FORTIETH REPORT

COMMITTEE ON PETITIONS

(SEVENTEENTH LOK SABHA)

MINISTRY OF FINANCE

(DEPARTMENT OF FINANCIAL SERVICES)

(Presented to Lok Sabha on 13.12.2022)

LOK SABHA SECRETARIAT
NEW DELHI

December, 2022/Agrahayana, 1944 (Saka)

CPB No. 1 Vol. XL

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

CONTENTS

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 Arvind Ganpat Sawant
8. Shri Brijendra Singh
9. Shri Sunil Kumar Singh
10. Shri Sushil Kumar Singh
11. Shri Manoj Kumar Tiwari
12. Shri Prabhubhai Nagarbhai Vasava
13. Shri Rajan Baburao Vichare
14. *Vacant*
15. *Vacant*

SECRETARIAT

1. Shri T.G. Chandrasekhar - Additional Secretary
2. Shri Raju Srivastava - Director
3. Shri Vivek Saini - Executive Officer

FORTIETH 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 Fortieth Report (Seventeenth Lok Sabha) of the Committee to the House 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 Fortieth Report at their sitting held on 12 December, 2022.

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.

12 December, 2022
21 Agrahayana, 1944 (Saka)

REPORT

REPRESENTATION RECEIVED FROM SHRI ABHISHEK REGARDING 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.

Shri Abhishek had submitted a representation dated 29.06.2022 to the Committee on Petitions 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 representationist, in his representation, *inter-alia* invited attention to the ever increasing numbers of ATM frauds in the financial capital of India, i.e., Mumbai and stated that as per reliable data recently published, Maharashtra, in general, and Mumbai, in particular, reported the highest number of ATM frauds in the entire country, followed by Delhi and Chennai. In Mumbai alone, people lost crores of rupees due to cloning or skimming of debit as well as credit cards. The anti-social elements are now employing various means to get control of people's bank accounts through ATM or debit cards. The most commonly used trick is installing skimmer devices on ATMs and Point-of-sale machines, which are then used to fraudulently copy data from cards. This data is then put on blank cards and illegal transactions are carried out. The representationist, in his representation, further stated that if we go into the modus operandi of this fraud, we find that various Banks have installed ATM machines in various parts of Mumbai. However, the Indian Overseas Bank, Indian Bank, Union Bank of India, and Canara Bank have the highest number of machines in Maharashtra, particularly in Mumbai. Since these banks have the highest number of machines, their daily transactions through ATM machines are also very high. When we discuss the ATM fraud, we find that the AM machines are rigged by these scamsters which is an indication that the Attendants/Security Personnel employed by these scamsters. Whenever any customer come to the ATM outlet to withdraw money through debit or credit card, their cards are cloned either through installing electronic devices or through some hidden camera. Since all these nefarious activities are done inside the Bank's ATM

outlets, it is the duty of these Banks to ensure that these types of activities are contained. Alarmed by these ATM frauds, particularly, in cities and towns of Maharashtra, the Reserve bank of India had asked the Banks to upgrade their ATMs or else face action. More particularly, in 2018, these Banks were asked to implement a host of security measures by August and upgrade all ATMs with supported version of operating system in a phased manner by June 2019. Anti-skimming devices prevent the skimmer from functioning. Similarly, white listing solutions allow only trusted applications to work on the ATM and block any other application. However, even today, that is over three years past the deadline, there has been no upgradation or insufficient updradation from these Banks and ATM frauds are going unabated. There could also be a situation that whenever these Banks upgrade their operations, the scamsters immediately devise means to overcome the fireballs installed by these Banks. It is also important to mention here that the Reserve Bank of India has also mandated these Banks to replace all existing magnetic stripe-only cards with EMV chip cards. Chip-based cards use higher standards of data encryption and storage technology compared to magnetic stripe cards. Sensitive customer data is stored on a chip in these, making it difficult for fraudsters to access customer information. The information in the chip is encrypted and so is the transmission of information thereon. However inspite of issuing EMV chip cards by these Banks, the ATM frauds have not stopped. In my view, these Banks have to adopt some innovative method to do away with the requirement of putting the 4-digit security code into the ATM Machine to withdraw money from the Debit/Credit Cards. Until and unless this practice is replaced by a new, innovative and technology driven method, like biometric signature, these ATM frauds would not going to stop. In this regard, these Banks may make an argument that changing the ATM Machines by making it biometric complaint would going to increase their financial burden. However, these Banks should think that the yearly money what they are losing due to these ATM Frauds would conveniently going to off-set the expenditure of making the ATM Machines biometric complaint. The representationist has, therefore, requested to look into the matter by examining aforementioned issues raised in his representation.

3. The Committee on Petitions (Seventeenth Lok Sabha) took up the representation of Shri Abhishek for examination under Direction 95 of the Directions by the Speaker, Lok Sabha. Accordingly, the representation was referred

to the Ministry of Finance (Department of Financial Services) for furnishing their comments on the issues raised in the representation along with a detailed List of Points.

