DHANLAXMI BANK

CUSTOMER RELATIONS POLICY

Version: 9 (2025)

Table of Contents

1. Introduction

Banking is a service industry, where customer is the most essential ingredient for its successful operation. Reserve Bank of India, over a period of time has enunciated various regulatory directives, which is based on certain principles and practices. Studies conducted by various committees such as the Talwar Committee, Goiporia Committee, Tarapore Committee, etc., are the pillars on which customer service policy of banks are built. We have taken all the possible steps to imbibe the spirit of RBI directives.

Broadly, a customer can be defined as a user or a potential user of bank services. A 'Customer' may include:

- A person or entity that maintains an account and / or has a business relationship with the bank;
- One on whose behalf the account is maintained (i.e. the beneficial owner).
- Any person or entity connected with a financial transaction which can pose significant reputational or other risks to the bank, say, a wire transfer or issue of a high value demand draft as a single transaction.
- Beneficiaries of transactions conducted by professional intermediaries, such as Stock Brokers, Chartered Accountants, Solicitors, etc. as permitted under the law.

1.1 Infrastructure facilities at branches:

Branches shall provide sufficient customer service space, adequate furniture, drinking water facility etc. People with physical infirmities like pensioners, senior citizens, disabled persons, etc., will be provided with special treatment. Branches will provide special infrastructure support for physically challenging and aged customers.

1.2 Separate enquiry counters at branches:

With the advent of electronic banking, the customer's experience of banking is no longer fully under the control of the bank. Fraudsters constantly creating more diverse and complex fraudulent ruses are using advanced technology and social engineering techniques to commit the frauds. Spreading awareness among consumers has become imperative. Continual education and timely information provided to customers will help them to understand security requirements and take appropriate steps in reporting security problems.

Taking into account the risks arising out of unauthorized debits, the Bank has incorporated RBI's *Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions* (DBR.No.Leg.BC.78/09.07.005/2017-18 dated July 6, 2017) into this policy. The Bank has also aligned this policy with the *Integrated Ombudsman Scheme, 2021* and *Internal Ombudsman Directions, 2023*. Accordingly, the policy stipulates clear liability limits, mandatory timelines for re-credit (10 working days), and the mechanism for proactive compensation and customer awareness.

Based on the same, Bank has formulated our "Customer Relations Policy" to comply with the guidelines of Reserve Bank of India.

2. Objective & Scope

In the endeavor to provide the best services to customers, the Bank has formulated its Customer Relations Policy. The policy guidelines aim to assist the staff in rendering high-quality customer service consistently and to continually improve its services. The objective of this policy is to highlight the quality standards to be adopted by the Bank for rendering high-quality customer service.

3. Electronic Banking Transaction - Strengthening of systems and procedures

The systems and procedures in bank are designed to make customers feel safe about carrying out electronic banking transactions. To achieve this, bank has put in place:

- Appropriate systems and procedures to ensure safety and security of electronic banking transactions carried out by customers;
- Robust and dynamic fraud detection and prevention mechanism;
- Mechanism to assess the risks (for example, gaps in the bank's existing systems) resulting from unauthorized transactions and measure the liabilities arising out of such events;
- Appropriate measures to mitigate the risks and protect themselves against the liabilities arising there from; and
- A system of continually and repeatedly advising customers on how to protect themselves from electronic banking and payments related fraud.

Broadly, the electronic banking transactions can be divided into two categories:

- ✓ Remote/ online payment transactions (transactions that do not require physical payment instruments to be presented at the point of transactions e.g., internet banking, mobile banking, card not present (CNP) transactions), Pre-paid Payment Instruments (PPI), and
- ✓ Face-to-face/ proximity payment transactions (transactions which require the physical payment instrument such as a card or mobile phone to be present at the point of transaction e.g., ATM, POS, etc.)

4. Electronic Banking Transaction - Roles and Responsibility of the Bank

- The Bank shall advise its customers to mandatorily register for SMS alerts and wherever available register for e-mail alerts, for electronic banking transactions. The SMS alerts shall mandatorily be sent to the customers, while email alerts may be sent, wherever registered.
- The customers shall be advised to notify their bank of any unauthorized electronic banking transaction at the earliest after the occurrence of such transaction, and informed that the longer the time taken to notify the bank, the higher will be the risk of loss to the bank/ customer.

