FIFTY-SIXTH REPORT

COMMITTEE ON PETITIONS

(SEVENTEENTH LOK SABHA)

MINISTRY OF FINANCE

(DEPARTMENT OF FINANCIAL SERVICES)

(Presented to Lok Sabha on 19.12.2023)

LOK SABHA SECRETARIAT
NEW DELHI

December 2023/Agrahayana, 1945 (Saka)

CPB No. 1 Vol. LVI

Published under Rule 382 of the Rules of Procedure and Conduct of Business in Lok Sabha (Sixteenth Edition).

CONTENTS

	PAGE
COMPOSITION OF THE COMMITTEE ON PETITIONS	**(ii)**
INTRODUCTION.....	**(iii)**
REPORT	
Action Taken by the Government on the recommendations made by the Committee on Petitions (Seventeenth Lok Sabha) in their Fortieth Report on the representation of Shri Abhishek relating to increasing frauds in ATMs of Indian Overseas Bank, Indian Bank, Union Bank of India and Canara Bank in Mumbai – Urgent need to re-draw effective strategy for ATM transactions and other important issues related therewith.	**1**
ANNEXURE	
Minutes of the 30th sitting of the Committee on Petitions held on 18.12.2023.	23

COMPOSITION OF THE COMMITTEE ON PETITIONS

Shri Harish Dwivedi - *Chairperson*

MEMBERS

2. Shri Anto Antony
3. Shri Hanuman Beniwal *
4. Prof. Sanjay Sadashivrao Mandlik
5. Shri P. Ravindhranath
6. Dr. Jayanta Kumar Roy
7. Shri Brijendra Singh
8. Shri Sunil Kumar Singh
9. Shri Sushil Kumar Singh
10. Shri Manoj Kumar Tiwari
11. Shri Prabhubhai Nagarbhai Vasava
12. Shri Rajan Baburao Vichare
13. Shri Bharat Ram Margani
14. Vacant
15. Vacant

SECRETARIAT

1. Shri Raju Srivastava - Joint Secretary
2. Shri Tenzin Gyaltsen - Deputy Secretary
3. Shri Harish Kumar Sethi - Under Secretary

---

* *Resigned his Lok Sabha seat w.e.f. 15.12.2023.*

FIFTY-SIXTH REPORT OF THE COMMITTEE ON PETITIONS
(SEVENTEENTH LOK SABHA)

INTRODUCTION

I, the Chairperson, Committee on Petitions, having been authorised by the Committee to present on their behalf, this Fifty-Sixth Report (Seventeenth Lok Sabha) of the Committee to the House on the Action Taken by the Government on the recommendations made by the Committee on Petitions (Seventeenth Lok Sabha) in their Fortieth Report on the representation of Shri Abhishek relating to increasing frauds in ATMs of Indian Overseas Bank, Indian Bank, Union Bank of India and Canara Bank in Mumbai – Urgent need to re-draw effective strategy for ATM transactions and other important issues related therewith.

2. The Committee considered and adopted the draft Fifty-Sixth Report at their sitting held on 18 December, 2023.

3. The observations/recommendations of the Committee on the above matters have been included in the Report.

NEW DELHI;

HARISH DWIVEDI
Chairperson,
Committee on Petitions

18 December, 2023
27 Agrahayana, 1945 (Saka)

REPORT

ACTION TAKEN BY THE GOVERNMENT ON THE RECOMMENDATIONS MADE BY THE COMMITTEE ON PETITIONS (SEVENTEENTH LOK SABHA) IN THEIR FORTIETH REPORT ON THE REPRESENTATION OF SHRI ABHISHEK RELATING TO INCREASING FRAUDS IN ATMs OF INDIAN OVERSEAS BANK, INDIAN BANK, UNION BANK OF INDIA AND CANARA BANK IN MUMBAI – URGENT NEED TO RE-DRAW EFFECTIVE STRATEGY FOR ATM TRANSACTIONS AND OTHER IMPORTANT ISSUES RELATED THEREWITH.

The Committee on Petitions (Seventeenth Lok Sabha) presented their Fortieth Report to Lok Sabha on 13 December, 2022 on the representation of Shri Abhishek relating to increasing frauds in ATMs of Indian Overseas Bank, Indian Bank, Union Bank of India and Canara Bank in Mumbai – Urgent need to re-draw effective strategy for ATM transactions and other important issues related therewith.

2. The Committee had made certain observations/recommendations in the matter and the Ministry of Finance (Department of Financial Services) was asked to implement the recommendations and requested to furnish their action taken notes thereon for further consideration of the Committee.

3. Action Taken Notes have since been received from the Ministry of Finance (Department of Financial Services) in respect of all the observations/ recommendations contained in the aforesaid Report. The observations/ recommendations made by the Committee and the replies furnished thereto by the Ministry of Finance (Department of Financial Services) are detailed in the succeeding paragraphs.