4. In order to have realistic assessment of the issues/points raised in the representation of Shri Abhishek, the Committee undertook an on-the-spot study Visit to Mumbai on 15 September, 2022. During the said Study Visit, the Committee held informal discussion with the representative of the Ministry of Finance (Department of Financial Services) and representatives of Indian Overseas Bank, Indian Bank, Union Bank of India and Canara Bank.

5. The Committee desired to know the details of total number of ATMs or other Money Vending Machines installed by Indian Overseas Bank, Indian Bank, Union Bank of India and Canara Bank in Mumbai. The Ministry of Finance (Department of Financial Services)/Indian Overseas Bank/Canara Bank/Union Bank of India/Indian Bank, in a written reply, submitted the following information:-

Indian Overseas Bank

A total of 37 ATMs/Cash Recyclers are installed by our Bank in Mumbai.

Canara Bank

ATM Network Mumbai	*ONSITE*	*OFFSITE*	*TOTAL*	*METRO*	*URBAN*	*SEMI URBAN*	*RURAL*
TOTAL	*226*	*160*	*386*	*268*	*55*	*47*	*16*

Union Bank

Total number of ATMs installed by Union Bank of India in Mumbai is 515.

Indian Bank

Indian Bank has installed 117 ATMs in Mumbai as on 31.08.2022.

6. On being enquired by the Committee about the mechanism developed by the Government/Reserve Bank of India to contain online frauds/card cloning

(ATM/Debit Card, Credit card and Internet banking) in the country and the effectiveness of the measures adopted by these Banks to contain the problem, the Ministry of Finance (Department of Financial Services)/Indian Overseas Bank/Canara Bank/Union Bank of India/Indian Bank, in a written reply, submitted the following information:-

Indian Overseas Bank

Reserve Bank of India has issued directives to Banks in the year 2018 to install anti skimming devices in all the ATMs. Our Bank has complied with this directive fully and anti-skimming devices are installed in all our ATMs by the year 2019 itself. All the new ATMs procured by bank after 2018 are provided with anti-skimming devices

For E-com transactions involving Debit / Credit cards, second factory authentication has been implemented and structured alert messages with important information are being sent to the customers along with OTP, at the pre-approval stage of transaction.

IOB has successfully implemented fraud monitoring tool known as clari5 since 2019. The bank has developed various preventive scenarios after doing the due monitoring under monitoring scenarios.

This has also resulted in reduction in frauds related to Mumbai from 26 in FY 2019-20 to just 7 in FY 2021-22. Continuous fine tuning of scenarios makes the FTM tool more versatile.

Canara Bank

- *All our ATMs are enabled with EMV feature for security in ATMs.*
- *Implementation of Terminal Security Solution in all ATMs to ensure security from any malware attack.*
- *Ensuring disabling of USB ports, disabling auto-run facility, white-listing solution to ensure security in ATMs.*
- *Implementation of Transport Layer Security Solution in All ATMs to ensure secure communication between ATM terminal and ATM Switch.*

- *Canara Bank is the First Bank to complete implementation of Transport Layer Security (TLS) solution in all the ATMs.*

- *End to End Management Implementation and Management of E-surveillance of Capex ATM Sites Under OPEX Model.*

- *Upgradation of Operating System of ATMs/Cash Recyclers to latest version.*

Union Bank

To avoid Card Cloning, Union Bank of India is deploying ATMs with steel pin PAD and have shields covering all three sides to be recessed to avoid shoulder surfing or capture by the external camera. Bank has replaced all Magstripe card with EMV chip and PIN cards and set the road map for 100% anti-skimming implementation. Guidelines issued to all branches, Regional Offices, Zonal Offices as mentioned below:

Union Bank of India customers are advised to immediately block/de-active the card through channels such as UMOBILE, Call Centre, Branch.

Card transaction monitoring team investigate it and matters are taken up with NPCI. Based on the complaints received from banks, NPCI find compromise point of use of ATM/POS called CPP (Compromised point and Period) of cards through which unauthorized transactions are reported. NPCI also send the list of Union Bank of India's cards used in CPP for hot listing the cards which are hot listed/blocked by Bank's ATM switch team.

If CPP is in Union Bank of India ATM, branch is required to call CCTV ATM support provider for video footage of compromised period for further confirmation of Cloning activity and providing the same to NPCI /Police for investigation.

For preventions of frauds, Bank has implemented centre of external cyber threats by C-SOC and transaction related fraud controls in EFRM (Enterprise Fraud Risk Management). Moreover, Bank has implemented operational and technical controls in various channels to mitigate the risks of various types of

frauds such as phishing, KYC, identity theft, IB, UPI, Mobile banking, ATM etc.

