent of customer education and awareness, etc.

Accordingly, RBI is in the process of developing a Consumer Protection Index with 'Consumer Education and Awareness' as a metric. Further, for awareness programmes impact assessment, we are also taking up surveys and complaint data analysis for designing and improving both grievance redress and awareness initiatives.

I4C has also requested all Ministries for Government of India and all States/UTs to celebrate "Cyber Jaagrookta Divas" on first Wednesday of every month for dissemination of Cyber Hygiene, along with a request to prepare an annual action plan.

I4C also took up the matter with UGC and accordingly UGC has released the syllabus for course content on Cyber Security for Undergraduate and Post Graduate levels on 6th October 2022, which may be taught in various colleges and universities across the country. Also, I4C has requested NCERT to include Cyber Hygiene in various classes in schools across the country. In addition, campaigns have been carried out to promote reach of I4C, National Cyber Crime Reporting Portal, Helpline No. 1930 to masses and reinforce the message of prevention of cybercrimes, which, inter-alia, includes:

i. The MHA has released basic and advanced manual on cyber hygiene for cyberspace and a newsletter Cyber Pravah on 03.01.2022 of the Indian Cyber crime Coordination Centre (I4C).

ii. Organized One day conference on 'Cyber Safety & National Security' at Vigyan Bhawan on 20th June, 2022 as part of the 'Azadi ka Amrit Mahotsav' with the theme 'साइबरअपराधसेआजादी, आजादीकाअमृतमहोत्सव'.

iii. A session on Information Security, Prevention of cybercrime and Cyber Security for Cyber Hygiene was organized by MHA with the Chief Information and Security Officer (CISO), of Ministries to Govt. of India.

iv. Published 'Handbook for adolescents/students on cyber safety'.

v. Published 'Information Security Best practices' for the benefit of Government Officials.

vi. Organized of Cyber Safety and Security Awareness weeks through C-DAC in association with Police Department in different States.

vii. States/UTs have also been requested to carry out publicity of helpline number and National Cyber Crime Reporting Portal i.e. https://www.cybercrime.gov.in so as to create mass awareness.

viii. Organized National Conference of Chief Information, Security Officers (CISOs) / Chief Risk Officers (CROs) and private experts etc. on 09.09.2021 & 31.08.2022 to discuss about critical sector risks, best practices in cyber security, emerging trends in cyber security etc and to bridge gap amongst corporate and LEAs.

ix. Organized National Conference with State/UT Nodal Officers to discuss various case studies on investigation on cybercrimes from various States/UTs for prevention of cybercrimes.

**Recommendation Serial No.3(v) Paragraph No.1**

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.

**Reply of the Government**

RBI has taken following measures for strengthening of Internal Grievance Redress mechanism at Regulated Entities:

*Internal Ombudsman at Regulated Entities*: The Reserve Bank has set up an Internal Ombudsman (IO) mechanism with a view to strengthen the internal grievance redressal system of RBI Regulated Entities (REs) and to ensure that the rejected, including partially rejected, complaints of the customers are vetted within the REs itself by an authority placed at the apex of the RE's grievance redressal mechanism to minimize the need for the customers toapproach other fora for redressal. The entities covered under the IO mechanism are:

- Scheduled commercial banks with 10 or more banking outlets,
- (Deposit-taking NBFCs (NBFCs-D) with 10 or more branches, Non-Deposit taking NBFCs (NBFCs-ND) with asset size of Rs.5,000 crore and above and having public customer interface,

- Non-bank System Participants who are issuers of Pre-paid Payment Instruments (PPIs) and have more than one crore outstanding PPIs and
- Credit Information Companies (CIC)

The IO Mechanism stipulates that the IO and the RE shall ensure that the final decision is communicated to the complainant within 30 days from the date of receipt of the complaint. The implementation of the IO Mechanism is monitored on a continuous basis.

*Strengthening of Grievance Redress Mechanism in Banks:*A circular dated January 27, 2021 was issued for strengthening the grievance redress mechanism in banks. The framework comprises of (i) enhanced disclosures on complaints, aimed at providing greater insight into the volume and nature of complaints received by the banks as also the quality and turnaround time of grievance redressal by banks; (ii) recovery of cost of redress of maintainable complaints from the banks against whom the number of maintainable complaints received in the Offices of RBI Ombudsmen are in excess of the respective bank's peer group averages; (iii) intensive review of the grievance redressal mechanism by RBI and (iv) regulatory and supervisory action including corrective actions for banks found deficient in redress of customer grievances.