4. In paragraphs 13 and 14 of the Report, on the aspect of electronic mode of transaction vis-à-vis customers' confidence, the Committee had observed/ recommended as follows:-

> *"Since time immemorial, the Banking Industry has always been an indispensable Institution that contributes significantly to the sustainability and maintenance of a country's economy. The advent of technology, during the last 2-3 decades, has fundamentally revolutionized the system of traditional banking and also brought perceptible changes in the banking landscape not only in the country but also in the world. Today, banking is no longer confined to physically going to the bank branches*

as electronic banking system has grown significantly and has also been increasing at a fast pace. Although, a variety of digital products and services, including internet banking, NEFT, RTGS, and also the 'Mobile Banking', have entered the Indian banking system and completely altered the method of effecting financial transactions, ATM banking, as one of the first e-banking tools, continues to be one of the most popular modes in the country. Automated Teller Machine or ATM is the most accessible and notable banking product which is the outcome of innovation in the information and communication technology. Use of ATMs not only assisted banks in extending their banking services, it also provided convenience and ease to the customers. Initially, the ATMs were introduced to provide cash to the customers but subsequently, with the technological developments, its services have been extended to include cash withdrawals, funds transfers from one account to the other and also making online payments.

The Committee note that as the landscape of Indian Banking system has undergone a noticeable change, during the past few years, it has been transformed to digital mode of transaction. With the increased use of ATM on one hand, the ATM/online frauds, on the other hand, have also witnessed a surge at an unprecedented level. Today, the Bank Frauds, in general, and ATM frauds, in particular, have become such a routine feature that the credibility of banks to insulate their customers from these fraudsters albeit initiating various technological-driven methods, have been eroding at a fast pace. In this backdrop, the Committee urge the Government and the Banks to initiate technology-driven innovative measures to redress these issues so that the confidence of the customers while using the electronic mode of transaction is not eroded any further. In this regard, the Committee would be glad to know the 'Action Plan' of various financial institutions/banks for restoring the confidence of their customers while using various electronic mode of transaction."

5. The Ministry of Finance (Department of Financial Services), in their action taken reply, have submitted as follows:-

"A number of steps have been taken to enhance security of digital payment transactions, including those of card transactions, online transactions etc., and to reduce online banking frauds which include, inter alia, the following :-

(i) enabling all ATMs for processing EMV chip and PIN cards;
(ii) mandating PIN entry for all ATM transactions;
(iii) conversion of magnetic strip card to EMV chip and PIN cards;
(iv) restricting international usage by default and enablement of the same only after specific mandate from the customer;

(v) certification of merchant terminals;
(vi) Capping the value/mode of transactions/beneficiaries;
(vii) mandating enablement of online alerts for all transactions;
(viii) setting daily limits; and
(ix) issuing alerts upon addition of beneficiaries.

Further, to help customers recover losses sustained on account of fraudulent transactions, Reserve Bank of India (RBI) has issued instructions on limiting the liability of customers in cases of unauthorized electronic banking transactions and, the burden of proving customer liability in case of an unauthorized electronic banking transaction has now been migrated on to the bank.

Also, banks are required to set up internal control systems to combat frauds and actively participate in fraud prevention committees/ task forces which formulate laws to prevent frauds and take proactive fraud control and enforcement measures.

Further, as per RBI guidelines on 'Customer Protection – Limiting Liability of Customers in Unauthorized Electronic Banking Transactions', banks have been instructed to design systems and procedures to make customers feel safe about carrying out electronic banking transactions, and banks must put in place–

(i) appropriate systems and procedures to ensure safety and security of electronic banking transactions carried out by customers;

(ii) robust and dynamic fraud detection and prevention mechanism;

(iii) mechanism for assessment of the risks and measurement of the liabilities resulting from unauthorized transactions;

(iv) appropriate measures to mitigate the risks and protect themselves against the liabilities arising therefrom; and

(v) a system of continually and repeatedly advising customers on how to protect themselves from electronic banking and payments related fraud.

As per inputs received from public sector banks (PSBs), they are following all the aforesaid RBI guidelines, and they have a Board-approved policy on payment for

losses sustained by the customers on account of unauthorized electronic banking transactions, fraudulent transactions including ATM transactions."

6. In paragraphs 15 and 16 of the Report, on the methods to outsmart the fraudsters', the Committee had observed/recommended as follows:-

"The Committee, during the course of examination of the representation, note that most of the banking operations are becoming digital and the physical form(s) of transactions getting substituted by the electronic mode at a fast pace, the fraudsters have also gradually attained expertise in outsmarting the electronic surveillance and technology-driven fireballs of the Banks for duping the customers. It is an undeniable fact that the Committee have also acknowledge that on every single day, new methods are being developed by the fraudsters to cheat/dupe the customers of their money deposited in the Banks.

In this chronology, the Committee note that the incidence of ATM cloning, deciphering of PIN and passwords, phishing, skimming and cajoling the customers to reveal their account-related information to the fraudsters, purely with an impression that the customers have been making conversation to some banking official and thereafter siphoning off their deposits, have become an perennial feature, throughout the country. Although, with the rapid and continuous dissemination of information by almost all the financial institutions, including Banks, thereby, cautioning their customers of the rapid ingenious techniques being adopted by these fraudsters and also the fact that the majority of customers have also transformed themselves to remain extra vigilant and do not get tempted by these fraudsters, the Committee could gauge that these fraudsters, in majority of incidents, outsmart not only the mechanism of dissemination of information devised by the Banks but also the newly attained vigilant attitude of the customers as a result of which, the ATM and other online transaction related frauds have not shown sign of receding in the country. The Committee, therefore, impress upon Government/Banks to be proactive in their approach to outsmart the hackers/fraudsters and also to keep on updating their electronic anti-skimming devices/fireballs on a regular basis. In this endeavor, the Management of the Banks should also attempt to create inter-linking of their electronic paraphernalia so that the nefarious activities of defrauding the customers by these fraudsters could be brought down to a maximum possible extent. The Committee would like to be apprised of the action taken by the Ministry, on this count, within three months of the presentation of Report to the House."