Details of "nature of Cyber Frauds and the controls placed by the Bank to plug the said gaps" are as given under:

Sl. No.	Type of Cyber Frauds	Controls Placed by Bank
1.	Phishing sites& Rogue Mobile Apps	• Bank has formulated an Anti-phishing team for 24X7 monitoring • Periodic Email Phishing simulation exercises are conducted • Bank has implemented the Email security solutions • Bank has subscribed the Threat Intel services, Anti-phishing, Anti-rogue and other services to get the phishing URLs alert & subsequent take down services before causing any major damages to customers.
2.	ATM Card Skimming	• Bank has in place the Anti-Skimming solutions at ATM Terminals • The TSS (Terminal Security Solution) is implemented on all ATM terminals. • TLS 1.2 and above communication between ATM terminal to ATM Switch.
3.	Fraud Using Screen sharing App / Remote Access	• Bank is conducting a comprehensive awareness program for employees as well as customers. • Awareness information is available also in corporate website.
4.	SIM Swap/ SIM Cloning	• Bank's Mobile application are using SIM binding controls.

Digital transactions of Bank are governed by Digital Payment Security Framework prescribed by RBI as given below.

Sl. No.	Type of Delivery Channel	Security Controls Placed by Bank
	Internet Banking	• Dual Login (Web Portal user & Transaction user), 2FA through OTP, Hardware or Software token, strong CAPTCHA with anti-bot features for all retail /

		corporate customer with server-side validation in order to plug brute force/ DoS attacks and prevent its exploitation. • *DNS Security implemented to prevent DNS cache poisoning attacks and for secure handling of cookies.* • *Virtual keyboard option to avoid keystroke-based attacks.* • *Termination of online session within 2 minutes* • *Strict Password policy for maintaining both login / transactions passwords.* • *Same look and feel for both net banking portal and bills payment & presentment modules of billers* • *WAF with protection mode for server security* • *Network DDoS and Clean Pipe Service.*
	Mobile Banking	• *Dual Login PINs (Login and Transaction).* • *Encryption of Mobile Banking Application* • *Version check control through Bank's website and SMS for every new version release for Mobile App through authentic Play store of Mobile O/S.* • *Allowing app installation/ execution after baseline requirements are met.* • *Minimal data collection/ app permissions is ensured* • *Application containerization* • *Code obfuscation* • *WAF with protection mode for server security* • *Network DDoS and Clean Pipe Service* • *Device binding of Mobile App.*
	ATM / Card Payment Securi	• *PCI-DSS certification for ATM Switch* • *PoS terminals with PIN entry installed at the merchants for capturing card payments* • *Terminal Line Encryption – TLE through TLS 1.2 & above* • *CVV generation and validation through dedicated secured HSM* • *BIOS password, disabling USB ports, disabling auto-run facility, applying the latest patches of operating system and other software's, terminal security solution, time-based admin access* • *Implemented anti-skimming and white-listing solution* • *ATM terminals OS is upgraded with latest version.*

All these above measures adopted by the Bank i.e. anti-skimming devices in all the ATMs, and all our ATMs are EMV compliant etc., have collectively produced a very good result to prevent the ATM frauds.

While analyzing ATM related fraud cases reported during FY 2021-22, we observed that 90 percent of such cases were related to chargeback transactions where the transactions were authorized through magnetic stripe at ATM terminals of other banks.

Since all ATM terminals of our bank are now EMV compliant, fraudsters were using the cloned cards of our bank's customers' debit cards at Non-EMV compliant ATMs of other bank for withdrawing the money fraudulently.

ATM Frauds have been drastically reduced, w.e.f., 01-01-2022, i.e., when our bank (EFRMS implementation team) developed and deployed one rule in Fraud Navigator module which allowed Non-EMV ATM transactions (except Micro ATMs) up to a limit of Rs. 5000.00 in a day.

Indian Bank

We have implemented the following RBI guidelines to contain online frauds / card cloning:-

S. No.	RBI Guideline	Circular	Status
1	All ATMs should be provided with Anti-skimming feature to detect card skimming devices.	21.06.2018	Complied
2	All new Debit/Credit cards should be issued as EMV chip based cards and all magnetic stripe based cards should be replaced with EMV chip based cards.	27.08.2015	Complied
3	All ATM should be enabled for processing of EVM chip based Cards	26.05.2016	Complied
4	Mandatory Additional Factor Authentication (OTP based) for all online transactions	18.02.2009	Complied
5	At the time of issue / re-issue, all cards shall be enabled for use only at contact based points of usage [viz. ATMs and Point of Sale (PoS) devices] within India. Facility should be provided to the customers for enabling the online transactions and international transactions through internet banking, mobile banking or our branches based on their needs.	15.01.2020	Complied

Migrating all our cards from magnetic stripe to EMV and implementing EMV functionality in all our ATMs has helped our Bank in stopping magnetic stripe based ATM transactions in our ATMs since January 2020. It means, if a fraudster tries to withdraw cash from our ATM using a counterfeit magnetic stripe card, the transaction will be declined and cash will not be dispensed. As a result, fraudulent transactions through magnetic stripe mode are prevented in our ATMs since January 2020. Similarly, processing of fallback transactions (i.e. when an ATM is unable to read EMV chip data from the card, it will read the data from magnetic stripe) were stopped for other Bank ATMs since January 2020 and for our ATMs since August 2021 to decline unauthorized transactions attempted using counterfeit EMV cards. With effect from 1st April 2022, National Payments Corporation of India (NPCI) has also stopped processing of magnetic stripe transactions in their network. Hence no ATM fraudulent transactions are reported in other Bank ATMs after 31.03.2022.

