केनरा बैंक Canara Bank

Policy
for
Customer Protection for Limiting Liability of Customers in Unauthorized Electronic Banking Transactions for the year 2020-2021

Strategic Planning & Development Wing

Head Office, 112, JC Road, Bengaluru

Policy for Customer Protection for Limiting Liability of Customers in Unauthorized Electronic Banking Transactions for the year 2020-2021

1. OBJECTIVE:

Financial Inclusion, Customer Protection and Fair Practices in Banking operations are the important pillars of Customer Service in Banks. To strengthen these thrust areas and to clearly determine the customer liability in respect of unauthorised Electronic Banking Transactions (EBT), Reserve Bank of India has issued revised directions vide their Circular No. DBR.No.Leg.BC.78/09.07.005/2017-18 dated 6th July, 2017. To give effect to these guidelines, a separate "Policy for Customer Protection for Limiting Liability of Customers in Unauthorized Electronic Banking Transactions (EBT)" as mandated by RBI is framed by our Bank.

2. BACKGROUND:

Due to increased thrust on digitization from the Government as well as from the Bank and increased use of digital platforms by customers, complaints/grievances relating to digital transactions are on the increase. It is also observed that due to increased incidence of cyber-crimes relating to Electronic Banking Transactions, customer complaints are on the increase. Further, increased awareness amongst customers about their rights have also resulted in increase in grievances relating to EBT.

In this context, considering the recent surge in customer grievances relating to unauthorized EBT resulting in erroneous debits to customer accounts/cards, to safeguard and protect the interest of the consumers, Reserve Bank of India (RBI) has issued the revised guidelines for determining the Customer Liability in case of un-authorized EBT.

3. ROLES AND RESPONSIBILITIES:

3.1. Systems & Procedures

3.1.1. Broadly, the Electronic Banking Transactions (EBT) are divided into two categories;

a) Remote / Online payment transactions / Card Not Present (CNP) Transactions where physical payment instruments are not required for making transactions for example; Mobile Banking, Internet Banking, Pre-paid payment instruments (PPI) etc.

b) 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.)

3.1.2. Safety and security measures for customers to carry out Electronic Banking Transactions (EBT);

The Bank has designed, and shall continually strive to strengthen, systems and procedures to make customers feel safe about carrying out electronic banking transactions.

To achieve this, the bank shall put in place:

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

a) the bank shall ask its customers to mandatorily register for SMS alerts and wherever available register for e-mail alerts, for electronic banking transactions.
b) The SMS alerts shall mandatorily be sent to the customers, while email alerts may be sent, where the customer requests for the same and e-mail id is registered.

ii. robust and dynamic fraud detection and prevention mechanism;

a) The Bank shall provide One Time Password (OTP) to the customers through their registered mobile number at the time of making the payment of any transaction through payment gateway for confirmation/ authentication of the account holder.
b) Security measures like virtual keyboard in Internet Banking, Mandatory PIN verification for Debit Cards at POS machines as an additional security feature and introduction of EMV Chip based Cards, are also been implemented.
c) All alternative channels are integrated with EFRM (Enterprise wide Fraud Risk Management) tool for real-time fraud detection & prevention.

iii. **mechanism to assess the risks resulting from unauthorized transactions and measure the liabilities arising out of such events;**

a) Bank is having the system to absorb the liabilities and to mitigate the risks arising out of unauthorized transactions.

iv. appropriate measures to mitigate the risks and protect themselves against the liabilities arising there-from;

a) Bank shall send alerts through mobile for all types of Card related and online banking transactions.
b) Risks and liabilities that may arise due to un-authorized EBT / fraudulent transactions would be met by appropriate Insurance cover taken by the Bank.

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

a) The Bank, from time to time, shall educate the customers to protect themselves from Electronic Banking and Payments related frauds through various channels.
b) Customers shall be periodically advised to have efficient security precautions and practices in protecting their personal computer, Smart-

phones and to avoid conducting financial transactions from public or internet café computers. For this purpose, Do's & Don'ts have been notified in Bank's Website.

