Customer Relations Policy

Introduction

Customer Service is a key focus area of the Bank. Customer Service for the Bank is a holistic approach targeting consistent improvement in customer experience and quality of operations. The Bank is committed to increased use of technology to provide instant services and convenience to its customers.

In the backdrop of increased thrust on financial inclusion, customer protection, there is a need for clearly defining the rights and obligations of customers in case of unauthorized electronic banking transactions in specified scenarios to address the customer risks arising out of unauthorised debits to customer accounts. Accordingly, the Banks are required to formulate the Customer Relations Policy which covers the aspects of customer protection, mechanism for creating customer awareness on the risks and responsibilities involved in electronic banking transactions, timelines for effecting compensation and the customer liability in such scenarios. The Bank has a separate Customer Compensation Policy of the Bank that reflects the Bank's on-going efforts to provide transparency and fairness in the treatment of customers.

The Bank's Customer Relations Policy is outlined below:

1. Electronic Banking Transactions

The electronic banking transactions can be divided into two categories:

(i) 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

(ii) 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.)

2. Systems and procedures

To make customers feel safe about carrying out electronic banking transactions, the Bank shall endeavour to put in place:

(i) appropriate systems and procedures to ensure safety and security of electronic banking transactions carried out by customers;
(ii) robust and dynamic fraud detection and prevention mechanism;
(iii) mechanism to assess the risks resulting from unauthorised electronic banking transactions and measure the liabilities arising out of such events;
(iv) appropriate measures to mitigate the risks and protect itself against the liabilities arising therefrom; and
(v) a system of continually and repeatedly advising customers on how to protect themselves from electronic banking and payments related fraud.

3. Roles and Responsibility of the Bank

- The Bank shall advise its customers to mandatorily register for SMS alerts and as well as e-mail alerts, for electronic banking transactions. The SMS alerts shall mandatorily be sent to the customers, wherever mobile number is registered. The Bank shall also send e-mail alerts to the customers, wherever e-mail id is registered.

- The customers shall be advised to notify the Bank of any unauthorised electronic banking transaction at the earliest after the occurrence of such transaction. The longer the time taken by the customers 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 [like: website, customer care, SMS, IVR and reporting to any branch (during branch working hours)] for reporting unauthorised electronic transactions.

- The Bank shall also enable a direct link on the Bank's website for lodging the complaints, with specific option to report unauthorised electronic transactions. The Bank shall also ensure immediate response (including auto response) is sent to the

customers acknowledging the complaint. The communication systems used by the Bank shall record the time and date of delivery of the message and receipt of customer's response, if any, to them.

- 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.

- On receipt of report of an unauthorised electronic banking transaction from the customer, the Bank shall take immediate steps to prevent further unauthorised electronic banking transactions in the account.

- The Bank shall regularly conduct awareness on safe electronic transactions to its staff, customers, merchants and vendors on regular basis through:
    - e-mails,
    - ATMs,
    - customer care,
    - net banking,
    - mobile banking

- This will be made available on the Banks' website. Such information will include rights and obligation of the customers as well as non-disclosure of sensitive information. Awareness communication will include aspect such as situations in which customer is entitled for compensation, how, when and to whom unauthorised electronic banking transaction is to be reported, the need for immediate reporting in view of risk of increasing loss, definition of unauthorised electronic banking transaction, the need for disclosure of sensitive information example password, PIN, OTP, date of birth, details of transactions, etc.

- The Bank may use services of qualified external vendors to investigate unauthorised electronic banking transaction reported by the customer.

- The Bank will conduct detailed investigation and ensure that it can clearly identify cause of the incident and the entity responsible.

- Based on the outcome of investigation, the Bank shall communicate its decision to the customer. In case the complaint is being closed in Bank's favour, and the customer requests for supporting proofs, the same shall be made available by the Bank. Bank also has onus to prove that all logs/proofs/reports for confirming two factor authentication is available, wherever applicable. Any unauthorized electronic banking

transaction which has been processed post second factor authentication known only to the customer would be considered as sufficient proof of customer's involvement/consent in effecting the transaction.

- In case during investigation or based on external feedback received, if it is found that the customer has falsely claimed or disputed a valid transactions, the Bank shall reserves its right to take due preventive action in the same.

