Table of Contents

Customer Protection Policy Version 2.0

Table of Contents

Introduction:

With the increased thrust on financial inclusion, customer protection and considering the recent surge in customer grievances relating to unauthorized transactions resulting in debits to their accounts / cards / mobile wallets, the criteria for determining the customer liability in these circumstances have been reviewed for electronic banking transactions. Taking into account the risks arising out of unauthorized debits to customer accounts owing to customer negligence / Bank negligence / banking system frauds / third party breaches, the rights and obligations of customers in case of unauthorized transactions in specified scenarios, aspects of customer protection, including the mechanism of creating customer awareness on the risks and responsibilities involved in electronic banking transactions and customer liability in such cases of unauthorized electronic banking transactions are reviewed and a policy was prepared.

1. Objective of the Policy:

This policy document aims to make customer more confident against the risks arising out of unauthorized debits to customer accounts owing to customer negligence / Bank negligence / banking system frauds / third party breaches and to clearly define the rights and obligations of customers in case of unauthorized transactions in specified scenarios to use electronic banking transactions and defined the maximum customer liability for the electronic banking transactions to make customers feel safe about carrying out electronic banking transactions.

The Bank believes that providing the protection to the customer against unauthorized electronic transactions is a boon to customer service to make customers feel safe about carrying out electronic banking transactions and which is essential not only to attract new customers, but also to retain existing ones.

2. Scope/Coverage:

This policy covers procedural guidelines to be followed by business owners in case of perpetration of frauds in customer's account, establishment of fraud, timely restoration, and follow up for expeditious restoration of amount in the account of customer, recovery of the restored amount.

3. Intended recipients:

This policy covers procedural guidelines to be followed by business owners in case of perpetration of frauds in customer's account. As per the RBI mandate, we are also required to display the policy on our corporate website along with the details of grievance handling / escalation procedure.

4. RBI Guidelines:

While the primary responsibility for preventing frauds lies with banks themselves, Reserve Bank of India (RBI) has been advising banks from time to time about the major fraud prone areas and the safeguards necessary for prevention of frauds. RBI has also been circulating to banks, the details of frauds of an ingenious nature not reported earlier so that banks could introduce necessary safeguards by way of appropriate procedures and internal controls.

RBI through their communication DBR.NaLeg.BC.78/09.07.005/2017-18 dated 6th July 2017 in respect of Customer Protection — Limiting Liability of Customers in Unauthorized Electronic Banking transactions, has once again reiterated the need for providing protection to customers.

The gist of the said circular is as under: –

Electronic Banking Transactions:

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) like Mobile Wallet etc., and

• **Face-to-face/ proximity payment transactions** - Transactions which require the physical payment instrument such as a card or mobile phone etc. to be present at the point of transaction e.g. ATM, POS, etc.

The system and procedures in Bank must be designed to make customers feel safe about carrying out electronic banking transaction. To achieve this, Bank must 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 therefrom; and
- A system of continually and repeatedly advising customers on how to protect themselves from electronic banking and payments related fraud.

Reporting of unauthorized transactions by customers to bank:

Bank must ask their 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 must be advised to notify 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.

To facilitate this, Bank provides 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. Further, a direct link for lodging the complaints, with specific option to report unauthorized electronic transactions shall be provided by bank on home page of their 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.

Immediate action to be taken by branch and further follow-up to be taken on detection of fraud:

As soon as it comes to the knowledge of the base branch / contact center / concerned department/ or any other officials of Bank through any mode of communication, following immediate action is to be taken.

The branch has to immediately block / de-register the digital channel from where the fraud has happened with the consent of customer so that the subsequent fraud attack on the particular account can be protected and liability of future fraud after notifying by customer can also be protected.