7. The Committee further desired to know the quantum of ATM frauds reported under ATM/Debit Card/Credit Card/Internet Banking by Indian Overseas Bank, Canara Bank, Union Bank of India, Indian Bank in Mumbai during the last five years, the Ministry of Finance (Department of Financial Services)/Indian Overseas Bank/Canara Bank/Union Bank of India/Indian Bank in written reply furnished the following data:-

Indian Overseas Bank

(A). Amount involved Rs.1 lakh and above:

Bank (s)	2017-18		2018-19		2019-20		2020-21		2021-22	
	No. of Frauds	Amount involve (Rs. in crore)	No. of Fraud	Amount involved (Rs. in crore)	No. of Fraud	Amount involved (Rs. in crore)	No. of Frauds	Amount involved (Rs. in crore)	No. of Frauds	Amount involved (Rs. in crore
IOB	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA

(B). Amount involved Rs.1 lakh and below:

Bank(s)	2017-18		2018-19		2019-20		2020-21		2021-22	
	No. of Frauds	Amount involved (Rs. in crore)	No. of Frauds	Amount involved (Rs, in crore)	No. of Frauds	Amount involved (Rs. in crore)	No. of Frauds	Amount involved (Rs. in crore)	No. of Frauds	Amount involve d

										(Rs. in crore)
IOB	NA	NA	NA	NA	26	0.13	4	0.008	7	0.013

Canara Bank

(A) Amount Involved Rs. 1 lakh & Above – NIL

(B) Amount Involved Rs. 1 lakh and Below

Amount Involved Rs.1 Lakh and below										
Banks	2017-18		2018-19		2019-20		2020-21		2021-22	
	lo. of Frauds	Amount nvolved (Rs. In Cr)	lo. of Frauds	Amount nvolved (Rs. In Cr)	lo. of Frauds	Amount nvolved (Rs. In Cr)	No. of Frauds	Amount nvolved (Rs. In Cr)	lo. of Frauds	Amount Involved (Rs. In Cr)
Canara Bank	13	0.04	43	0.14	1	0.002	7	0.02	98	0.22

Union Bank

(A). Amount involved Rs. 1 lakh and above:

Bank Nam	2017-18		2018-19		2019-20		2020-21		2021-22	
	No of frauds	Amount involved In Cr.	No of frauds	Amount involved in Cr	frauds	Amount involved in Cr	No Of frauds	Amount involved in Cr	No of frauds	Amount involved In Cr.
UBI	2	0.24	2	2.95	13	0.26	3	0.04	3	0.04

(B). Amount involved Rs. 1. Lakh and below:

Bank Name	2017-18		2018-19		2019-20		2020-21		2021-22	
	No of frauds	unt involved In Cr.	No of frauds	Amount involved in Cr	o of frauds	nt involved in Cr	No of frauds	Amount involved in Cr	No of frauds	Amount involved In Cr.
UBI	40	0.09	34	0.08	103	0.30	138	0.36	102	0.23

Indian Bank

Details of frauds reported in Mumbai under ATM/Debit Card/Credit Card/Internet Banking

Bank	2017-18		2018-19		2019-20		2020-21		2021-22		2022-23	
Indian Bank	No of Frauds	Amount involved (In C	No of Frau	Amount involv	No of Fra	volved (In Cr)	No of Fra	Amount invo	No of Fra	volved (In Cr)	No of Fra	volved
	0	0	1	0.0125	0	0	1	0.0125	1*	0.0192	3	0.0
	Amount involved below Rs.1 lac											
ndian Bank	1	0.005	5	0.0112	13	0.0468	3	0.0122	14*	0.0462	36	0.12

** Out of the 15 frauds reported in 2021-22, only one fraud was reported in Indian Bank ATMs, for a transaction happened in February 2021. No fraud is reported in our ATMs in Mumbai since then.*

8. The Committee, thereafter, enquired about the details of the action taken by the Banks on various aspects pursuant to the issuance of Master Circular dt.1 July 2015,by the Reserve Bank of India on 'Frauds – Classification and Reporting' *inter alia* advising the Banks to examine the fraud cases, the Ministry, in a written reply, furnished the following information:-

Indian Overseas Bank

Reporting of ATM-related fraud cases in Mumbai to the Law Enforcement Agencies.

Our CCMGRC (Cyber Crime Monitoring and Grievances Redressal Cell) team is working 24X7X365 days and takes care of complaints. We are not reporting frauds directly to LEA, however we promptly reported to the queries of LEA and provided the required details like, CCTV footage/Account statement/KYC documents/debit freeze details and tracking of money movement to other payment merchant/Fis.

Staff accountability.
There is no involvement of staff in any unauthorized electronic transactions reported so far.

Proceedings against the erring staff.

Not Applicable

Steps taken to recover the amount involved in the fraud.