7. The Ministry of Finance (Department of Financial Services), in their action taken reply, have submitted as follows:-

"RBI has issued instructions on Cyber Security Framework in Banks and have mandated Scheduled Commercial Banks (SCBs) to report all unusual cyber incidents to RBI within two to six hours of occurrence of such incidents. These incidents are analysed for the pattern of attack and the vulnerabilities exploited, and where needed, advisories/alerts are issued to the banks so as to avoid repeat attacks/exploitation of the same vulnerabilities. Further, the incidents are also analysed from the point of view of sophistication of attack as well as the systemic impact, and are categorized under critical, high, medium and low categories. RBI also reviews the cyber security developments and threats on an ongoing basis and necessary measures are taken to strengthen the cyber resilience of banks. Comprehensive steps taken in order to strengthen security of digital transactions, inter alia, include the following:-

(i) A comprehensive circular on Cyber Security Framework in Banks was issued by RBI on 2.6.2016, wherein banks were advised to put in place a board-approved cyber-security policy elucidating the strategy containing an appropriate approach to combat cyber threats given the level of complexity of business and acceptable levels of risk.

(ii) Guidelines on Cyber Security Controls for third party ATM Switch Application Service Providers (ASPs) have been issued by RBI on 31.12.2019.

(iii) Master Directions on Digital Payment Security Controls have been issued by RBI on 18.2.2021, wherein banks have been advised to put in place necessary controls to protect the confidentiality and integrity of customer data, and processes associated with the digital product/services offered.

(iv) A National Cyber Crime Reporting Portal has been launched by the Ministry of Home Affairs to enable public to report incidents pertaining to all types of cybercrimes, and a toll-free number has also been operationalised to get assistance in lodging online complaints.

(v) For immediate reporting of financial frauds and to stop siphoning-off of funds by the fraudsters, Financial Cyber Fraud Reporting and Management System module has been made operational by the Indian Cyber Crime Coordination Centre (I4C), working under the Ministry of Home Affairs.

(vi) *The Indian Computer Emergency Response Team (CERT-IN) under the Ministry of Electronics and Information Technology issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis to ensure safe usage of digital technologies, and is working in coordination with service providers, regulators and Law Enforcement Agencies (LEAs) to track and disable phishing websites and facilitate investigation of fraudulent activities.*

(vii) *Ministry of Electronics & Information Technology (MeitY) in consultation with Department of Financial Services (DFS), RBI, National Critical Information Infrastructure Protection Centre(NCIIPC) and regulated entities have identified and notified certain systems/ products/ services in respect of RBI, National Payment Corporation of India (NPCI), SBI, HDFC Bank, ICICI Bank, PNB, Bank of Baroda, Union Bank of India, Kotak Mahindra Bank, Canara Bank and Axis Bank as Critical Information Infrastructure (CII), to reduce the vulnerabilities to various cyber threats and attacks.*

Further, banks also submit periodic credit information, including information on frauds, in respect of borrowers having exposures of ₹5 crore or above to RBI's Central Repository of Information on Large Credits (CRILC) for supervisory purposes and is disseminated among RBI's regulated entities to help them in taking credit decisions. Also, Credit Information Companies have been advised by RBI to disseminate the information received by them pertaining to suit filed accounts of willful defaulters, on their respective websites to maintain the transparency and public awareness about such defaulters.

Besides that, a Central Fraud Registry (CFR), a web-based and searchable database, has been made available by RBI, for which banks have been given access through user-ids and password. Banks have been advised to make full use of the CFR for timely identification, control, reporting and mitigation of fraud risk, and also to put in place proper systems and procedure to ensure that the information available in CFR is made use as a part of the credit risk governance and fraud risk management.

In addition, several other initiatives have also been taken to spread awareness on prevention of cybercrimes. These initiatives include, dissemination of messages on cybercrime through short message service (SMS), radio campaigns, publicity on prevention of cybercrime and cyber safety tips through official social media accounts, conducting of electronic-banking awareness and training (e-BAAT) programmes by

RBI, etc. Further, a half-day conference on "FINSCY" (Financial Services Cyber Security) was organized by DFS on 18.01.2023 to assess cyber security measures currently putting in place in the financial sector and readiness of the sector to any future cyber threats. Various organizations such as I4C, CERT-In, NCIIPC, RBI, IRDAI, PFRDA, SBI, LIC, HDFC Bank and ICICI Bank had made presentations regarding cyber security framework in their respective organizations in the said event.

As per RBI data on frauds reported by SCBs under the category "Card/Internet-ATM/Debit Cards", the amount involved in such frauds, based on the year of occurrence, has declined from Rs.116 crore in the financial year 2019-20 to Rs.76 crore in the financial year 2020-21 (Y-o-Y decline of 34.5%) and to Rs.68 crore in the financial year 2021-22 (Y-o-Y decline of 10.5%)."