This policy shall be read in conjunction with the Customer Grievance Redressal Policy and Customer Compensation Policy of the Bank. To know more about Customer Grievance Redressal Policy and Customer Compensation Policy please refer: https://www.icicibank.com/customer-service-policies.page.

4. Rights and obligations of the Customer

a) Rights

In case of unauthorised electronic banking transactions with one or more of Card not present/Card present/Payment mode, customer is entitled to receive:

- SMS alerts where mobile number is registered in the Bank for all financial electronic debit transactions.
- e-mail alerts where valid e-mail ID is registered for alerts with the Bank for all financial electronic debit transactions.
- Intimation at registered e-mail/mobile number with complaint number and date & time of complaint.
- Compensation in line with this policy document wherever applicable including getting shadow credit within 10 working days from the reporting date and final credit or reversal of shadow credit within 90 days of the reporting date, subject to customer fulfilling their obligations and the Bank's investigation of the case.

b) Obligations

Customer is bound by following obligations whenever they use or are likely to use the physical card, card information or mobile/net banking or any other electronic mode to conduct financial transactions. The obligations of the customer include but not limited to:

- Record their complaint through any of multiple modes available like- SMS, customer care, e-mail ID, branch and website
- Mandatorily register for SMS alerts (electronic transactions)

- Update their registered contact details as soon as such details are changed. Bank will only reach out to customer at the last known e-mail id/mobile number. Any failure of the customer to update the Bank with changes shall be considered as customer negligence
- Provide all necessary documentation - customer dispute form, proof of transaction success/failure and should also file a police complaint and provide copy of the same to the Bank
- Co-operate with the Bank's investigating authorities and comply with the Bank's reasonable requirements towards obtaining details of transactions, investigation purposes etc.
- Share relevant documents as needed for investigation viz. customer dispute form, copy of passport in case of international transactions and police complaint
- Authorise the Bank to block their account(s) to reduce likelihood of additional loss
- Not to share sensitive information [such as Card number, 3D secure PIN, ATM PIN, Unique Registration Number (URN), Debit/Credit Card PIN, Card Verification Value (CVV), iMobile login PIN, Net Banking user id and password, One Time Password (OTP), etc.] to any entity including bank staff
- Protect their device as per best practices specified in the Bank's website (device includes smart phone, feature phone, laptop, desktop and TAB)
- Abide by the process mentioned on the following link https://www.icicibank.com/online-safe-banking/index.page
- Set limits on their transaction to ensure that the exposure is minimised
- Verify their transactions from time to time in the bank and or credit card statement and raise query with the Bank as soon as possible in case of any error
- Go through various instructions and awareness communication sent by the Bank or check on the Bank's website at https://www.icicibank.com/ on a regular basis
- Change ATM PIN frequently, at least once a month
- Memorise their PIN and not to share the PIN or card with anyone, not even their friends or family
- Not to take help from strangers for using the ATM card or handling their cash
- Press the 'Cancel' key before moving away from the ATM and should remember to take the card and transaction slip
- Report lost/stolen ATM card to card-issuing bank immediately
- Not to save confidential information such as debit/credit card numbers, CVV numbers or PIN's on the mobile phone.

Customer will be responsible for safeguarding confidential information related to their account and will be liable for losses arising due to compromising of such information and not fulfilling their obligations.

5. Reporting of the unauthorised transaction by the Customer to the Bank:

- For any complaint related to ATM/Debit/Credit card transaction at an ATM, customer shall take it up with the card-issuing bank
- Customer shall report unauthorised electronic banking transaction to the Bank at the earliest, with at least the following details viz. Customer account number, date of transaction, amount of transaction
- Customer shall follow Bank's reporting process viz.:
- Report through SMS or to specified Bank's designated mobile number or on link https://www.icicibank.com/. In case, they are unable to do so, they could report through customer care or at the nearest branch
- Lodge police complaint and maintain copy of the same and furnish police complaint when sought by Bank's authorised staff
- Customer shall forthwith notify the Bank in case of loss or theft of payment instrument or device such as debit card, credit card, mobile, etc. Failure to report such incidence would be treated as negligence on part of customer.

6. Liability of a Customer

(a) Zero Liability of a Customer

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

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

(ii) 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 electronic banking transaction.