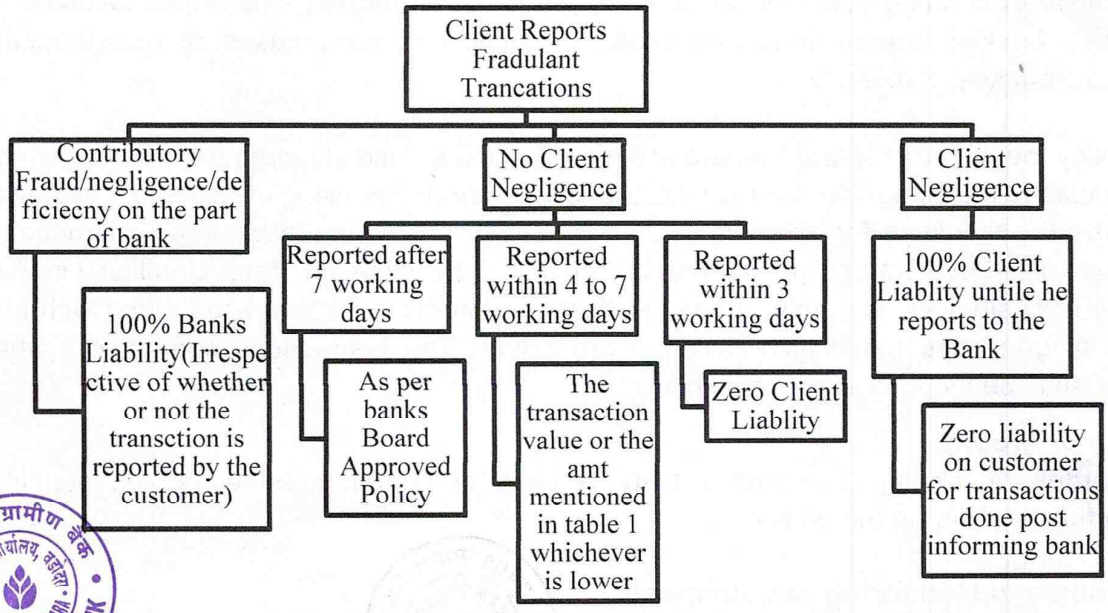
To enable customers to instantly respond to the Banks, Banks are required to provide a standard number on which dispute may immediately be logged through a short SMS such as "Yes/No".

The communication systems used by Bank to send alerts and receive their responses thereto must 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. 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 unauthorized transaction from the customer, bank must take immediate steps to prevent further unauthorised transactions in the account.

On receipt of report of an unauthorized transaction from the customer, Bank must take immediate steps to prevent further unauthorized transactions in the account

Limited Liability of a Customer:

Customer Protection — Limited Liability of customer in Unauthorized Electronic Banking Transaction as per RBI



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 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 insurance claim, if any may be credited to the same account on settlement.

Bank may also at their 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 transaction.

Further, banks shall ensure that:

- 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 shown on above chart.
- Where it is unable to resolve the complaint or determine the customer liability, if any, within 90 days, the compensation as prescribed in Table 1 and 2 will be paid to customers.
- 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.

Board Approved Policy for Customer Protection:

Taking into account the risks arising out of unauthorized debits to customer accounts owing to customer negligence/ bank negligence/ banking system frauds/ third party breaches, banks need to clearly define the rights and obligations of customers in case of unauthorised transactions in specified scenarios. Banks shall formulate/ revise their customer relations policy, with approval of their Boards, to cover aspects of customer protection, including the mechanism of creating customer awareness on the risks and responsibilities involved in electronic banking transactions and customer liability in such cases of unauthorised electronic banking transactions.

The policy must be transparent, non-discriminatory and should stipulate the mechanism of compensating the customers for the unauthorised electronic banking transactions and also prescribe the timelines for effecting such compensation keeping in view the instructions contained in above paragraph related to "Reversal Timeline for Zero Liability/ Limited Liability of customer". The policy shall be displayed on the bank's website along with the details of grievance handling/ escalation procedure. The instructions contained in this circular shall be incorporated in the policy.

Burden of Proof:

The burden of proving customer liability in case of unauthorized electronic banking transaction shall lie on the bank.