*Alternate Grievance Redress (AGR) Mechanism:*The RB-IOS which integrated the three erstwhile Ombudsman Schemes for banks, NBFCs and Non-Bank System Participants and was launched on November 12, 2021 has made the Ombudsman mechanism simpler, efficient and more responsive. It brought in the 'One Nation One Ombudsman' approach under which there is no limitation of territorial jurisdictions for the customer. The RB-IOS has been extended to Non-Scheduled Primary Urban Co-operative banks holding deposits of Rs.50 crore and above and also to Credit Information Companies. The new scheme has also done away with the restrictive grounds of complaints and now covers all complaints against the REs relating to 'deficiency in service', other than the grounds explicitly excluded under the Scheme. RB-IOS is being

administered through 24 RBI Ombudsmen located at 20 Regional Offices of RBI. Complaints against entities not presently covered under the RB-IOS are redressed by the Consumer Education and Protection Cells located at 31 Regional Offices of RBI. A complainant whose grievance is not resolved within 30 days of lodgement or who is not satisfied with the resolution provided by the RE at the first resort can lodge his complaint to the RBI Ombudsman on a 24x7 web-based end to end automated CMS portal.Under the AGR mechanism, the REs are required to:

- Appoint a Principal Nodal Officer at their head office who shall not be a rank less than a General Manager or an officer of equivalent rank and shall be responsible for representing the RE and furnishing information on behalf of the RE in respect of complaints filed against them.
- The RE may appoint such other Nodal Officers to assist the Principal Nodal Officer as it may deem fit for operational efficiency.
- The RE shall display prominently for the benefit of their customers at their branches/places where the business is transacted, the name and contact details (Telephone/mobile number and E-mail ID) of the Principal Nodal Officer along with the details of the complaint lodging portal of the Ombudsman (https://cms.rbi.org.in).

The complainant can approach the RBI Ombudsman under Reserve Bank-Integrated Ombudsman Scheme if he has not received any response within 30 days or his complaint has been rejected/ partially rejected by the RE.

*Master Circular on Customer Service dated July 01, 2015*: The Master Circular on Customer Service dated July 01, 2015, has also stipulated dealing with complaints and improving customer relations like providing a complaints/suggestions box, complaint book /register. A complaint form along with the name of the Nodal Officer for complaint redressal, is required to be provided in the homepage of the bank itself to facilitate

complaint submission by customers. In addition, the name, address and telephone numbers of the Controlling Authority of the bank to whom complaints can be addressed is also required to be given prominently by the banks. The Master Circular on Customer Service dated July 01, 2015 is available at: https://www.rbi.org.in/Scripts/BS_ViewMasCirculardetails.aspx?id=9862

RBI has further informed that to bring uniformity in the guidelines applicable to the different types of Regulated Entities (REs) under the IO mechanism, the erstwhile four Internal Ombudsman Schemes applicable to the above four entities were integrated into a Master Direction and the Master Direction – Reserve Bank of India (Internal Ombudsman for Regulated Entities) Directions, 2023 was issued on December 29, 2023. The framework reaffirmed that the Internal Ombudsman shall be positioned as an independent, apex level authority on consumer grievance redress within the regulated entities.

Any regulated entity that partially or fully rejected a complaint had to pass the rejection through the Internal Ombudsman of the Regulated Entity who would independently evaluate the complaint. The RE may appoint more than one Internal Ombudsman and a number of Deputy Internal Ombudsman based on volume of complaints and assist the Internal Ombudsman in the quality of disposal of complaints.

The Internal Ombudsman / Deputy Internal Ombudsman shall not be eligible for reappointment or for extension of term in the same RE. The Internal Ombudsman / Deputy Internal Ombudsman cannot be removed before the completion of his / her contracted term without the explicit approval of the Reserve Bank of India. The emoluments, facilities and benefits accorded to the Internal Ombudsman / Deputy Internal Ombudsman, once determined, shall not be changed during the tenure of Internal Ombudsman / Deputy Internal Ombudsman. The office of the Internal Ombudsman shall preferably be placed in the Head Office or Corporate Office of the regulated entity. All these measures would ensure adequate power and independence of the Internal

Ombudsman.1.8 Under the Reserve Bank Integrated Ombudsman Scheme (RB-IOS, 2021)

(ii) The Regulated Entity shall ensure that a copy of the Scheme is available in all its branches to be provided to the customer for reference upon request thereby making it easier to lodge a complaint

(iii) The salient features of the Scheme along with the copy of the Scheme shall be displayed and updated on the website of the Regulated Entity.

The Regulated Entities are being advised to have the Scheme and copies of the complaint format, also in vernacular languages, at all branches.