8. In paragraph 17 of the Report, on the aspect of user-friendly and Integrated System of filing fraud-related complaints, the Committee had observed/recommended as follows:-

"The Committee note that there is no uniformity amongst the Banks in filing complaints relating to ATM frauds by the customers. From the submissions made by the Ministry, the Committee have gauged that some Banks require customers to file complaint with the Law Enforcement Agencies, while other Banks file complaint themselves and also co-ordinate with the Law Enforcement agencies in some cases. There is also no uniformity amongst the Banks operating at various regions of the country in dealing with the cases of fraud either involving a small amount or a substantial amount of more than one lakh rupees. Besides, there is also no uniformity relating to the level of Authority in the Banks that would be dealing with the cases of ATM and/or online frauds."

9. The Ministry of Finance (Department of Financial Services), in their action taken reply, have submitted as follows:-

*"In regard to filing of complaints, it is submitted that complaint pertaining to all types of cybercrimes, including, banking frauds, unauthorized card transactions, online transactions etc. can be lodged on the National Cyber Crime Reporting Portal, which are routed automatically to state/UT law enforcement agency for further action. Also, a toll-free number **'1930'** has been operationalised for lodging online cyber complaints, including in respect of frauds pertaining to banking transactions. Citizen Financial Cyber Fraud Reporting and Management System was launched by on-boarding all the states/UTs for quick reporting of financial cyber frauds and to*

prevent flow of funds, siphoned off by fraudsters in the least possible time.

*Further, RBI vide its circular dated 12.11.2021, has integrated its existing three Ombudsman schemes into **'One Nation One Ombudsman'** approach, making the Ombudsman mechanism jurisdiction neutral, to provide cost-free redressal of customer complaints involving 'deficiency in services', including the unauthorized electronic fund transfer rendered by entities regulated by RBI. The complaints under the Scheme made online are registered on RBI's Complaint Management System portal, and a Centralized Receipt and Processing Centre has been set up at RBI, Chandigarh for receipt and initial processing of physical and email complaints in any language.*

To help customers recover loss sustained on account of fraudulent transactions, RBI has issued instructions on limiting the liability of customers in cases of unauthorized electronic banking transactions. In case where the deficiency lies neither with the bank nor with the customer, but elsewhere in the system, the liability of a customer is zero, if she or he informs the bank regarding an unauthorized electronic transaction within three working days of receiving information in respect of the transaction from the bank. Liability of the customer ranges from Rs. 5,000 to Rs. 25,000, if reported within 4-7 working days, and if reported beyond 7 working days, it shall be determined as per the bank's Board approved policy. Further, in cases where the loss is due to negligence by a customer, any loss occurring after the reporting of the unauthorized transaction shall be borne by the bank. Banks have also been advised by RBI to ensure that any complaint is resolved and liability of the customer, if any, is established within a maximum period of 90 days. Also, the burden of proving customer liability in case of an unauthorized electronic banking transaction has now been migrated on to the bank."

10. In paragraph 18 of the Report, the Committee had observed/recommended as follows:-

"The Committee also note that whenever, any customer is duped by these fraudsters, the first and foremost requirement relates to informing the 'Helpline' services of the Bank where the customer is having his account. However, since there are occasions when customer uses ATM of a different Bank or make use of different online payment platforms, after being defrauded by the scamsters, they often get perplexed as to which Bank needs to be contacted on immediate basis. The Committee are, therefore, of considered view that for filing of fraud-related complaints, there should be a user-friendly and uniform system for all the Banks. In this regard, the Committee, after considering that there is a unified system of

registering online complaints with the Police, Fire Department and Ambulance Services which is hassle free, impress upon all the Banks to develop an integrated system of filing fraud-related complaints, both ATM-related and online frauds which would be operative throughout the country. With a view to developing an integrated system of filing fraud-related complaints, the Ministry should also consult the Ministry of Telecommunications for allotment of an easy recognizable telephone number similar to that of Police, Fire Department, Ambulance Services, etc. The Committee would like to be apprised of the action taken by the Ministry on this count within three months of the presentation of this Report to the House."

11. The Ministry of Finance (Department of Financial Services), in their action taken reply, have submitted as follows:-

*"Government has launched the National Cyber Crime Reporting Portal to enable public to report incidents pertaining to all types of cybercrimes, including banking frauds, unauthorised card transactions, online transactions etc. A toll-free number **'1930'** has also been operationalised for lodging online cyber complaints, including in respect of frauds pertaining to banking transactions. Citizen Financial Cyber Fraud Reporting and Management System module has been launched for immediate reporting of financial frauds and to stop siphoning off fund by the fraudsters."*

12. In paragraph 19 of the Report on the aspect of setting up of an 'All India Agency' for investigation of bank-related frauds, the Committee had observed/recommended as follows:-

"The Committee, while examination the representation, note that during the last few years, ATM, online and other bank-related frauds have attained a new dimension, which are now being committed by fraudsters from a remote location, i.e., most of the time, beyond the geographical boundaries of a State/Union-Territory. Due to this peculiar character of the crime, whenever, any fraud takes place, the Bank(s) and the Investigation Agencies have serious jurisdictional problem due to which the pace of investigation often gets retarded. It is also a well-recognized fact that the 'time factor' is the most important determining element in stopping the transfer of funds to the fraudsters as well as nabbing the culprits by the Investigation Agencies. In this regard, the Committee have also experienced that due to lack of any unified apparatus, on the one hand, it becomes difficult to recover the money from the fraudsters and on the other hand, it takes a long time, even years, to nab such culprits and brought them to justice. Keeping in view this functional problem, the Committee strongly recommend the Ministry of Finance (Department of Financial

Services) to constitute an 'Expert Committee', consisting some of their senior officers along with the officers of Banks, senior officials of the Ministry of Home Affairs and the Ministry of Law to explore the feasibility of creation of an 'All India Authority' for dealing with all bank-related online frauds. The said 'Expert Committee' should be given the mandate to work out various legal requirements, administrative setup, delineation of jurisdiction, etc., so that they are able to give their report to the Government within a specified time. The Committee would like to be apprised of the action taken by the Ministry on this count within three months of the presentation of this Report to the House."