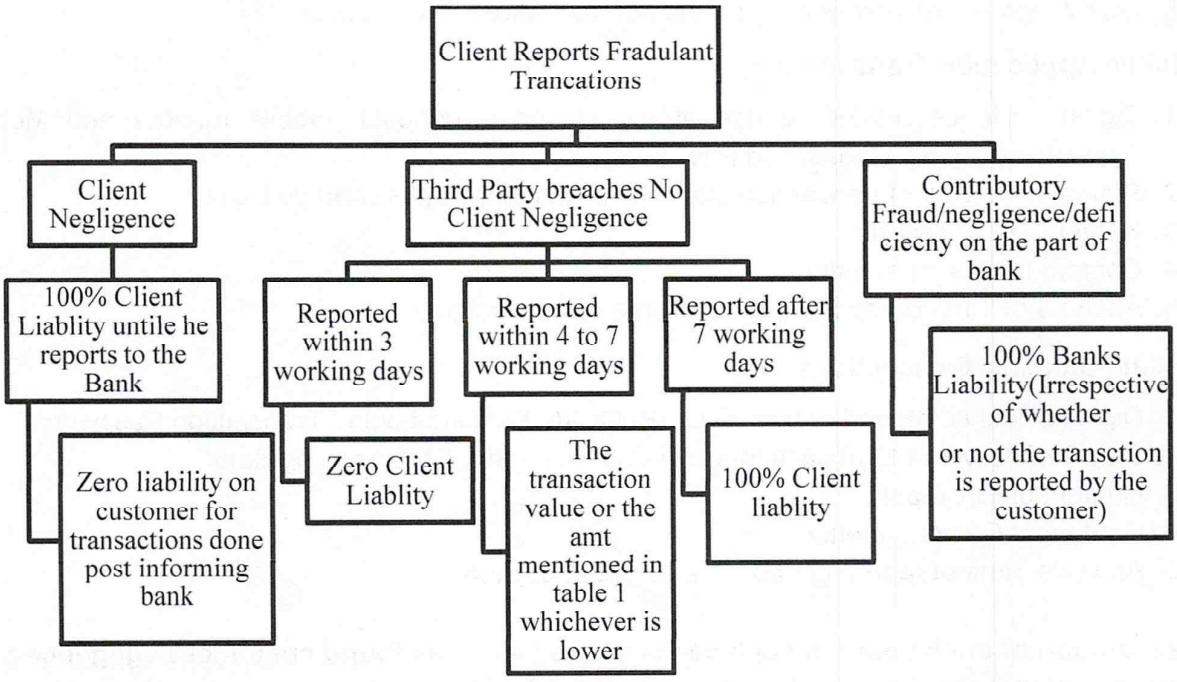
Reporting and Monitoring Requirements:

The banks shall put in place a suitable mechanism and structure for the reporting of the customer liability cases to the Board or one of its Committee. The reporting shall, inter alia include volume/ number of cases and the aggregate value involved and distribution across various categories of cases viz., card present transactions, card not present transactions, internet banking, mobile banking, ATM transactions, etc. The Standing Committee on Customer Service in each Bank shall periodically review the unauthorized electronic banking transactions reported by customers or otherwise, as also the action taken thereon, the functioning of the grievance redress mechanism and take appropriate measures to improve the systems and procedures. All such transactions shall be reviewed by the bank's internal auditors.

5. Guidelines to be followed by bank to determine the Liability of Customers in unauthorized Electronic Banking Transactions:

As advised by RBI in the said communication, Bank has formulated the policy and clearly define the rights and obligations of customer in case of unauthorized transaction in specified scenarios.

To determine the Customer Liability in unauthorized Electronic Banking Transaction, Bank will use the following mechanism –



6. Right and Obligation of customer in case of unauthorized electronic banking transaction in specified scenario:

Scenario 1:

Customer Negligence - Unauthorized Electronic Banking Transaction happened due to customer negligence (such as where he has shared the payment credentials etc.)
Customer Liability - 100% customer liability.