- The Bank shall provide customers with 24x7 access through multiple channels (at a minimum, via website, phone banking, SMS, e-mail, IVR, a dedicated toll-free helpline, reporting to home branch, etc.) for reporting unauthorized transactions that have taken place and/ or loss or theft of payment instrument such as card, etc.
- Bank shall also enable customers to instantly respond by "Reply" to the SMS and e-mail alerts and the customers need not search for a web page or an e-mail address to notify the objection, if any. Further, a direct link for lodging the complaints, with specific option to report unauthorized electronic transactions will be provided by the bank on home page of our website.
- The loss/ fraud reporting system shall also ensure that immediate response (including auto response) is sent to the customers acknowledging the complaint along with the registered complaint number. The communication systems used by bank to send alerts and receive their responses thereto will record the time and date of delivery of the message and receipt of customer's response, if any, to them. This shall be important in determining the extent of a customer's liability.
- Bank shall advise customers to mandatorily register mobile numbers for SMS alerts, and encourage registration for e-mail alerts. In cases where mobile number is not provided, Bank shall limit electronic transaction facilities in line with RBI's cybersecurity and fraud risk mitigation guidelines, while ensuring financial inclusion obligations are not compromised.
- On receipt of report of an unauthorized transaction from the customer, bank will take immediate steps to prevent further unauthorized transactions in the account.
- Bank shall conduct Customer relation programmes and Branch level Customer service meetings to interact with different cross sections of customers for identifying action points to upgrade the customer service. Branch Level Customer Service Committee, comprising of Branch staff and customers (including one Senior Citizen) as members shall be conducted once in every month to study complaints/suggestions/difficulties faced by customers and evolve ways and means for improving the customer service.
- Bank may display the existing mandatory instructions in the Comprehensive Notice Board and the notice board may be updated on a periodical basis.
- The Bank shall regularly conduct awareness on safe electronic transactions to its staff, customers, merchants and vendors on a regular basis through:
    - e-mails,
    - ATMs,
    - Net banking,
    - Mobile banking

  This policy shall be read in conjunction with the Grievance Redressal Policy and Compensation Policy of the Bank which are available in website of the Bank.

5. Reporting of Unauthorized electronic transactions by customers to banks

- For any complaint related to ATM/Debit/Credit card transactions at an ATM, customer shall take it up with the card issuing bank.

- Customer shall report unauthorized electronic banking transaction to the Bank within three working days; with at the least the following details viz. Customer account number, date of transaction, amount of transaction, Transaction Reference Number (RR/UTR No.) and Beneficiary details.
- Customer shall report shall through multiple channels like website, phone banking, SMS, e-mail, IVR, a dedicated toll-free helpline, reporting to home branch, etc.
- Customer shall block the online services in the account by the missed call facility, website, phone banking, SMS, e-mail, IVR, a dedicated toll-free helpline offered by the bank. Customer shall also block/hot list the debit/credit cards through Net banking/Mobile banking platforms.
- The National Cybercrime Reporting Portal (https://cybercrime.gov.in) allows direct reporting of online crimes, including financial frauds. Customer can register all types of online crimes through this portal. The helpline number 1930 is available 24 hours a day.
- Lodge police complaint and maintain a copy of the same and furnish police complaint when sought by Banks authorised staff.
- Customer shall notify the Bank within three working days, in case of loss or theft of payment instrument or device such as debit card, credit card, mobile phone, etc. Failure to report such incidence would be treated as negligence on part of customer.

6. Electronic Transaction - Limited Liability of a Customer

6.1 Zero Liability of a Customer

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

- Contributory fraud/ negligence/ deficiency on the part of the bank (irrespective of whether or not the transaction is reported by the customer).
- 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 unauthorised transaction.

6.2 Limited Liability of a Customer

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

- In cases where the loss is due to negligence by a customer, such as where he has shared the payment credentials, the customer will bear the entire loss until he reports the unauthorised transaction to the bank. Any loss occurring after the reporting of the unauthorised transaction shall be borne by the Bank.

- In cases where the responsibility for the unauthorised electronic banking transaction lies neither with the bank nor with the customer, but lies elsewhere in the system and when there is a delay (of four to seven working days after receiving the communication from the bank) on the part of the customer in notifying the bank of such a transaction, the per transaction liability of the

customer shall be limited to the transaction value or the amount mentioned in Table 1, whichever is lower.

Table 1	
Maximum Liability of a Customer	
Type of Account	**Maximum liability (₹)**
• BSBD Accounts	5,000
• All other SB accounts	10,000
• 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 Rs.5 lakh	
• All other Current/ Cash Credit/ Overdraft Accounts	25,000
• Credit cards with limit above Rs.5 lakh	

If the delay in reporting is beyond seven working days, customer liability shall be determined transparently in line with RBI guidance and communicated in writing to the customer, with reasons. The Bank shall not exercise unfettered discretion and shall ensure decisions are fair, non-discriminatory, and subject to Internal Ombudsman review.

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 in the Table 2 as follows:

Table 2	
Summary of Customer's Liability	
Time taken to report the fraudulent transaction from 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 Table 1, whichever is lower
Beyond 7 working days	Will be decided as per the discretion of the Bank

The number of working days mentioned in Table 2 shall be counted as per the working schedule of the home branch of the customer excluding the date of receiving the communication.