13. The Ministry of Finance (Department of Financial Services), in their action taken reply, have submitted as follows:-

"Ministry of Home Affairs (MHA) has apprised that it had constituted in December 2014, an Expert Group to study the gaps and challenges, prepare a roadmap for effectively tackling cybercrimes in the country and give suitable recommendations on all facets of cybercrime. The Expert Group submitted its report in September 2015, and identified the following gaps and challenges in tackling Cybercrimes:-

(i) Lack of centralized online reporting mechanism.
(ii) Inadequate infrastructure for cybercrime monitoring and investigation.
(iii) Lack of skilled cyber professionals.
(iv) Challenges related to technology and Research & Development.
(v) Lack of citizen awareness.
(vi) Legal and jurisdiction related issues.
(vii) Lack of standard operating procedure for cybercrime investigation.
(viii) Inadequate institutional structure and funding to tackle cybercrime.
(ix) Lack of clear-cut roadmap for tackling cybercrime

The Expert Group also made specific recommendations to combat cybercrime in the country and recommended creation of Indian Cyber Crime Coordination Centre to strengthen the overall security apparatus to fight against Cybercrime.

Accordingly, the Indian Cyber Crime Coordination Centre was established to provide a framework and ecosystem for law enforcement agencies (LEAs)to deal with the cybercrimes in a comprehensive and coordinated manner. The Indian Cyber Crime Coordination Centre focuses on tackling all the issues related to cybercrime for the citizens, which includes improving coordination between various Law Enforcement Agencies and the stakeholders, driving change in India's overall capability to tackle cybercrime and to improve citizen satisfaction level.

The following are the key components of the Indian Cyber Crime Coordination Centre:-

(a) National Cybercrime Threat Analytics Unit:

(i) Platform for analysing all pieces of puzzles of cybercrimes;

(ii) Produce cybercrime threat intelligence reports and organize periodic interaction on specific cybercrime centric discussions;

(iii) Create multi-stakeholder environment for bringing together law enforcement specialists and industry experts.

(b) National Cyber Crime Reporting Portal:

(i) Facilitate reporting of all types of cybercrime incidents, including banking frauds, unauthorised card transactions, online transactions etc.;

(ii) Since majority of the cyber incidents reported on National Cyber Crime Reporting Portal relate to financial frauds, a platform "Citizen Financial Cyber Fraud Reporting and Management System" was launched in April, 2021 by on-boarding all the States/UTs for quick reporting of financial cyber frauds, by taking appropriate action in accordance with law, to prevent flow of funds, siphoned off by fraudsters in the least possible time;

(iii) Facilitate complainants to view status of action taken on the reported incident.

(c) National Cybercrime Ecosystem Management:

(i) Develop ecosystems that bring together academia, industry and Government to spread awareness on cybercrimes, establish standard operating procedures to contain the impact of cybercrimes and respond to cybercrimes;

(ii) Provide support for development of all components of cybercrime combating ecosystem.

(d) National Cybercrime Training Centre:

(i) Standardization of course curriculum focused on cybercrimes, impact containment and investigations, imparting practical cybercrime detection, containment and reporting trainings on simulated cyber environments;

(ii) Development of Massive Open Online Course on a cloud-based training platform;

(iii) To focus on establishing Cyber Range for advanced simulation and training on cyber-attack and investigation of such cybercrimes.

(e) National Cybercrime Forensic Lab (NCFL) Ecosystem:

(i) Forensic analysis and investigation of cybercrime as a result of new digital technology and techniques;

(ii) A centre to support investigation process. NCFL and associated Central Forensic Science Laboratory to be well-equipped and well-staffed in order to engage in analysis and investigation activities to keep-up with new technical developments.

(f) Platform for Joint Cybercrime Investigation Team:

(i) To drive intelligence-led, coordinated action against key cybercrime threats and targets;

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

(g) National Cybercrime Research and Innovation Centre:

(i) Track emerging technological developments, proactively predict potential vulnerabilities, which can be exploited by cybercriminals;

(ii) To leverage the strength and expertise of all stakeholders, be it in academia, private sector or inter-governmental organizations;

(iii) Create strategic partnerships with all such entities in the area of

research and innovation focused on cybercrimes, cybercrime impact containment and investigations.