Customer Right - Customer to bear the entire loss until he / she reports the unauthorized transaction to the bank. Any loss occurring after the reporting of the unauthorized transaction shall be borne by the Bank.

Customer Obligation - Approach the Bank as soon as the customer becomes aware of the unauthorized debit. Customer is required to be vigilant while doing electronic banking transaction. The concerned electronic Banking channel team will check customer negligence based on the following parameters and put it to channel head for approval before communicating the same to customer.

Debit Card Transactions:

1. ATM cash withdrawal and other POS transactions: Digital evidence related to use of physical Debit Card and PIN for the Cash Withdrawal and POS transaction, status of delivery of transaction alert / OTP and other SMS send by Bank.
2. E-commerce and other OTP based transaction: If it is e-commerce transaction and other transactions where Bank is sending OTP to customer then the status of OTP delivery.
3. Analysis of EJ log.
4. Content of FIR report.
5. Content of Customer letter.
6. Analysis of Time of reporting fraud & time of transaction
7. Analysis of card blocking.
8. CCTV footage: as and when required not mandatorily for all cases.

Mobile Application Transactions:

1. Digital evidence related to use of the customer handset, mobile number and Mobile Application Login / Transaction PIN.
2. Status of delivery of transaction alert / OTP and other SMS send by Bank.
3. Content of FIR report.
4. Content of Customer letter.
5. Analysis of Time of reporting fraud & time of transaction.

Online Banking Transactions:

1. Digital evidence related to use of the IP, Online Banking Login / Transaction Password.
2. Status of delivery of transaction alert / OTP and other SMS send by Bank.
3. Content of FIR report.
4. Content of Customer letter.
5. Analysis Time of reporting fraud & time of transaction.

Restoration of the amount in such cases where Bank has found customer negligence and where customer has reported the unauthorized Electronic Banking transaction within the timeline provided by RBI:

Bank will treat such cases as 100% client liability. However, in exceptional cases based on Bank's discretion, Bank can reimburse an amount up to Rs. 10,000/- or transaction value whichever is lower.

After ascertaining the following points respective branch may send the proposal to the Head Office for the sanction duly recommended by the Branch Head and Regional Head as per **Annexure A** attached herewith within a period of 60 days from the date of unauthorized transaction.

- Business relationship with the customer.
- Past records of the customer for such type of grievances.
- Established Integrity of the customer.
- Branch be satisfied for the reason of negligence given by the customer for such unauthorized transaction.

The sanctioned amount will be debited to the P/L Account of the branch where customer is maintaining account.

To ensure timely compensation to customer in unauthorized electronic banking transaction administrative power of Rs. 10,000/- per transaction is assigned to General Manager, Head Office subject to monthly reporting of PSR to next higher authorities

7. Information required from customer to resolve the complaint in respect of Unauthorized Electronic Banking transaction:

- Channel details like channel name, location etc. (from customer)
- Transaction details like transaction type, account, date, amount etc. (from customer)

Other details required to be collected by the internal teams as mentioned below:

- SMS alert details.
- Electronic channel logs / EJ

Bank will also require following documents from customer, which are required to be sent by branch to RO/HO to process the insurance claim once Bank will give shadow credit in customer account.

- Claim Form
- Copy of FIR duly attested by Notary Public.
- An undertaking (Performa enclosed) for loss amount up to Rs.25000/- and Affidavit for and amount above Rs. 25000/-
- Letter of the customer reporting the branch about the fraud.
- Copy of a/c Passbook, which shows transactions date, time & amount (Bank Passbook 1st Page & 1 Month statement prior to fraudulent transaction to till date also required)/statement generated from Finacle.
- Photo copies of all pages of Passport, if applicable.
- Translated copy of documents in English duly attested by Notary Public, if the documents are in regional language.

Any other documents required by Insurance Co./Bank

All the complaint received from the customer in respect of Unauthorized Electronic Banking transaction to be reported to respective Branch for immediate action.

Branch will take appropriate action i.e.

For ATM transaction, complaint to be lodged in DCRS portal and intimate the same to Regional Office/Head Office.

