SHRI VEERSHAIV CO-OP BANK LTD; KOLHAPUR (MULTI-STATE BANK)

LIMITED LIABILITY POLICY

(Customer protection – Limited Liability of Customers in Unauthorized ELECTRONIC Banking Transaction)

F.Y.2023-2024

CONTENTS

BACKGROUND

Co-operative Banks in India have become an integral part of the success of Indian Financial Inclusion story. They have achieved many landmarks since their formation and have helped a normal rural Indian to feel empowered and secure.

With the increased thrust on IT enabled financial inclusion and related customer protection issues, and considering the recent surge in customer grievances relating to unauthorized transactions resulting in debits to their accounts/cards, the criteria for customer liability in these circumstances have been reviewed.

The systems and procedures in Bank is designed to make customers feel safe 24/7 about carrying out electronic banking transactions with their account. To achieve this mechanism with guidelines to the concerned department about ATM/Debit card services. To achieve this, Bank has fulfilled the prescribed guidelines:

1. PREAMBLE

Shri Veershaiv Co op Bank Ltd,Kolhapur., (hereinafter referred to as the "Bank") provides banking Services through its branch network of 30 branches. The bank has adopted and implemented this Limited Liability of Customers Policy (hereinafter referred to as the "Policy") with a view to regulate the business of the Bank and it outlines the requirements and condition under which a department or program obtains authorization to operate electronic banking transactions of the Bank and how the electronic banking payment operation is expected to be established and managed. As per this Policy, any existing customer or even the non-customer may avail the benefit of the Bank's Services. The Bank have enabled merchants to accept all Visa/ MasterCard/RuPay cards for payment. The Bank branch team executives are always available to assist the Bank's customers for their various needs.

3. OBJECTIVES OF THE POLICY

The objective of this policy is to Limiting the Liability of Customers in Unauthorized Electronic Banking Transactions and also Strengthening of systems and procedures to a wider segment of banks across all geographical locations and to provide procedure, requirements, and condition under which a liability of both i.e., bank and customers are given under this policy.

We have set up internal control system to combat fraud prevention committees/task forces which formulate laws to prevent frauds and take proactive fraud control and enforcement measures.

4. SCOPE

a) Provide access to financial payment services to every citizen along with ability to conduct card transactions.
b) To equip each collection point with a method to accept online card payments.
c) Migrate payment transactions from cash dominated to non-cash dominated transactions.
d) Liability of Customers of Co-operative Banks in Unauthorized Electronic Banking Transactions.

5. OWNERSHIP & CUSTODIAN OF THE POLICY

The Operations Department shall be the owner of this Policy.

6. APPLICABILITY

This Policy is applicable to all stakeholders and third party vendors.

7. RESPONSIBILITY

The Bank's Management is responsible for approval and execution of the Policy. The time of review of policy and the management of the same will be taken care from time to time.

8. VALIDITY

This policy will continue to be in force till the reviewed policy comes into place.

9. DEFINITIONS :

A	**Acquirer Bank**	is the Bank which has acquired the transaction orthe Bank whose Point of Sale (PoS) terminal has been used.
B	**Debit Card**	a card issued by a bank allowing the holder to transfermoney electronically to another bank account when making a purchase.
C	**Cardholder**	is a Non-consumer or consumer customer to whom a payment card is issued to or any individual authorized to use the payment card.
D	**Issuer**	is the Bank in which the cardholder has his/her account and holds card issued by the Bank.
E	**Merchants**	are Entities, which agree to accept credit cards/DebitCards/ATM cards for payment of Goods & Services.
G	**Onsite**	are ATM machines that are set up in the premises where there is a bank branch so that both the

	ATMs	physical branch and the ATM can be used. This is known as being on site and this can be used for several purposes. Many people can use this to avoid the lines that are present in the branch and hence save on the time required to complete their transactions.
H	**Third Party Vendor**	means a service provider through whom either the services are availed or offered.

10. Customer Responsibility-

Customers must take appropriate measures to safeguard their accounts/ cards by using strong Passwords and Pins, which need to be changed at regular intervals. Pins/ Passwords and OTP must not be shared with anyone via email or telephone including employees of the Bank. The Bank will never ask for such credentials. It is the responsibility of the customer to promptly report any unauthorized transaction on the account/ card to Bank.

11. BANK's RESPONSIBILITY FOR ESTABLISHING SYSTEMS AND PROCEDURES UNDER THE LIMITED LIABILITY POLICY :

The systems and procedures are been strongly strengthened & designed by the Bank to make customers feel safe while executing of electronic banking transactions. Bank's Management, concerned departments and vendor have been taking care for strengthening system and procedure of e-banking secured practice and also developed IT infrastructure as per RBI guidelines.