(b) Limited Liability of a Customer

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

(i) In cases where the loss is due to negligence by a customer, such as where they have shared the payment credentials, the customer will bear the entire loss until they reports

the unauthorised electronic banking transaction to the Bank. Any loss occurring after the reporting of the unauthorised electronic banking transaction shall be borne by the Bank.

(ii) 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	Between 4 & 7 working days (₹)	More than 7 working days (₹)
BSBD Accounts	5,000	100% Customer Liability
All other SB accounts	10,000	
Pre-paid Payment Instruments and Gift Cards	10,000	
Current/Cash Credit/Overdraft Accounts of MSMEs	10,000	
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	10,000	
Credit cards with limit up to Rs.5 lakh	10,000	
All other Current/Cash Credit/Overdraft Accounts	25,000	
Credit cards with limit above Rs.5 lakh	25,000	

7. Overall liability of the customer

The overall liability in third party breaches, as detailed above, where the deficiency lies neither with the Bank nor with the customer but lies elsewhere in the system, is summarised below:

Table 2: Overall liability of the customer

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	As per the policy

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

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

On being notified by the customer, the Bank shall credit (shadow reversal) the amount involved in the unauthorised electronic transaction to the customer's account within 10 working days from the date of such notification by the customer (without waiting for settlement of insurance claim, if any). The Bank may also at its discretion decide to waive off any customer liability in case of unauthorised electronic banking transactions even in cases of customer negligence. The credit shall be value dated to be as of the date of the unauthorised electronic banking transaction.

The Bank shall also ensure the following:

(i) a complaint is resolved and liability of the customer, if any, established within such time, as may be specified in the Bank's Board approved policy, but not exceeding 90 days from the date of receipt of the complaint, and the customer is compensated as per provisions of paragraphs 6 a. to 8 above;
(ii) where it is unable to resolve the complaint, or determine the customer liability, if any, within 90 days, the compensation as prescribed in paragraphs 6 a. to 8 is paid to the customer; and
(iii) in case of debit card/ bank account, the customer does not suffer loss of interest, and in case of credit card, the customer does not bear any additional burden of interest.

9. Monitoring and Review

The Standing Committee on Customer Service shall review the unauthorised electronic banking transactions reported by customers or otherwise at half-yearly interval (data at September 30 and March 31) along with the action taken thereon, the functioning of the grievance redressal mechanism and take appropriate measures to improve the systems and procedures. The Bank shall also report to the Customer Service Committee of the Board all such transactions on a half yearly basis (data at September 30 and March 31). The reporting shall include volume/number of cases and the aggregate value involved and distribution across various categories of cases. These transactions shall be reviewed by the Internal Audit Group as per Risk Based Audit Plan of respective year.

10. Definitions and Explanations

- Card not present means transactions that require use of Card information without card being physically used e.g. e-commerce transactions.
- Card present means transactions that require use of physical card e.g. at ATM or shops.
- Payment transaction means transactions that involve transfer of funds from one account/wallet to another electronically and do not require card information e g. NEFT.
- Unauthorised electronic banking transaction means debit to customer's account without their consent.
- Consent means acceptance of a transaction debit either through standing instructions, as per accepted banking practice and regulation, based on account opening process and related matters or based on additional authentication required by the bank such as response to OTP, challenge questions or use of Card details (CVV/ Expiry date).
- Date and time of reporting means date and time on which customer has submitted a unique complaint and which has been responded to by the Bank. Date of receiving communication from the Bank is excluded for purpose of computing number of working days for all action specified in this policy. The working schedule of the home branch would be considered for calculating working days for customer reporting. Time of reporting will be as per Indian Standard Time.
- Number of days will be computed based on working days.
- Mode of reporting will be based on customer complaint through short message service (sms), e-mail ID, Mobile Banking or website whichever is first received by the Bank independent of multiple reporting of unauthorised electronic banking transaction.
- Loss in foreign currency if any shall be converted to Indian currency for the purpose of this policy as per the Bank’s policies on conversion at card rate, net of commission.

- The Bank shall take confirmation on which all accounts to be blocked on account of fraudulent transaction reported by the customer.

Last Reviewed date: 18th September, 2018