For Unauthorized Electronic Banking transaction of other channels like Mobile Banking, IMPS, UPI etc. also be reported to respective Branch for immediate action and in turn branch will forward to Regional Office/ Head office immediately.

After receiving complaint from the customer in Unauthorized Electronic Banking transaction, Bank will take action as mentioned in Table 4.

To ensure timely compensation to customer in unauthorized electronic banking transaction, administrative power as per Table 5 is granted to respective authorities in such cases where Bank is liable to compensate the customers.

Respective authority will use the restoration power given in Table 5 to compensate the customer in such cases where Bank is liable to compensate the customer or in such cases where the Banking Ombudsman or any other regulatory agency has given advisory or passed award.

8. Facility of Electronic transaction to such customers which have not registered their mobile number in their accounts:

As per the RBI guidelines "The banks may not offer facility of electronic transactions, other than ATM cash withdrawals, to customers who do not provide mobile numbers to the bank". However looking to the customer convenience and the following security feature available in these electronic channels, Bank has decided to allow all Electronic transactions to such customers.

1. **Face to face / proximity payment transactions** - All these transactions are performed based on the two factor authentication. In all such transactions (like ATM Cash Withdrawal, POS transaction, QR code based transaction) customer is required to present physical payment instrument (Card or Mobile number) and their credential like PIN, Biometric etc.
2. **Remote/ online payment transactions** - All these transactions are performed based on the two factor authentication. Customer who have not registered their mobile number in their account are not able to use Bank's various Mobile based Application. They are also not able to perform E-commerce transaction through Debit cards as Bank is using OTP authentication as second factor authentication in these transactions.

9. Strengthening of systems and procedures

All the electronic banking channels are having its inbuilt system and procedures to ensure safety and security of electronic banking transaction carried out by customers. To update these systems in view of increased risk threats, Bank's Audit / IT security team at DC/ CISA Auditors are conducting regular audit / review of electronic channels. Bank is continuously improving the security parameter based on the audit findings.

FRM solution of NPCI for monitoring of Domestic Debit Card Transaction. FRM solution of NPCI for monitoring of IMPS/UPI Transaction.

Bank is also continuously and repeatedly advising customer on how to protect themselves from electronic banking and payments related fraud through various modes like Website, SMS, Notification, Advertisement etc.

10. Fraud Risk Management Guidelines:

Reporting of fraud to various authorities as per RBI, our Bank's extant guidelines.

11. Reporting:

Bank will submit a report on following points to Board of any unauthorized electronic banking transaction.

- Any unauthorized electronic banking transaction reported by customer and Amount paid by bank.
- Department found similar nature of fraud in various cases.
- Found any staff accountable for any unauthorized electronic banking transaction

- Found any contributory fraud / negligence / deficiency on the part of the Bank
- Lacuna/weakness in system and procedure, if any

12. Staff accountability:

Bank will ascertain the staff accountability in such cases where Bank has incurred losses due to negligence on the part of the staff.

For ascertaining comparative negligence or liability on the part of the staff a committee to be formed at Head Office as per Table 6:

The Committee will verify the investigation report submitted by the investigating officer and will submit findings to Sanctioning authority. Sanctioning Authority will decide the staff accountability on the basis of findings submitted by the committee.

13. Customer's Responsibility:

- Bank will not be under obligation and responsible for loss to the customers due to customer's carelessness in keeping cards, Use ID, login ID, PIN, OTP or other security information and not adhering "Do's and Don'ts" issued by the Bank, until and unless the Bank has been notified by the customer.
- The Bank will not be responsible for loss to the customer, if the customer acts fraudulently and for acts without reasonable care which has resulted in loss. Bank will also not be responsible for loss arising out of loss of cards, login ID, PIN, compromise of password or confidential information until and unless the Bank has been notified of such loss/compromise and Bank has taken steps to prevent its misuse.
- The Bank will not be responsible for loss to the customer, if the customer has not notified his current Mobile number, Address, email ID with his base branch. These updated information is required to Bank to send Transaction Alert/other information to customer.