Bank has divided and created electronic banking transactions into two categories in order to make customers feel safe and secure while performing of the banking transactions:

a) Remote/ online payment transactions – These transactions do not require physical transactions and pre-paid Payment Instruments
b) Face-to-face/proximity payment transactions

For safe and secured e-banking services, bank has followed certain checklists as per the RBI guidelines. The said checklist is as follows:

a) Establishing and organizing the strong reporting mechanism which is tested, audited for customer friendly services.
b) Developing and maintaining security measures for ensuring safety and security of customer e-transactions.
c) Establishing and managing robust and dynamic fraud detection and prevention mechanism. In line with NPCI guidelines, the Bank is sending alerts to customers for

business decline viz. Pin tries exceeded, Invalid PIN, Insufficient Funds, per transaction limit exceeded.

d) Developing mechanism to assess the risks resulting from unauthorized transactions and measure the liabilities arising out of such events (ATM Debit card frauds or unauthorized transactions);

e) Developing appropriate measures to mitigate the risk and protect customers against the liabilities arising there from; and

f) Establishing effective system of continually, repeatedly, advisory methods, for customer as awareness program for protecting themselves from electronic banking and payment related frauds.

g) Establishing and organizing information security governance framework (consist of the leadership organizational structure and process that safeguard information)

h) Assignments of roles accountability

i) Establishing effective access management

j) Continuous monitoring, reviewing, exception reporting and taking action thereof for improving the effectiveness of the said policy.

k) Control measures have taken by the bank in order to reporting of the unauthorized transactions by the customer.

12. REPORTING METHOD OF UNAUTHORISED TRANSACTION BY CUSTOMER TO BANK:

Limited liability policy provides management directives towards reporting mechanism for limited liability within the Bank and recommends appropriate security controls that need to be implemented and maintain and manage Cyber crime related issues or unauthorized transactions incidents in the Bank. Bank strives to secure methods of electronic banking transactions by ...

a) We are asking or informing our customers to register for SMS alerts and, wherever available, register for e-mails alerts for electronic banking transactions.

b) We notify our customers for notification of any unauthorized electronic banking transaction at the earliest after the occurrence of such transaction

c) We have established e-banking services to the customers with 24x7 access through multiple channels at a minimum, via website, e-mail, a dedicated toll-free helpline, reporting to home branch, etc. for reporting unauthorized transactions that have taken place and/or loss or theft of payment instrument such as card, etc.

d) We have enabled immediate response mechanism for our customers acknowledging the complaint registered with the complaint number.

e) The bank may not offer facility of electronic transactions, other than ATM cash withdrawals, to customers who do not provide mobile numbers to the bank.

f) We have established a direct link for lodging the complaints, with specific option to report unauthorized electronic transactions on home page of Bank's website.

g) For avoiding unauthorized transactions liability, the Bank has improved "Vendor Management system and procedure" and also taken Legal Protection against the third party breaches.

13. LIMITED LIABILITY OF CUSTOMER

New features are established by the Bank with reference to the RBI's guidelines, to enhance the Limiting Liability of Customers in Unauthorized Electronic Banking Transactions and which helps in smooth functioning of the ATM transactions.

Under certain circumstances customers will be held liable for the loss occurred due to unauthorized transactions as per the RBI guidelines.

Bank has established the criteria for managing customer limited liability against unauthorized transactions:

A) Zero Liability of a Customer

A customer's entitlement to zero liability shall arise where the unauthorized transaction occurs in the following events:

a) Contributory fraud/ negligence/deficiency on the part of the Bank (irrespective of whether or not the transaction is reported by the customer).
b) Third party breach where the deficiency lies neither with the Bank nor with the customer but lies elsewhere in the system, and the customer notifies the Bank within 'three working days' of receiving the communication from the Bank regarding the unauthorized transaction.

B) Limited Liability of a Customer

A customer shall be liable for the loss occurring due to unauthorized transactions in the following cases:

When it is found that the loss is due to customer's negligence, where he has shared the payment credentials (such like card number, expiry date, OTP, OAC, PIN No, CVV No.), to known or unknown persons then the customer will bear the entire loss until he reports the unauthorized transaction to the Bank. Any loss occurring after the reporting of unauthorized transaction shall be borne by the Bank.

a) In cases where the responsibility for the unauthorized electronic banking transaction lies neither with the bank nor with the customer, but lies elsewhere in the system and the customer notifies the bank of such a transaction within **four to seven working days** of receiving a communication of the transaction, the per transaction liability of the customer shall be limited to the transaction value or the amount mentioned in below table, whichever is lower.
b) However the bank will not be liable for any loss caused by a technical breakdown of the payment system if the breakdown of the system was recognizable for the cardholder by a message on the display of the device.