3.1.3. Reporting of Unauthorized Electronic Banking Transactions by customers to the Bank

i. Customers desirous of undertaking electronic banking transactions shall be asked to mandatorily register for SMS alerts and, wherever available, register for e-mail alerts.

ii. Customers shall be advised to notify the bank of any unauthorized electronic banking transaction at the earliest after the occurrence of such transaction, and shall be educated that the longer the time taken to notify the bank, the higher will be the risk of loss to the Bank/Customer.

- Customers are required to report to Bank immediately on knowing the occurrence of the unauthorized EBT.

iii. To facilitate immediate reporting by the customers, the bank shall provide its 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.

a) Call Centre with single point contact Toll free number 18004250018 is functional in the Bank 24x7 to cater to customers in 6 regional languages i.e. Bengali, Kannada, Malayalam, Marathi, Tamil and Telugu, besides Hindi and English for reporting the unauthorized EBT / and / or loss or theft of payment instrument such as card etc,.
b) Customers can also reach the Bank through multiple channels like website (webchat/registering online complaints), SMS, Internet Banking, Mobile Banking, reporting to home branch etc.,
c) The Bank shall also enable customers to instantly respond by "Reply" to the SMS and e-mail alerts and the customers should not be required to search for a web page or an e-mail address to notify the objection, if any.
d) A separate direct link is available with specific options for lodging the grievances regarding unauthorized Electronic Banking Transactions(EBT) in the Home Page of Bank's website www.canarabank.com
e) On receiving the SMS / e-mail alerts, Customers are required to instantly respond in case of any suspicion/objection. Procedure for notifying unauthorised EBT has been described in Grievance Redressal Mechanism in point no. **4.1.1.(a) of page no.11 & 12**.]
f) The Bank shall not offer facility of Electronic Banking transactions, other than ATM Cash withdrawals, to customers who do not provide mobile numbers to the Bank. In such cases, on receiving information about unauthorized transactions from the customer, Bank will take immediate steps to prevent further unauthorized EBT in the account by way of blocking the Card.

iv. The Bank shall provide the following mechanism to ensure that response from the customers reach the Bank:

a) Upon receiving the complaint, customers will get system generated acknowledgement along with registered complaint number in Canara Public Grievance Redressal System (CPGRS) package.
b) Bank shall immediately block (may be temporarily), the internet and mobile banking facilities / all accounts of the customer linked to the mobile number, whenever any information received regarding un-authorized Electronic Banking Transactions.
c) For determining the extent of a customer's liability regarding unauthorised EBT, the details of sending alerts through SMS / e-mail and any response received thereto, are recorded with date and time for all complaints in CPGRS Package.

3.2. Limited Liability of a Customer in case of unauthorized EBT

3.2.1. Zero Liability of a Customer

A customer's entitlement to zero liability shall arise where the un-authorized EBT occurs in the following cases:

i) Contributory fraud / negligence / deficiency on the part of the Bank. If the un-authorized transaction was made due to contributory fraud / negligence / deficiency on the part of the Bank, customer has zero liability to bear, irrespective of whether or not the transaction is notified / 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 3 working days of receiving communication from the bank regarding the un-authorized EBT.