*In addition, a toll-free number **'1930'** has also been operationalised for lodging online cyber complaints, including in respect of frauds pertaining to banking transactions."*

OBSERVATIONS/RECOMMENDATIONS

Effective implementation of steps/measures by the Financial Institutions/Banks for increasing confidence of the customers while using electronic modes of transaction

14. The Committee while examining the representation of Shri Abhishek relating to increasing frauds in ATMs of Indian Overseas Bank, Indian Bank, Union Bank of India and Canara Bank in Mumbai – urgent need to re-draw effective strategy for ATM transactions – in light of the comments/replies furnished by the Ministry of Finance (Department of Financial Services) had highlighted the noticeable change in the landscape of Indian Banking System during the past few years, which has been transformed to digital mode of transaction. The Committee, in this context, had noted that with the increased use of ATM/Online banking as e-banking tools for effecting financial transactions, the ATM/online frauds have also witnessed a surge at an unprecedented level. The Committee had further noted that the Bank frauds, in general, and the ATM frauds, in particular, have become such a routine feature that the credibility of Banks to insulate their customers from these fraudsters *albeit* initiating various technological-driven methods, have been eroding at a fast pace. The Committee had, therefore, urged the Government and the Banks to initiate technology-driven innovative measures to redress these issues so that the confidence of the customers while using the electronic mode of transaction is not eroded any further. The Committee had also suggested for formulating the 'Action Plan' by various Financial Institutions/Banks for restoring the confidence of their customers while using various electronic mode of transactions.

15. Based on the replies furnished the Ministry of Finance (Department of Financial Services) in response to the above recommendation(s) of the Committee, it is noted that various efforts are being made to enhance security of digital payment transactions, including those of card transactions, online transactions, etc., in order

to reduce online banking frauds. The Committee, in this regard, also acknowledge that the Reserve Bank of India (RBI) has issued instructions on limiting the liability of customers in cases of unauthorized electronic banking transactions and, the burden of proving customer liability in case of an unauthorized electronic banking transaction has now been migrated on to the Bank and they are now required to set up internal control systems to combat frauds and actively participate in fraud prevention committees/ task forces which formulate laws to prevent frauds and take proactive fraud control and enforcement measures. Further, as per RBI Guidelines on 'Customer Protection – Limiting Liability of Customers in Unauthorized Electronic Banking Transactions', Banks have been instructed to design systems and procedures to make customers feel safe about carrying out electronic banking transactions, and Banks must put in place (i) Appropriate systems and procedures to ensure safety and security of electronic banking transactions carried out by customers; (ii) Robust and dynamic fraud detection and prevention mechanism; (iii) Mechanism for assessment of the risks and measurement of the liabilities resulting from unauthorized transactions; (iv) Appropriate measures to mitigate the risks and protect themselves against the liabilities arising there from; and (v) A system of continually and repeatedly advising customers on how to protect themselves from electronic banking and payments related fraud. The Committee, in this connection, are informed that the Public Sector Banks have been following all the aforesaid RBI Guidelines, and further, they also have a Board-approved Policy on payment for losses sustained by the customers on account of unauthorized electronic banking transactions, fraudulent transactions including ATM transactions.

16. The Committee though acknowledge various steps/measures being adopted by the Banks to enhance security of digital payment transactions, including those of card transactions, online transactions, etc., in order to reduce ATM/Online banking

frauds, recommend the Ministry of Finance (Department of Financial Services) to ensure that these steps/measures are implemented effectively by the Financial Institutions/Banks so that the confidence of their customers are maintained while using various electronic modes of transaction. The Committee further desire that the RBI Guidelines on 'Customer Protection – Limiting Liability of Customers in Unauthorized Electronic Banking Transactions' and other relevant Instructions/Advisories should be scrupulously followed by all the Financial Institutions/Banks. The Committee may be apprised of the necessary steps taken by the Ministry of Finance (Department of Financial Services)/RBI in this regard.

Effective implementation of all Instructions/Guidelines/Advisories issued by the RBI from time to time in all the Financial Institutions/Banks

17. The Committee, during the course of examination of the representation, had expressed their concerns over the fact that the banking fraudsters have been gradually attaining expertise in outsmarting the electronic surveillance and technology-driven fireballs of the Banks for duping the customers while developing new methods of cheating/duping the customers of their money deposited in the Banks resulting into increasing number of incidences of ATM cloning, deciphering of PIN and passwords, phishing, skimming, etc. The Committee had therefore impressed upon the Government/Banks to be proactive in their approach to outsmart the hackers/fraudsters and also to keep on updating their electronic anti-skimming devices/firewalls on a regular basis. The Committee had also suggested that the Management of the Banks, in this endeavour, should also attempt to create inter-linking of their electronic paraphernalia so that the nefarious activities of defrauding the customers by these fraudsters could be brought down to a maximum possible extent.

18. In response to the aforesaid recommendation(s) of the Committee, the Ministry of Finance (Department of Financial Services), in their action taken replies, have informed that the Reserve Bank of India (RBI) has issued instructions on Cyber Security Framework in Banks and have mandated Scheduled Commercial Banks to report all unusual cyber incidents to RBI within two to six hours of occurrence of such incidents, which are analysed for the pattern of attack and the vulnerabilities exploited, and if needed, advisories/alerts are issued to the Banks so as to avoid repeat attacks/exploitation of the same vulnerabilities. Further, RBI also reviews the cyber security developments and threats on an ongoing basis and necessary measures are being taken to strengthen the cyber resilience of Banks. Besides, RBI has issued Guidelines on Cyber Security Controls for third party ATM Switch Application Service Providers (ASPs) and Master Directions on Digital Payment Security Controls. The Ministry of Finance (Department of Financial Services) have further informed that a National Cyber Crime Reporting Portal and Financial Cyber Fraud Reporting and Management System Module which has been made operational by the Indian Cyber Crime Coordination Centre (I4C), are being administered by the Ministry of Home Affairs to enable public to report incidents pertaining to all types of cybercrimes, financial frauds and to stop siphoning-off of funds by the fraudsters. Besides, a toll-free number, i.e., '1930' has been operationalised to get assistance in lodging online complaints related to cyber and banking frauds. In addition to the above, the Indian Computer Emergency Response Team (CERT-IN) under the Ministry of Electronics and Information Technology (MeitY) issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis to ensure safe usage of digital technologies, and is working in coordination with service providers, regulators and Law Enforcement Agencies (LEAs) to track and disable phishing websites and facilitate investigation of fraudulent activities. The Ministry have also informed the Committee that RBI has constituted the Central Fraud Registry (CFR) for