Whenever suspicious transaction happens or department receives the complaint regarding the suspicious transactions, Bank promptly follows up for

recovery of money. We provide all the inquired details to LEA which eventually helps them and bank in recovering the amount. Bank is continuously monitoring the NCRP portal for and updating the complaints for recovery of lost amount.

Claiming insurance, wherever applicable.

The Bank has taken Banker's Indemnity Policy, and for all frauds reported to Bank/detected by bank insurance claims are preferred with insurance provider promptly and followed up for claim settlement.

Streamlining the system as also the procedures so that frauds do not recur.

For identification and prevention of fraud our Bank has implemented EFRM solution since 2019 which is effectively deployed and is active till date. This EFRM solution "Clari5" helps us to identify various suspicious transaction patterns and also prevent the recurring fraudulent transactions through its Prevention Mode.

Canara Bank

The complaint with Law Enforcement Agencies (Police/ Cyber Police) is being filed by the customers in all cases to proceed further with the insurance claims as it is a pre-requisite. If the same is not filed by the customer, then the Bank is filing the complaint invariably.

Staff accountability is being fixed as per the policy guidelines of the Bank wherever involvement of staff is confirmed after internal investigation.

Action against the erring staff is being taken as per the policy guidelines of the Bank.

The complaint with Police/ Cyber Police is being filed by the customers in all cases to proceed further with the insurance claims to recover the amount.

Insurance is being claimed wherever applicable.

Bank is implementing all the security measures and streamlining the system and procedure so as to avoid the frauds.

Union Bank

Our bank files complaint with LEAs in all eligible cases. As per the RBI master direction on frauds, the cases below 1.00 lakh where staff involvement was not there, the filing of compliant with LEAs is not mandatory.

For the period 2015-16, 2016-17, 2017-18, 2018-19 & 2019-20, all the ATM fraud cases reported in Mumbai were committed by outsiders.

No staff was involved in ATM frauds.

Bank files complaint with LEAs in all eligible cases and lodges insurance claim in all the eligible cases.

Our Bank claims the insurance in all the eligible cases.

To minimize digital frauds, bank conducts segmentation review, control gap assessment and IS Audit periodically or on need basis. Bank also create awareness amongst customers through SMS and other digital channels not to share PINs, Passwords etc. to anyone including Bank staff. Digital Frauds through ATM Debit cards have reduced significantly since Bank is issuing only Chip based Cards to the customers. Green PIN generation facility has been provided instead of sending the PINs physically by Post to avoid any misuse. More system controls are brought in through implementation of DCMS (Debit Card Management System) for keeping better control for issuing of Debit Cards and its activation.

Indian Bank

No.	Guideline	Status of Compliance
1.	Reporting of ATM-related fraud cases in Mumbai to the Law Enforcement Agencies.	For all the cases reported during the five years period in Mumbai, police complaint / FIR was lodged by customer to the law enforcement. Further, customers are being advised to lodge police complaint / FIR and requested to submit the copy of the same at the time of reporting.
2.	Staff Accountability	Staff accountability is examined during the

		examination of fraud cases, in cases staff lapses is established (3 cases), necessary action is initiated against the erring staff
3.	*Proceedings against the errin*	*-do-*
4.	*Steps taken to recover the a fraud.*	*In addition to the recovery of the amount from the culprits through law enforcement agencies, we are also taking up the frauds with the online payment gateways, merchants and their banks to freeze the account of beneficiary of fraud transactions and to the refund the amount available in the account.*
5.	*Claiming insurance, wherever applicable*	*Bank has entered into the Bankers Indemnity Policy with M/s United India Insurance Company for an insurance coverage of Rs.10 Crores for loss incurred due to (i) cash loss in ATMs and (ii) fraudulent transactions through debit/credit cards, net banking, UPI, POS, AEPS etc.*
6.	*Streamlining the system as also the procedures so that frauds do not recur.*	*Bank has implemented various fraud prevention measures such as implementation of anti-skimming features, EMV technology, Fraud Risk Management System, Additional Factor Authentication for online transactions, facility to block the payment channels and other control measures to streamline the systems*

9. Regarding, the Reserve Bank of India Circular on 'Customer Protection - Limiting Liability of Customers in Unauthorized Electronic Banking Transactions dated 6 July 2017, the Committee enquired about the details of action taken by Indian Overseas Bank, Canara Bank, Union Bank of India, Indian Bank pursuant to the said Circular, Ministry, in a written reply, submitted the following information:-

Indian Overseas Bank

Our Bank has a Board Approved Policy in this regard and the same is published in the Bank's website for the information all customers and public. And the RBI 's policy directives are complied with by our Bank.

Entitlement of 'Zero Liability' in case of unauthorized transactions occurring due to contributory fraud/negligence/deficiency on the part of Bank and due to third party breach with customer in Mumbai notifying such transaction to

Indian Overseas Bank, Indian Bank, Union Bank of India and Canara Bank within three working days.

Bank in compliance to RBI circular is compensating the accountholders, as per their eligibility and in accordance to the RBI guidelines.