3.2.2. Limited Liability of a Customer

A customer shall be liable for the loss occurring due to un-authorized transactions in the following cases;

i) In cases where the loss is due to negligence by customer, such as, where he/she has shared the payment credentials, the customer shall bear the entire loss until he/she reports the un-authorized EBT to the bank. Any loss occurring after the report of the un-authorized EBT shall be borne by the bank.
ii) In cases where the responsibility for the un-authorized 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 4 to 7 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 under above paragraph (ii)

Type of Account	Maximum Liability (Rs.)
➢ BSBD Accounts	5000.00
➢ 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.25.00 lakh ➢ Credit Cards with limit up to Rs. 5.00 lakh	10000.00
➢ All other current/Cash Credit/Overdraft Accounts ➢ Credit cards with limit above Rs.5.00 lakh	25000.00

iii) Further, if the delay in reporting is beyond 7 working days, the customer liability shall be determined as follows;

"In case where neither the Bank is at fault nor the customer, but the fault lies elsewhere in the system and there is a delay in reporting beyond 7 working days and within 60 days of receiving communication from the bank, the Bank will compensate the customer with Rs.100/- per Rs.5000/- of the amount involved, subject to a maximum Rs.1000/- for each instance". The compensation shall be paid within Ten (10) working days of establishing the customer's liability.

However, if the delay in notifying is beyond 60 days after receiving the communication from the Bank, the Bank is not liable to compensate the customer.

In cases where the customer does not provide the relevant documentation as requested by the Bank within 15 calendar days of Bank seeking the documents, the Bank is not liable to compensate the customer.

3.2.3. <u>Third Party Breaches</u>

Overall liability of the customer in third party breaches as detailed in **3.2.1(ii)** & **3.2.2(ii)** above, where the deficiency lies neither with the Bank nor with the customer but lies elsewhere in the system is summarized in the Table-2

Table – 2

Summary of customer's liability

Time taken to report the fraudulent transaction from the date of receiving the communication	Customer's Liability (Rs)
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 and within 60 days	As per point no.3. 2.2.(iii)

Note: 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.

3.2.4. Reversal Time for Zero Liability / Limited Liability of customer

i) On being notified by the customer, the bank shall credit **(shadow reversal**) the amount involved in the un-authorized EBT 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 credit shall be value dated to be as of the date of un-authorized EBT.

ii) Bank is having the discretion on the merits of the case to decide to waive off any customer liability (whether part or full) in case of un-authorized electronic banking transaction even in cases of customer negligence.

The Competent Authority for waiving of customer's liability (part or full) in case of un-authorized electronic banking transactions where customer is negligent shall be MD & CEO of the Bank or in absence of MD&CEO, Executive Director of the Bank**.**

3.2.5. Further, Bank shall ensure that;

i) A complaint is resolved and liability of the customer if any is established within 90 days from the date of receipt of the complaint and the customer is compensated as per provisions mentioned above.

ii) Where it is unable to resolve the complaint or determine the customer liability if any within 90 days, a compensation as prescribed in point no. 3.2.1 to 4 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.

4. COMPLIANCE / MONITORING OF IMPLEMENTATION OF THE POLICIES:

4.1. Details of Grievance handling / escalation mechanism for Unauthorised Electronic Banking Transaction (EBT):

4.1.1. The following are the Channels through which customers can report unauthorised EBT;

a) **SMS:** SMS messages will be sent to registered mobile number for all debit transactions appending a message which reads as "If this transaction is not initiated by you please report by SMS "SUSPECT" to 56161 to block accounts linked to this mobile number". In case of any unauthorised Electronic Banking Transactions, to stop further debits in the account;
   - Domestic Customers can respond by sending SMS as SUSPECT to 56161

b) **Website:** Customers can lodge complaint in our Canara Public Grievance Redressal System (CPGRS) Package regarding unauthorised EBT through our website www.canarabank.com. (under Customer Services -- Register for Grievances)

c) Customers can report the unauthorized EBT transactions through Internet Banking & Mobile Banking channel.

d) Customer can report the unauthorized EBT through the home branches.

e) **Dedicated Toll Free Help Line:** Customers can report unauthorised EBT by dialing dedicated Toll Free Help Line (1800 425 0018)

4.1.2. Further

a) The Bank will settle the liability of unauthorized EBT in each case as per the procedure mentioned in Table-1 & 2 respectively.