timely identification, control, reporting and mitigation of fraud risk and spreading awareness on prevention of cybercrimes, etc. The Committee have further been informed that as per RBI data on frauds reported by SCBs under the category "Card/Internet- ATM/Debit Cards", the amount involved in such frauds, based on the year of occurrence, has declined from Rs.116 crore in the Financial Year 2019-20 to Rs.76 crore in the Financial Year 2020-21 (Y-o-Y decline of 34.5%) and to Rs.68 crore in the Financial Year 2021-22 (Y-o-Y decline of 10.5%).

19. The Committee while acknowledging mechanisms in place which are being implemented through various Instructions/Guidelines issued by the RBI from time to time with regard to identification, control, reporting of cyber crimes, online banking frauds, etc., and also mitigation of fraud risk vis-a-vis spreading awareness on prevention of cybercrimes, etc., would like to recommend the Ministry of Finance (Department of Financial Services) to ensure effective implementation of all such Instructions/Guidelines/Advisories issued by the RBI from time to time in all the Financial Institutions/Banks, while reviewing and updating their electronic anti-skimming devices/firewalls on a regular basis in order to minimize the fraud incidences. The Committee would like to be apprised of the necessary steps taken in this regard.

Publicizing the information related to complaints lodging mechanism, portals, etc.

20. The Committee had observed that there is no uniformity amongst the Banks operating at various regions of the country in dealing with the cases of filing complaints relating to ATM frauds by the customers and the level(s) of Authority in the Banks which would be dealing with the cases of ATM and/or online frauds. The Committee while underscoring the need for a user-friendly and uniform system for all

the Banks for filing of fraud-related complaints, had impressed upon all the Banks to develop an integrated system of filing fraud-related complaints, both ATM-related and online frauds which would be operative throughout the country.

21. From the action taken replies of the Ministry of Finance (Department of Financial Services), in response to the above recommendation(s), the Committee take note of the fact that in regard to filing of complaints pertaining to all types of cybercrimes, including banking frauds, unauthorized card transactions, online transactions etc., can be lodged on the National Cyber Crime Reporting Portal, which are routed automatically to States/UTs Law Enforcement Agencies for further action. Further, a toll-free number '1930' has been operationalised for lodging online cyber complaints, including in respect of frauds pertaining to banking transactions. Also, Citizen Financial Cyber Fraud Reporting & Management System has been launched by on-boarding all the states/UTs for quick reporting of financial cyber frauds and to prevent flow of funds, siphoned off by the fraudsters in the least possible time. The Committee have further been informed that RBI has integrated its existing three Ombudsman Schemes into 'One Nation One Ombudsman' approach, making the Ombudsman mechanism jurisdiction neutral, to provide cost-free redressal of customer complaints involving 'deficiency in services', including the unauthorized electronic fund transfer rendered by entities regulated by RBI. The complaints under the Scheme made online are registered on RBI's Complaint Management System portal, and a Centralized Receipt and Processing Centre has been set up at RBI, Chandigarh for receipt and initial processing of physical and email complaints in any language. Besides, RBI has also issued instructions on limiting the liability of customers in cases of unauthorized electronic banking transactions.

22. The Committee are of the considered opinion that in-spite of well number of complaints lodging portals, such as National Cyber Crime Reporting Portal, toll-free number '1930', Citizen Financial Cyber Fraud Reporting & Management System, RBI's Complaint Management System portal and further integration of existing three Ombudsman schemes into 'One Nation One Ombudsman' approach by RBI in dealing with the cases of filing complaints relating to ATM frauds and/or online frauds by the customers, the relevant information on existing complaints lodging portals, process, etc., for filing complaints relating to ATM frauds, online frauds, have not been properly disseminated to the vulnerable customers. The Committee, therefore, urge the Ministry of Finance (Department of Financial Services) to ask all the Financial Institutions/Banks to widely publicise all these complaints lodging portal, toll free numbers, etc., through digital, print as well as social media by displaying banners/posters containing the contact numbers, website, process of filing of complaints, etc., in order to make the public aware of the process of lodging complaints. The Committee would like to be apprised of the necessary steps taken in this regard.

Revisiting and analysing the findings and the recommendations of the Expert Group

23. Keeping in view the functional problem in handling the ATM frauds and nabbing the culprits by the Investigation Agencies vis-à-vis attaining a new dimension in ATM, online and other bank related frauds being committed by fraudsters from a remote location and serious jurisdictional problem being faced by the Bank(s) and the Investigation Agencies, the Committee had recommended the Ministry of Finance (Department of Financial Services) to constitute an 'Expert Committee', consisting some of their senior officers along with the officers of Banks, Ministry of Home Affairs and the Ministry of Law to explore the feasibility of creation

of an 'All India Authority' for dealing with all bank-related online frauds which should be given the mandate to work out various legal requirements, administrative setup, delineation of jurisdiction, etc., so that they are able to give their report to the Government within a specified time.