## CHAPTER V

## OBSERVATIONS/RECOMMENDATIONS IN RESPECT OF WHICH FINAL REPLIES OF THE GOVERNMENT ARE STILL AWAITED

**-NIL-**

**NEW DELHI**
**4 December, 2024**
**13 Agrahayana, 1946 (Saka)**

**BHARTRUHARI MAHTAB,**
**Chairperson,**
**Standing Committee on Finance**

**Minutes of the Seventh sitting of the Standing Committee on Finance (2024-25).**

**The Committee sat on Wednesday, the 04 December, 2024 from 1500 hrs to 1530 hrs in Committee Room 'G-074', Parliament Library Building, New Delhi.**

**PRESENT**

**Shri Bhartruhari Mahtab – Chairperson**

**LOK SABHA**

2. Shri P. P. Chaudhary
3. Shri Lavu Sri Krishna Devarayalu
4. Shri Gaurav Gogoi
5. Shri Kishori Lal
6. Shri Harendra Singh Malik
7. Shri Chudasama Rajeshbhai Naranbhai
8. Thiru Arun Nehru
9. Shri N. K. Premachandran
10. Dr. C. M. Ramesh
11. Dr. Jayanta Kumar Roy
12. Shri Prabhakar Reddy Vemireddy

**RAJYA SABHA**

13. Shri Milind Murli Deora
14. Dr. Ashok Kumar Mittal
15. Shri Sanjay Seth
16. Dr. Dinesh Sharma
17. Smt. Darshana Singh
18. Shri Pramod Tiwari

**SECRETARIAT**

| | | | |
|---|---|---|---|
| 1. | Shri Gaurav Goyal | - | Joint Secretary |
| 2. | Shri Vinay Pradeep Barwa | - | Director |
| 3. | Shri Kuldeep Singh Rana | - | Deputy Secretary |
| 4. | Shri T. Mathivanan | - | Deputy Secretary |

2. At the outset, the Chairperson welcomed the Members to the sitting of the Committee. Thereafter, the Committee took up the following draft reports for consideration and adoption:

i. First Report on Demands for Grants (2024-25) of the Ministry of Finance (Departments of Economic Affairs, Expenditure, Financial Services, Investment & Public Asset Management and Public Enterprises).

ii. Second Report on Demands for Grants (2024-25) of the Ministry of Finance (Department of Revenue).

iii. Third Report on Demands for Grants (2024-25) of the Ministry of Corporate Affairs.

iv. Fourth Report on Demands for Grants (2024-25) of the Ministry of Planning.

v. Fifth Report on Demands for Grants (2024-25) of the Ministry of Statistics and Programme Implementation.

vi. Sixth Report on Action Taken by the Government on recommendations contained in 59th Report (Seventeenth Lok Sabha) on the subject 'Cyber Security and Rising Incidence of Cyber/White Collar Crimes'.

vii. Seventh Report on Action Taken by the Government on recommendations contained in 66th Report (Seventeenth Lok Sabha) on the subject 'Performance Review and Regulation of Insurance Sector'.

After some deliberations, the Committee adopted the above draft Reports with minor modifications and authorised the Chairperson to finalise them and present the Reports to the Parliament.

The Committee then adjourned.

**APPENDIX**

(*Vide* Para 4 of the Introduction)

ANALYSIS OF THE ACTION TAKEN BY THE GOVERNMENT ON THE OBSERVATIONS/RECOMMENDATIONS CONTAINED IN THE FIFTY-NINTH REPORT OF THE STANDING COMMITTEE ON FINANCE (SEVENTEENTH LOK SABHA) ON THE SUBJECT 'CYBER SECURITY AND RISING INCIDENCE OF CYBER/WHITE COLLAR CRIMES' OF THE MINISTRY OF FINANCE (DEPARTMENT OF FINANCIAL SERVICES), MINISTRY OF HOME AFFAIRS AND MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

| | | Total | % of total |
|---|---|---|---|
| (i) | Total number of Observations/ Recommendations | 05 | |
| (ii) | Observations/Recommendations which have been accepted by the Government (vide Recommendations at Sl.Nos. 1, 4 and 5) | 03 | 60% |
| (iii) | Observations/Recommendations which the Committee do not desire to pursue in view of the Government's replies | Nil | 0.00 |
| (iv) | Observations/Recommendations in respect of which replies of the Government have not been accepted by the Committee (vide Recommendations at Sl.Nos. 2 and 3) | 02 | 40% |
| (v) | Observations/Recommendations in respect of which final reply of the Government are still awaited | Nil | 0.00 |