To credit (Shadow Reversal) by Indian Overseas Bank, Indian Bank, Union Bank of India and Canara Bank, the amount involved in unauthorized electronic transaction to the customer's account in Mumbai within ten working days from the date of such notification by the customer (without even waiting for settlement of insurance claim, if any)

Bank provides shadow credit in the account of the complainant immediately, without waiting for conclusion of bank's investigation or settlement of insurance claim as per RBI circular. The timelines are adhered to properly.

While implementing the Reserve Bank of India Circular dated 6 July 2017 on 'Customer Protection-Limiting Liability of Customers in Unauthorized Electronic Banking Transactions' by Indian Overseas Bank, Indian Bank, Union Bank of India and Canara Bank, the total monetary loss incurred by these Banks in Mumbai and on All India basis during the last five years.

The loss to bank in last 5 years pertaining to Mumbai alone is Rs. 11,56,179/- and the loss to bank in last 5 years is ₹ 1.64 crore on all India basis.

Canara Bank

Canara Bank is following the Zero Liability policy of the Reserve Bank of India.

Canara Bank is following all the guidelines for reported Card related Unauthorized Electronic Banking Transaction (UEBT) as per UEBT Policy for Customer Protection for Limiting Liability of Customers in Electronic Banking Transactions (EBT).

There is no monetary loss incurred by the bank for last 3 Financial years i.e. since 01.04.2020.

To make customers feel safe about carrying out electronic banking transactions our Bank has put in place appropriate systems and procedures

to ensure safety and security of electronic banking transactions carried out by customers.

Our Bank is always proactive in taking appropriate measures to mitigate the risks and protect customers from unauthorized transactions.

Union Bank

Our Bank has provided shadow credit in 560 cases of Mumbai.

Two ATMs of our Bank in Mumbai were cloned.

The total amount of Shadow credit of Union Bank Of India is Rs.48,61,970/-

The loss incurred for limited liability for the last 5 years is Rs. 0.54 Crore for Mumbai and Rs. 1.84 crore for all India.

Indian Bank

No.	Guideline	Status of Compliance
(i)	Entitlement of 'Zero Liability' in case of unauthorized transactions occurring due to contributory fraud/negligence/deficiency on the part of Bank and due to third party breach with customer in Mumbai notifying such transactions to Indian Overseas Bank, Indian Bank, Union Bank of India and Canara Bank within three working days.	Complied. Bank has implemented guidelines vide customer experience policy with regard to customer's entitlement to zero liability in cases of unauthorized transactions occurred due to contributory fraud/negligence/ deficiency on the part of Bank and due to third party breach. Also, for each transaction, Bank is sending an SMS alert to the customers, advising them to send an SMS "BLOCK" to 92895 92895 if the transaction is not done by them. It will block all types of online channels and prevent further transactions

(ii)	*To credit (Shadow Reversal) by Indian Overseas Bank, Indian Bank, Union Bank of India and Canara Bank, the amount involved in unauthorized electronic transactions to the customer's account in Mumbai within ten working days from the date of such notification by the customer (without even waiting for settlement of insurance claim)*	*Complied. The policy also covers guidelines with regard to providing shadow reversal for the amount involved on being notified by the customer within 10 working days from the date of notification.*

Monetary Loss Incurred By Indian Bank In Mumbai and on All India Basis During The Last Five Years While Implementing RBI Guidelines on Limiting Customer Liability

Financial Year		*No. of Cases*	*Amount (Rs.in crore)*	*Recovery Amount (Rs.in crore)*	*Insurance Amt Settled (Rs. in crore)*	*Loss (Rs.in crore)*
2017-18	*All India basis*	*42*	*0.40*	*0.12*	*0.10*	*0.18*
	In Mumbai	*1*	*0.01*	*0.00*	*0.00*	*0.01*
2018-19	*All India basis*	*89*	*0.79*	*0.12*	*0.15*	*0.52*
	In Mumbai	*6*	*0.02*	*0.00*	*0.01*	*0.01*
2019-20	*All India basis*	*161*	*1.16*	*0.30*	*0.38*	*0.48*
	In Mumbai	*13*	*0.05*	*0.00*	*0.03*	*0.02*
2020-21	*All India basis*	*89*	*0.74*	*0.33*	*0.41*	*0.00*
	In Mumbai	*4*	*0.02*	*0.00*	*0.00*	*0.02*
2021-22	*All India basis*	*94*	*0.37*	*0.10*	*0.07*	*0.20*
	In Mumbai	*15*	*0.07*	*0.01*	*0.02*	*0.04*
Total	***All India basis***	***475***	***3.46***	***0.97***	***1.11***	***1.38***
	In Mumbai	***39***	***0.17***	***0.01***	***0.06***	***0.10***

10. The Committee further enquired about the extent of compliance of Reserve Bank of India Circular dated 21 June 2018 on 'Control Measures for ATMs' in relation to the following aspects (i) Upgradation of ATMs software installed in Mumbai (ii) Issue of EMV Chip and Pin-based ATM Cards in Mumbai (iii) Providing customers with 24x7 access through multiple channels *via* website, phone banking, SMS, e-mail, IVR, dedicated toll-free helpline, etc., for reporting unauthorized transactions that have taken place and/or loss or theft of payment instrument, *viz.*, Card, etc., and Blocking ATM Card, Credit Card and pre-paid Card immediately if it is lost or stolen. The Ministry, in their written reply, submitted, as under:-

Indian Overseas Bank

Complied with

Canara Bank

The Operating System (Win 7 to Win 10) upgradation in ATMs of Mumbai region completed in 151 ATMs out of 368 ATMs and remaining are under progress.