24. The Committee note from the action taken replies of the Ministry Finance (Department of Financial Services) that in December, 2014, the Ministry of Home Affairs had constituted an Expert Group to study the gaps and challenges, prepare a roadmap for effectively tackling cybercrimes in the country and give suitable recommendations on all facets of cybercrime. The Expert Group had submitted its report in September, 2015, and identified a number of gaps and challenges in tackling Cybercrimes. Further, the Expert Group had also made specific recommendations to combat cybercrime in the country and recommended creation of Indian Cyber Crime Coordination Centre to strengthen the overall security apparatus to fight against Cybercrime. Accordingly, the Indian Cyber Crime Coordination Centre was established to provide a framework and ecosystem for law enforcement agencies to deal with the cybercrimes in a comprehensive and coordinated manner which focuses on tackling all the issues related to cybercrime for the citizens, which includes improving coordination between various Law Enforcement Agencies and the stakeholders, driving change in India's overall capability to tackle cybercrime and to improve citizen satisfaction level. The Committee note that the key components of the Indian Cyber Crime Coordination Centre are as follows:-

(a) National Cybercrime Threat Analytics Unit
(b) National Cyber Crime Reporting Portal
(c) National Cybercrime Ecosystem Management
(d) National Cybercrime Training Centre

(e) National Cybercrime Forensic Lab (NCFL) Ecosystem

(f) Platform for Joint Cybercrime Investigation Team

(g) National Cybercrime Research and Innovation Centre

25. The Committee though acknowledge the fact that the Expert Group constituted by the Ministry of Home Affairs in the year 2014, had submitted its Report in September, 2015 which had identified a number of gaps and challenges in tackling Cybercrimes and had specifically recommended to combat Cybercrime in the country and creation of Indian Cyber Crime Coordination Centre to strengthen the overall security apparatus to fight against Cybercrime, the decreasing trends on the reported frauds under the 'Card/Internet-ATM/Debit Card' have not been satisfactory and require urgent attention for revisiting the entire working of existing apparatus/mechanism for dealing with Cybercrimes. The Committee, therefore, urge the Ministry of Finance (Department of Financial Services) to take all the necessary steps to analyse the findings and recommendations of the said Expert Group with the help of all Indian Cyber Crime Coordination Centres so that the transfer of funds to the fraudsters can be stopped within no time and the culprits can be booked by the Investigation Agencies immediately. The Committee would like to be apprised of the necessary steps taken by the Ministry of Finance (Department of Financial Services) in this direction.

New Delhi;

18 December, 2023
27 Agrahayana, 1945 (Saka)

HARISH DWIVEDI,
Chairperson
Committee on Petitions

MINUTES OF THE THIRTIETH SITTING OF THE COMMITTEE ON PETITIONS (SEVENTEENTH LOK SABHA)

The Committee met on Monday, 18 December, 2023 from 1500 hrs. to 1715 hrs. in Committee Room No. 3, Parliament House Annexe Extension, New Delhi.

PRESENT

Shri Sunil Kumar Singh - In the Chair

MEMBERS

2. Shri Brijendra Singh
3. Shri Sushil Kumar Singh
4. Shri Manoj Kumar Tiwari
5. Shri Prabhubhai Nagarbhai Vasava
6. Shri Rajan Baburao Vichare

SECRETARIAT

1. Shri Raju Srivastava - Joint Secretary
2. Shri Tenzin Gyaltsen - Deputy Secretary

WITNESSES

*** *** *** ***

2. At the outset, in the absence of the Chairperson, the Committee under Rule 258(3) of the Rules of Procedure and Conduct of Business in Lok Sabha chose Shri Sunil Kumar Singh to act as Chairperson for the sitting.

3. Thereafter, the Chairperson welcomed the Members to the sitting of the Committee.

4. *** *** *** ***
5. *** *** *** ***
6. *** *** *** ***
7. *** *** *** ***
8. *** *** *** ***
9. *** *** *** ***
10. *** *** *** ***
11. *** *** *** ***
12. *** *** *** ***
13. *** *** *** ***

14. *** *** *** ***

15. The Committee, thereafter, took up for consideration the following draft Action taken Reports:-

(i) *** *** *** ***
(ii) *** *** *** ***

(iii) Action Taken Report on the action taken by the Government on the recommendations made by the Committee on Petitions (Seventeenth Lok Sabha) in their Fortieth Report on the representation of Shri Abhishek relating to increasing frauds in ATMs of Indian Overseas Bank, Indian Bank, Union Bank of India and Canara Bank in Mumbai - Urgent need to re-draw effective strategy for ATM transactions and other important issues related therewith;

(iv) *** *** *** ***
(v) *** *** *** ***
(vi) *** *** *** ***
(vii) *** *** *** ***
(viii) *** *** *** ***

16. After discussing the above mentioned eight draft Action Taken Reports in detail, the Committee adopted these Reports without any modification and authorised the Chairperson to finalise the draft Action Taken Reports and present the same to the House during the ensuing Session.

17. *** *** *** ***
18. *** *** *** ***

The Committee, then, adjourned.

*** *Does not pertain to this Report.*