b) The customer/complainant has to approach the Home/Base Branch for submission of documents regarding the reported unauthorised EBT for settlement of claims.

c) Customers can approach the Bank's internal grievance redressal machinery and approach alternate fora only after exhausting all the remedies available under Bank's internal grievance redressal mechanism, that is, the Branch Head, Regional Office, Circle Office and then finally Head Office.

d) The customer who has reported "SUSPECT" transactions has to furnish the following documents to the Base Branch where the account is maintained, within 15 days from the date of report of the transaction;

   i) Copy of Card and hot-listing date (screen shot of hot-listed card in CMS01 as provided by the Branch), if copy of the lost card is not available
   ii) Latest Account statement (for the month of suspect transactions reported)

iii) Passport copy (all pages), if loss is at international location (If customer does not hold passport, an undertaking letter from the cardholder by mentioning "CUSTOMER DO NOT HOLD PASSPORT")
iv) Copy of FIR or Acknowledgement of Police Complaint (If FIR / Police Complaint copy is in vernacular language, provide English / Hindi version of the same).
v) Copy of Dispute letter given by Customer to bank (If complaint copy is in vernacular language, provide English / Hindi version of the same).

It may be noted that there is an office of Internal Ombudsman at the Bank's Apex level of internal grievance redressal system (a retired Senior Executive of the rank of General Manager from another Bank) to whom the Bank is required to internally escalate all complaints for final decision/re-examination where the complaint is either proposed to be rejected or only partial relief is proposed.

4.1.3. Further, the Bank will –

a. On receiving the information from the customer regarding unauthorized Electronic Banking Transaction, block all the accounts linked to the mobile number to prevent further attempt of fraudulent transactions. Account can be unblocked on submission of request to the respective branch where the account/s is/are maintained.

b. Acknowledge all formal complaints (including complaints lodged through electronic means) within three working days of receipt and work to resolve it within a reasonable period, not exceeding 90 days (including the time for escalation and examination of the complaint by the highest ranking internal official responsible for grievance redressal). The 90 days period will be reckoned after all the necessary information sought from the customer is received;

c. Provide aggrieved customers the details of the Banking Ombudsman Scheme for resolution of a complaint if the customer is not satisfied with the resolution of a dispute, or with the outcome of a dispute handling process;

4.1.4. In addition, the Bank will –

a. After examining the matter, send final response or explain why it needs more time to respond and shall endeavor to do so at the earliest, but not later than 90 days from receipt of complaint.

b. Ensure the customer is refunded without delay and demur, if it cannot show proof beyond reasonable doubt to the customer on any disputed transaction (along with interest/charges).

4.2. Burden of Proof:

It is clarified that the burden of proving customer's liability in case of un-authorized Electronic Banking Transaction shall lie with the bank except in the following;

- Where the customer is negligent and has shared the payment credentials to unknown persons consequent to which occurrence of un-authorized Electronic Banking Transactions are noticed.

- On receipt of the required documents from the customers who has reported the unauthorised Electronic Banking transactions, Card Dispute Management section of Digital Banking Services Wing, Head Office will verify the genuineness of the credentials of the customers.

4.3. Reporting and Monitoring Requirements:

a. Customer Service Section, SP&D Wing at Head Office shall place an Office Note to the Customer Service Committee of the Board on quarterly basis where the details like number of un-authorized Electronic Banking Transactions, amount involved and distribution across various categories of cases viz., Card Present Transactions, Card Not Present transactions, Internet Banking, Mobile Banking, ATM transactions etc. and compensation paid will be covered. All such transactions shall also be reviewed by the Bank's Internal Auditors at the time of Internal Audit. Digital Banking Services Wing, Head Office will be the functional wing to deal with all cases of unauthorized EBT.

b. The Standing Committee on Customer Service of the Bank shall undertake a quarterly review of the unauthorized Electronic Banking Transactions reported by the customers, as also the action taken thereon.

*****