c) **Maximum Liability of a Customer**

Type of Account	Maximum liability
• BSBD Accounts	5,000
• All other SB accounts • Pre-paid Payment Instruments and Gift Cards • Current/Cash Credit/Overdraft Accounts of MSMEs • Current Accounts/Cash Credit/Overdraft Accounts of individuals with annual average balance (during 365 days preceding the incidence of fraud)/ limit up to Rs.25 lakh • Credit cards with limit up to ` 5 lakh	10,000
• All other Current/Cash Credit/Overdraft Accounts	25,000

d) If the delay in reporting is beyond **seven working days**, the customer liability will be determined as follows-

a) The Bank will consider the request received up to 89 days from receiving a communication of the transaction.
b) The Bank reserves the right to reject any request received on or after 90 days, for refund of amount on account of unauthorized electronic transactions.
c) Per transaction liability of the customer shall be determined as per the rule applicable to reporting within 4 to 7 working days.
d) Overall liability of the customer in third party breaches, where the deficiency lies neither with the bank nor with the customer but lies elsewhere in the system, is summarized below

from Time taken to report the fraudulent transaction the date of receiving the communication	**Customer's liability**
Within 3 working days	Zero liability
Within 4 to 7 working days	The transaction value or the amount mentioned in above Table, whichever is lower

Beyond 7 working days	The Bank will consider the request received upto 89 days from receiving a communication of the transaction. Per transaction liability of the customer shall be determined as per rule applicable to reporting within 4 to 7 working days.

The number of working days mentioned above shall be counted as per the working schedule of the home branch of the customer excluding the date of receiving the communication.

14. LIMITED LIABILITY POLICY STATEMENTS

Bank is committed to protect and safeguard the e-banking services from unauthorized transactions. Bank needs to ensure secure business operations for liability of unauthorized transactions.

Bank has established system and process for business sensitive, efficient, effective, and robust security environment that safeguards all e-banking services and assets of the bank which demonstrate our commitment provide safe and secured services to our constituents.

This policy provides management derivatives towards e-banking services within the bank and recommends and implements security standards.

15. LIABILITY TOWARDS UNAUTHORIZED TRANSACTIONS

In certain situations where Bank is liable to pay –

a) In the event of any bank's vendor or service provider is found negligent to provide secure ATM/Debit Card related services
b) If any third party vendor or Bank's service provider breaches and compromises sensitive data to unknown source which Banks customers results in ATM fraud
c) If Bank or Banks vendor found guilty due to non-compliance or became a part of any fraudulent activity
d) In case if bank is unable to resolve the complaint , or determine the customers' liability within 90 days, then the liability will be on the Bank
e) In case of ATM/Debit card cloned through bank's ATM machine then the liability will be on the Bank and not on the Customer.
f) If any direct losses incurred by a cardholder due to a banks system malfunction directly within the bank's control, Bank shall be responsible.

g) Bank's responsibility for the non-execution or defective execution of the transaction is limited to the principal sum and the loss of interest is subject to the Bank's Board policy.

h) Bank should make available to the all the customers in writing, a set of contractual terms and conditions governing the issue and use of such as ATM card / Debit card/ Account details

16. REVERSAL TIMELINE FOR LIMITED LIABILITY OF CUSTOMER

Bank has established reversal timeline for zero liability of the customer which are as follows:

a) Bank has established the strong reporting mechanism as per the RBI guidelines.

b) Bank has established various departments for reporting of the cases in order to make it easier for customers.

c) Departments such as IB cell, ATM cell, IT department, Data Centre and Risk Department have been established for strengthening system and procedure of e-banking transactions.

d) In the event of notification given by the customer, bank shall credit (shadow reversal) the amount involved in the unauthorized electronic transaction to the customer's account within 10 working days from the date of such notification by the customer (without waiting for settlement of insurance claim, if any).

e) The credit shall be value dated to be as of the date of the unauthorized transaction.

f) Bank at their discretion may decide to waive off customer's liability in case of unauthorized electronic banking transactions even in cases of customer negligence.

17. BOARD APPROVED POLICY FOR CUSTOMER PROTECTION

Bank has formulated the Limited Liability of the Customers policy in case of E-banking, electronic transactions as per the RBI. Following are the rules and regulations laid down by the RBI which are been followed and implemented by the board in this policy:

a) The policy includes establishing of mechanism for creating customer awareness on the risks and responsibilities involved in electronic banking transactions.

b) Bank provides for robust grievance redressal structure, escalation matrix, and clear timelines for resolution of customer complaints.

c) Establishing and managing strong system as to the reporting and monitoring of the unauthorized transactions are been established.