All our ATMs are enabled with EMV feature for ensuring security in ATMs.

*Customers are provided with 24*7 access through multiple channels via website, phone banking, SMS, e-mail, IVR, dedicated toll-free helpline etc. for reporting unauthorized transactions that have taken place and/ or loss or theft of payment instrument, viz., Card ,etc.*

*Customers are provided with 24*7 access through multiple channels for blocking ATM Card / Credit Card and pre-paid card immediately if it is lost or stolen.*

Union Bank

Following Controlled Measures for Union Bank of India ATMs in Mumbai:-

Anti-Skimming solutions at ATM Terminals is in place. The TSS (Terminal Security Solution) is implemented on all ATM terminals. TLS 1.2 and above communication between ATM terminal to ATM Switch. Terminal Line Encryption – TLE through TLS 1.2 & CVV generation and validation through dedicated secured HSM. Windows 10 upgradation is ongoing (386 completed out of 515). RBI has given timeline up to 31.03.2023 to complete this activity. BIOS password, disabling USB ports, disabling auto-run facility, applying the

latest patches of operating system and other software, terminal security solution, time-based admin access.

Upgradation of ATMs software installed in Mumbai.

ATM terminals OS is upgraded with latest version.

Issue of EMV Chip and Pin-based ATM Cards in Mumbai.

EMV Chip and Pin-based ATM Cards issued.

Providing customers with 24x7 access through multiple channels via website, phone banking, SMS, e-mail, IVR, dedicated toll-free helpline, etc., for reporting unauthorized transactions that have taken place and/or loss or theft of payment instrument, viz., Card, etc.

The System is in place providing customers with 24x7 access through multiple channels.

Blocking ATM Card, Credit Card and pre-paid Card immediately if it is lost or stolen.

The System is in place for blocking the cards if it is lost or stolen.

Indian Bank

(i)	*Upgradation of ATMs Software installed in Mumbai.*	*Complied. Based on the directions, we had upgraded all our ATMs from Windows XP to Windows 7 Operating System. Currently upgradation to Windows 10 is under progress. It is expected to be completed by 31.12.2022*
(ii)	*Issue of EMV Chip and PIN-based ATM cards in Mumbai*	*Complied. All cards are EMV Chip and PIN-based cards.*
(iii)	*Providing customers with 24x7 access through multiple channels via website, phone banking, SMS, e-mail, IVR, dedicated toll-free helpline, etc. for reporting unauthorized transactions that have been taken place and/or*	*Complied. Facility for reporting the unauthorized transactions has been provided through website, Mobile banking App, SMS, e-mail, IVR, toll-free helpline etc. on 24x7 basis.*

	loss or theft of payment instrument, viz. Card, etc.	
(iv)	*Blocking ATM Card, Credit Card and Pre-paid Card immediately if it is lost or stolen.*	*Complied. Facility for blocking the cards is provided through internet banking, mobile banking App, toll-free helpline and also at our branches.*

11. Thereafter, the Committee in order to get the finer details of the subject desired to know the other out-of-box measures that could be introduced by these Banks to contain the ATM frauds in the country, in written reply, the Ministry of Finance (Department of Financial Services)/Indian Overseas Bank/Canara Bank/Union Bank of India/Indian Bank, in a written reply, furnished the following:-

Indian Overseas Bank

ATM Skimming frauds happen mostly in fallback mode. This happens when ATM Terminal is unable to read card Chip, and transaction is put through using static data in the Magnetic Stripe of the card. We have blocked such transactions for our cardholders when transaction is attempted from other Bank ATM.

For transactions made by our card in our own ATM terminal, fallback transactions are currently allowed as count of such transactions are high. Bank has therefore proposed to introduce additional factor of authentication i.e. authorization of cash withdrawal in Fallback mode based on OTP to be sent to the registered mobile of the customer in addition to asking for Card PIN by the ATMs.

Canara Bank

Canara Bank has already implemented Terminal Security Solution in all ATMs to ensure security from any malware attack.

Canara Bank has already Implemented Transport Layer Security Solution in All ATMs to ensure end-to-end secure communication between ATM terminal and ATM switch.

Canara Bank is the First Bank to complete implementation of Transport Layer

Security (TLS) solution in all the ATMs.

Canara Bank has centralized the reconciliation process of cash in ATMs to ensure timely and immediate reconciliation.

Bank is in the process of implementation of E-Surveillance mechanism at the ATM lobbies to ensure timely alerts and quick response. The e-surveillance is expected to ensure detection of intrusions or unauthorized activities in the ATM premises. This system helps in fighting against ATM theft and vandalism.