14. Force Majeure:

The Bank shall not be liable to compensate customers for delayed credit, if some unforeseen events (including but not limited to civil commotion, sabotage, lockout, strike or other labour disturbances, accident, fires, natural disasters/calamities or other "Acts of God", war, damage to the Bank's facilities or of its correspondent , Bank's lack of connectivity, absence of the usual means of communication or all types of transportation etc., which are beyond the control of the Bank, prevent the Bank from performing Banking obligations within the specified service delivery parameters.

15. Review of Policy

The policy shall be reviewed **annually** and shall remain in force until the next review. Any instructions, guidelines, or circulars issued by statutory, regulatory, or supervisory authorities from time to time in respect of this policy shall be deemed to form an integral part of the policy.

In the event that any modification/amendment to the policy is necessitated due to changes in the operating environment, market conditions, or other relevant factors, the Risk Management Committee, headed by the Chairman, will be authorized to approve such modifications. The modifications so approved will be placed before the Board at the time of the subsequent periodic review for confirmation.

Annexure: A

FORMAT FOR RESTORATION PROPOSAL
(In case of customer negligent)

Note to:

Observations of the Branch	Observations of the RO

Sir,

Issue for consideration:

For Restoration proposal of un-authorized transactions for the below incidents:

- Un-authorized online transaction occurred in customer account and it is due to 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 beyond seven working days of receiving the communication from the bank regarding the unauthorized transaction.
- For the comparative negligence at the end of the customer

Background:

Sr. No.	Branch / Region	
1	Name of the a/c and Type (SB/CA/CC) of account in which Fraud was occurred.	
2	Amount involved	
3	Date of Occurrence	
4	Date of detection	
5	Reasons for delay in detecting the fraud	
6	Date of reporting.	
7	Brief history/modus operandi(i.e. Detail of accounts involved with names of Account holders, branches, Banks, Account Nos. transaction Nos. etc., modus operandi, and summery of Further remittance of money Involved in fraud be given here).	
8	Status of Insurance claim	
9	Whether complaint with Police/CBI filed, if so, by whom, Progress, if any.	
10	Whether customer has approached to any court/forum for restoration, if yes, details thereof and progress with our Stand	

Investigation/comments:

1	Investigation (By whom done with gist of report e.g. modus operandi, system & procedure Failure, etc.) (If more than one reports give details of all)	
2	Comparative negligence on the part of customer. (negligence on the part of customer which gave way for fraud should be assessed and commented here)	
3	Whether any lapses on part of staff/staff involvement and if so, action taken.(with present position)	
4	Action taken for recovery e.g. Lien marking of account wherein the fraudulent credit is given and recovery.	

Recommendation and Justification: -

1	Details of amount to be Written-off/Restored. (with appropriation of funds available if any)	
2	Justification for the restoration of amount which was deducted due to comparative negligence on the Part of customer. (negligence on the part of customer which gave way for fraud should be assessed and commented here) Basis of the justification for the restoration must be on the following points: • Business relationship with the customer. • Past records of the customer for such type of grievances. • Established Integrity of the customer. • Branch be satisfied for the reason of negligence given by the customer for such unauthorized transaction.	
3	Whether any lapses on part of staff/staff involvement and if so, action taken.(with present position)	
4	Action taken for recovery e.g. Lien marking of account wherein the fraudulent credit is given and recovery.	
5	Comments & recommendations of Branch Head	
6	Comments & recommendations of Regional Head	

Table 1
Maximum Liability of a customer
(Fraudulent transaction reported to the Bank within 4 to 7 days)

Type of Account	Maximum Customer Liability
• Basic Saving Bank Deposit accounts	Rs. 5,000/-
• All other SB accounts • Current / Cash credit / Overdraft Account of MSMEs • Current Accounts / Cash Credit / Overdraft Account of Individuals with annual average balance (during 365 days preceding the incidence of fraud) / limit up to Rs. 25 lacs	Rs. 10,000
• All other Current / Cash Credit / Overdraft Account	Rs. 25,000/-