7. Reversal Timeline for Zero Liability/ Limited Liability of customer

On being notified by the customer, the Bank shall credit (shadow reversal) the amount involved in the unauthorized transaction within 10 working days of notification, without waiting for settlement of insurance claim. The credit shall be value-dated to the date of unauthorized transaction. Any decision to waive customer liability shall be guided by RBI's *2017 Liability Circular* and reviewed by the Internal Ombudsman before rejection/waiver. Complaints shall be resolved within 90 days, failing which compensation shall be paid as per RBI rules. The credit shall be value dated to be as of the date of the unauthorized transaction.

Further, bank shall ensure that:

- a complaint is resolved and liability of the customer, if any, established within such time, as may be specified by the bank, but not exceeding 90 days from the date of receipt of the complaint, and the customer is compensated as per provisions above;
- where it is unable to resolve the complaint or determine the customer liability, if any, within 90 days, the compensation as mentioned in the policy is paid to the customer; and
- In case of debit card/ bank account, the customer does not suffer loss of interest, and in case of credit card, the customer does not bear any additional burden of interest.

8. Statement of account/ Pass Book

In line with RBI Circular DBR.No.Leg.BC.76/09.07.005/2016-17 dated June 22, 2017, the Bank shall provide adequate transaction details in passbooks/statements, including name of payee/remitter, mode, bank details, etc. The Bank shall also display upfront information on Deposit Insurance and Credit Guarantee Corporation (DICGC) cover, currently ₹5 lakh per depositor per bank (subject to change by RBI/DICGC), in passbooks and statements.

In the interest of better customer service, it has been decided that bank will at a minimum provide the relevant details in respect of entries in the accounts as indicated in the Table 3 below.

Table 3

Illustrative Narrations to be recorded in the Statement of Account / Passbook

I.	**Debit entries**	
1	Payment to third parties	(i) Name of the payee
		(ii) Mode - Transfer, Clearing, Inter - branch, RTGS / NEFT, Cash, Cheque (Number)
		(iii) Name of the transferee bank, if the payment is made through clearing / inter-branch transaction / RTGS / NEFT
2	Payment to 'self'	(i) Indicate "Self" as payee
		(ii) Name of the ATM / branch if the payment is made by ATM / another branch

Table 3		
Illustrative Narrations to be recorded in the Statement of Account / Passbook		
3	Issuance of drafts / pay orders / any other payment instrument	(i) Name of the payee (in brief / acronym)
		(ii) Name of the drawee bank / branch / service branch
4	Bank charges	(i) Nature of charges - fee / commission / fine / penalty etc.
		(ii) Reasons for the charges, in brief - e.g. return of cheque (number), commission / fee on draft issued / remittance (draft number), cheque collection charge (number), issuance of cheque book, SMS alerts, ATM fees, additional cash withdrawals, etc.
5	Reversal of wrong credits	(i) Date of the original credit entry reversed
		(ii) Reasons for reversal, in brief
6	Recovery of installments of a loan / interest on loan	(i) Loan account number
		(ii) Name of Loan account holder
7	Creation of fixed deposit / recurring deposit	(i) Fixed deposit / Recurring Deposit Account / Receipt Number
		(ii) Name of the Fixed Deposit / Recurring Deposit Account holder
8	Transactions at POS	(i) Transaction date, time and identification number
		(ii) Location of the POS
9	Any Other	(i) Provide adequate details on the same lines as mentioned above

Note: In case of single debit in account with multiple credits, the payee name / account number / branch / bank shall not be recorded. However, the fact of "multiple payees" will be indicated.

II.	**Credit Entries**	
1	Cash Deposit	(i) Indicate that it is a "cash deposit"
		(ii) Name of the depositor - self / third party
2	Receipt from third parties	(i) Name of the remitter / transferor
		(ii) Mode - Transfer, inter - branch, RTGS, NEFT, cash etc
		(iii) Name of the transferor bank, if the payment is received through inter- bank transaction, RTGS / NEFT
3	Proceeds of clearing / collection / draft etc. paid	(i) Name of draft issuing bank
		(ii) Date and number of the cheque / draft
4	Reversal of wrong debits (including charges)	(i) Date of the original debit entry reversed
		(ii) Reasons for reversal, in brief
5	Interest on deposits	(i) Mention if it is interest paid on the Savings Account / Fixed Deposit

II.	Credit Entries	
		(ii) Mention the respective Fixed Deposit Account / Receipt Number if it is interest paid on Fixed Deposit (s)
6	Maturity proceeds of Fixed Deposit / Recurring Deposit	(i) Name of the Fixed Deposit / Recurring Deposit holder
		(ii) Fixed Deposit / Recurring Deposit account / receipt number
		(iii) Date of maturity
7	Loan proceeds	(i)Loan account number
8	Any other	(i) Provide adequate details

9. Policy Validity

The policy would be valid for a period of 1 year from the date of approval of the Board before which the same should be reviewed. Any modification / review of the policy, irrespective of the reasons / nature of such modification / review, should be done only with the approval of the Board. No authority is authorised to grant extension of the validity period of the policy.