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	
Chapter- III*	Observations/Recommendations which the Committee do not desire to pursue in view of the Government's replies	
Chapter- IV*	Observations/Recommendations in respect of which replies of the Government have not been accepted by the Committee	
Chapter- V*	Observations/Recommendations in respect of which final reply of the Government is still awaited	
	ANNEXURE	
	Minutes of the Sitting of the Committee held on 04.12.2024	16
	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.	18

* *Not appended in the cyclostyled copy*

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 recommendations/observations 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 recommendations/observations contained in the Report. The replies have been analyzed and categorized as follows:

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

Recommendation No. 1, 4 and 5

(Total 03)
(Chapter- II)

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

Recommendation No. NIL

(Total NIL)
(Chapter- III)

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

Recommendation No. 02 and 03.

(Total 02)
(Chapter -IV)

(iv) Recommendations/ Observations 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

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