Table 2
Overall liability of the customer in third party breaches in such Unauthorised Electronic Banking Transactions where the deficiency lies neither with the bank nor with the customer but lies elsewhere in the system

Time taken to report the fraudulent transaction from the date of receiving the communication	Customer liability
Within 3 working days	Zero liability.
Within 4 to 7 working days	The transaction value or the amount mentioned in below Table 1, whichever is lower
Beyond 7 working days	100% Liability

Table 3
Current Channels available for registration of customer complaint related to unauthorized Electronic Banking Transactions –

Channel	Available during	Timing	Auto Response
Toll-free number for Debit Card	24x7	24x7	No
Reporting to home branch	As per Branch Timings	As per Branch Timings	No

Table 4
Operational Process and TAT

Sr. No.	Issue	Responsibility	Periodfor completion of the Task
1	Acknowledgement of the customer complaint about unauthorized Electronic Banking Transaction	Branch	T Day
2	Blocking of the channel after getting confirmation from the customer	Branch	T Working Day
3	Forwarding of complaint to respective channel owner	Branch	T +1 Working Day
4	Communication to customer to provide the missing details required for resolution of complaint	Branch	T +2 Working Day (the timeline of resolution will start only submission of all details required for resolution of complaints)
5	Collection of the Digital record like transaction alert logs, Electronic Channel logs / EJ to ascertain the negligence of the Bank / customer	Respective Electronic Channel team with help of IT team	T + 5 Working Day
6	Investigation of Unauthorized transaction to determine the extent of customer liability	Respective Electronic Channel team	T + 7 Working Day
7	Reply of complaint to customer and value dated shadow reversal of the amount involved in the unauthorized electronic transaction to the customer's account in such cases in such cases where customer negligence is not found *	Branch	T + 8 Working Day
8	Reply of customer complaint in such cases where Bank's found customer negligence along with the justification	Branch	T + 8 Working Day
9	Intimation of shadow reversal to customer with the details of document required to Bank to get the claim from the Insurance Company and to clear the unauthorized Transaction amount to customer account	Branch in co-ordination with Region and Respective Electronic Channel team	T + 8 Working Day
10	Submission of claim to Insurance Company after getting details / documents from the customer.	Branch	T + 30 Working Day
11	Examination of Staff accountability and the loopholes in the process	Respective Electronic Channel team in co-	T + 60 Working Day

		ordination with the Committee	
12	Investigation of Un-authorized Debit Cases	Respective Electronic Channel team/Head Office	T + 60 Working Day
13	Submission of Restoration proposal of branch to the Higher Authorities in such cases where Bank is liable to compensate the customer and didn't received the claim or received short claim from insurance company.	Region in co-ordination with Respective Electronic Channel team	T + 70 Working Day
14	Release of credit to customer Account	Region/Head Office	T + 70 Working Day
15	Review of such cases where Bank has decided to take back the amount credited in customer account (shadow reversal) or where Bank has rejected the customer complaint and customer is not satisfied with the justification given by the Bank	Region/Head Office	T + 85 Working Day

*Bank will give value dated shadow reverse to customer account by debiting a G/L Suspense Account. Entry of the G/L Suspense Account will be reversed either by claim proceed received from Insurance Company or through the Restoration amount. Regional Office will monitor and reconcile the account.

Table 5
Restoration Power

Authority to whom Restoration power is given in respect of unauthorized electronic banking transactions	Powers as per Administrative Power Guidelines	Restoration Power for Unauthorized Electronic Banking Transactions	Remark
Board	-	Full Power	-
Chairman	-	10 Lacs	-
GM	-	3 lacs	-
RM	-	1 lacs	-

Table 6
Committee to ascertain staff accountability

Committee at Level	Sanctioning authority	Headed by	Members	Quorum
Head Office	General Manager	General Manager	2 Chief Manager 2 Senior Manager	Committee Head and any one Chief Manager and Senior Manager

**********End of Policy**********