Bank has implemented anti-skimming device in all the ATMs to safeguard customer transactions.

Union Bank

For preventions of frauds, Bank has implemented centre of external cyber threats by C-SOC and transaction related fraud controls in EFRM (Enterprise Fraud Risk Management). Moreover, Bank has implemented operational and technical controls in various channels to mitigate the risks of various types of frauds such as phishing, KYC, identity theft, IB, UPI, Mobile banking, ATM etc

Indian Bank

We are in the process of implementing card-less cash withdrawal facility in our ATM, using the alternate authentication methods such as UPI PIN, Mobile Banking password and One Time Password, which will improve the security of ATM transactions and eliminate ATM frauds.

12. The Committee, taking a composite view of the issue, enquired that various types of frauds take place owing to utter negligence and/or ignorance of customers while using ATMs due to which the Banks have to incur financial loss. The Committee also asked if there is any mechanism available with these Bank(s) to distinguish frauds that occurred due to; (i) negligence on the part of Bank(s); and/or (ii)negligence/ignorance on the part of Customers while compensating the ATM users, the Ministry of Finance (Department of Financial Services)/Indian Overseas Bank/Canara Bank/Union Bank of India/Indian Bank, in a written reply, submitted, as under:-

Indian Overseas Bank

We have a mechanism in place to determine as to where the negligence is – whether on the part of customer or in the system, and the same is taken into account while compensating the customer.

Canara Bank

Canara Bank is following the Zero Liability policy of the Reserve Bank of India related to Unauthorized Electronic Banking Transaction.

Third party breach where the deficiency lies neither with the bank nor with the customer, Bank receives the insurance claim to compensate ATM users.

Union Bank

Bank has in place mechanisms to distinguish frauds.

EFRM Alert system has been introduced by TM &FM vertical.

Technology related Fraud Scrutiny committee (TRSFC) has been formed comprising members from RMD, CISO, CAID, Legal, DIT, ATM cell verticals to deliberate on fraudulent cases reported by customers/Branches/ROs.

CCTV Footage-Branch must get it through the help of ATM vendor/MS/E2E vendor. Branches will check functioning of CCTV footage and will preserve footage for disputed transactions.

Electrical Journal (EJ), Switch report, SMS/OTP logs, CPP alert referred as evidence.

Indian Bank

As far as ATM transactions are concerned, any transaction received in EMV mode is considered as a transaction performed using the original card issued to the customer. Fraudulent transactions done using counterfeit cards will be received either in magnetic stripe mode or in fallback mode. Hence if an EMV transaction is reported as fraudulent, it is considered as a negligence on the

part of customer since the such transaction can happen only if the original card and PIN are misplaced by the customer.

One Time Password (OTP) sent to the registered mobile number of the customers is mandatory for successful completion of the online transaction performed in India. Hence fraudulent online transactions are considered as a negligence on the part of customer when
(i) The OTP received by the customer is shared with the fraudster during vishing calls; or
(ii) The customer clicks on a link shared by fraudster and installs an application in the smartphone which provides remote access of the smart phone to the fraudster.

OBSERVATIONS/RECOMMENDATIONS

Electronic mode of transaction *vis-à-vis* customers' confidence

13. 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.

14. 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.

Methods to outsmart the fraudsters'

15. 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.

16. 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.

User-friendly and Integrated System of filing fraud-related complaints

17. 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 lac 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.

18. 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.

Setting up of an 'All India Agency' for investigation of bank-related frauds

19. 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.

NEW DELHI;

HARISH DWIVEDI,
Chairperson,
Committee on Petitions.

12 December, 2022
21 Agrahayana, 1944 (Saka)

CONFIDENTIAL

MINUTES OF THE TWENTY-FIFTH SITTING OF THE COMMITTEE ON PETITIONS (SEVENTEENTH LOK SABHA)

The Committee met on Monday, 12 December, 2022 from 1500 hrs. to 1700 hrs. in Committee Room 3, Block A, Parliament House Annexe Extension, New Delhi.

PRESENT

Shri Harish Dwivedi - Chairperson

MEMBERS

2. Shri Anto Antony
3. Shri Hanuman Beniwal
4. Prof. Sanjay Sadashivrao Mandlik
5. Dr. Jayanta Kumar Roy
6. Shri Arvind Ganpat Sawant
7. Shri Brijendra Singh
8. Shri Sunil Kumar Singh

SECRETARIAT

1. Shri T. G. Chandrasekhar - Additional Secretary
2. Shri Raju Srivastava - Director

2. At the outset, the Hon'ble Chairperson welcomed the Members to the sitting of the Committee.

3. The Committee, thereafter, took up for consideration the following Draft Reports :-

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

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

(iii) *** *** *** *** *** ***

(iv) *** *** *** *** *** ***

(v) *** *** *** *** *** ***

(vi) 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; and

(vii) *** *** *** *** *** ***

4. After discussing the above mentioned Draft Reports in detail, the Committee adopted all the seven Reports with minor modification(s). The Committee also authorised the Chairperson to finalise the Draft Reports and present the same to the House.

The Committee, then, adjourned.

***