18. BURDEN OF PROOF

The burden of proving customer liability in case of unauthorized electronic banking transactions lies on the Bank.

Customer should submit following documents / details

Shri Veershaiv Co-op. Bank Ltd. H. O. Tararani Chowk, Kolhapur (Multi-State Bank)

a) Duly filled up Dispute Management Form
b) Copy of FIR lodged with Police Authorities
c) Proof of his / her presence at a place other than the location of alleged fraud
d) Physical ATM / Debit card for hot listing

Following documents / details will be taken on record from concerned other Bank-

a) CCTV footage / Recording of the said ATM transactions along with 3 previous and 3 succeeding transactions to analysis.
b) ATM images
c) No Excess Cash Certificate
d) ATM Switch Report
e) Electronic Journal along with 3 previous and 3 succeeding transactions to analysis.
f) Duly signed Bank Account statement for 6 months (if required).
g) EOD Cash Balancing report.
h) SMS details.
i) Any other report as per requirement

Submission of all documents is necessary to consider / process the claim. In case of non-receipt of all documents within 45 days from an application, the Bank reserves the right to reject the claim.

19. REPORTING AND MONITORING

Bank has robust Reporting and Monitoring structure for e-banking unauthorized transactions.

a) Bank has established mechanism and structure for reporting of e-banking, online unauthorized electronic banking transactions for customer security.
b) The said reporting will be submitted to the Board or committee established by bank on Monthly basis.
c) The reporting should be specific, number of cases and the values involved and accordingly the distribution across various categories of cases.
d) All such transactions report should be reviewed by the bank's internal auditors on monthly intervals.
e) The report should be present in front of board for periodic review and based on the report along with the guidance of Board. They will establish consumer grievance strategy for avoiding liability of unauthorized banking transactions of the customer.

20. AWARENESS AMONGST CUSTOMERS

a) The Bank from time to time will create sufficient awareness amongst its customer's as to the risk and responsibilities involved in electronic banking transactions, and customer's liability in case of unauthorized transactions.
b) We had executed terms to put the cardholder under an obligation to take all appropriate steps to keep safe the card and the means (such as PIN or code) which enable it to be used.

Shri Veershaiv Co-op. Bank Ltd. H. O. Tararani Chowk, Kolhapur (Multi-State Bank)

21. REFERENCES

This Policy has been drafted with reference to the Guidelines issued by the Reserve Bank of India on Limiting Liability of Customers of Co-operative Banks in Unauthorized Electronic Banking Transactions.

a) RBI/2017-18/109-CBR.BPD.(PCB/RCB).Cir.No.06/12.05.001/2017-18-Limiting Liability of Customers of Co-operative Banks in Unauthorized Electronic Banking Transactions

b) RBI/2015-16/229 -DCBR.BPD.(PCB/RCB) Cir. No. 6 /19.51.026/2015-16 -Internet Banking Facility for Customers of Cooperative Banks

c) RBI/2007-2008/95 - UBD (PCB) Cir No. 6 /09.18.300/2007-08 - Guidelines for issue of ATM-cum-Debit Cards by UCBs.

d) RBI/2014-15/577 -DCBR.CO.BPD.(SCB).No.1/13.05.000/2014-15-First RBi- monthly Monetary Policy Statement 2015-16 – Issue of Credit Cards by Scheduled Urban Cooperative Banks.

e) NPCI Circular No. NPCI / 2013-14/NFS/101 DT. 10.12.13

22. CUSTOMER GRIEVANCE REDRESSAL

In case of customer complaints in connection to unauthorized electronic banking transactions, the customer shall contact the bank on:

Helpline no.-9558575551 If not attended then attempt No.

Email id –atmcc@shriveershaivbank.com

Grievance officer details -Mr.Somnath.G.Gavali

23.RIGHT TO CHANGE THE POLICY

Board of Directors will reverse the right to change the policy from time to time.

Read and passed in the Board of Directors Meeting as per Board Meeting Resolution No.12.Dated.-02/09/2022.

Shri Veershaiv Co-op. Bank Ltd. H. O. Tararani Chowk, Kolhapur (Multi-State Bank)

Manager,
Shri Veershaiv Co-op. Bank Ltd; Kolhapur.

MANAGING DIRECTOR
Shri Veershaiv Co-op. Bank Ltd. Kolhapur.
(Multi-State Bank)

-------- *** END *** --------

Shri Veershaiv Co-op. Bank Ltd. H. O. Tararani Chowk, Kolhapur (Multi-State Bank)