Customer Protection Policy

(Unauthorized Electronic Banking Transactions)

Version 2.5

Updated on November 28, 2025

1. Introduction:

HDFC Bank is committed to provide superior and safe customer service experience to all its customers. In order to enable the same, the Bank has over the years invested in technology and has robust security systems and fraud detection and prevention mechanisms in place to ensure safe and secure banking experience for its customers. As entailed in the Citizen's Charter, Bank already has in place policies such as Grievance Redressal Policy, Comprehensive Deposit Policy, Customer Rights Policy and Customer Compensation policy.

Keeping in mind the increasing thrust on financial inclusion & customer protection, the Reserve Bank of India had issued a circular on Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions. (RBI/2017-18/15 DBR.No.Leg.BC.78/09.07.005/2017-18 dated July 6, 2017) which inter-alia requires Banks to formulate a Board approved policy in regard to customer protection and compensation in case of unauthorized electronic banking transactions.

2. Objective:

This document seeks to communicate in a fair and transparent manner the Bank's policy on:

a) Customer protection (including mechanism of creating customer awareness on the risks and responsibilities involved in electronic banking transactions),
b) Customer liability in cases of unauthorized electronic banking transactions
c) Customer compensation due to unauthorized electronic banking transactions (within defined timelines)

3. Scope:

Electronic banking transactions usually cover transactions through below modes:

a) Remote/ online payment transactions (transactions that do not require physical payment instruments to be presented at the point of transactions e.g., Net Banking, Mobile Banking, Card Not Present (CNP) transactions, Smart apps, Pre-paid Payment Instruments (PPI) including but not limited to electronic wallets, etc.)
b) Face-to-face/ proximity payment transactions (physical payment instrument is required such as a card or mobile phone to be present at the point of transaction e.g., ATM, PoS, etc.)
c) Any other electronic modes of credit effected from one entity to another currently being used or adopted from time to time

This policy covers transactions only through the above modes. The policy excludes electronic banking transactions effected on account of an error by a customer (e.g., NEFT carried out to an incorrect payee or for an incorrect amount), transactions done under duress, claims due to opportunity loss, reputation loss, other incidental costs or collateral damage.

4. Applicability:

a) This policy is applicable to individuals/ entities that hold relationship with the bank viz.:
    i) Individual and non-individual customers who hold current or savings account.
    ii) Individual / non-individual entities that hold credit card /debit card and/or prepaid card/Term loan and/or Jumbo Loans.
    iii) Individual / non-individual entities that use other electronic payment modes / platforms of the Bank like Net Banking, Mobile Banking **(**IMPS/RTGS/NEFT), UPI, AePS and PPI wallets**(**PayZapp/FASTag).

b) This policy is not applicable to:
    i) Non-Customers who use Bank's infrastructure e.g. ATMs/ PoS etc.
    ii) Entities that are part of the ecosystem such as Interchange organisations, Franchises, Intermediaries, Agencies, Service partners, Vendors, Merchants etc.

iii) Cases wherein customer is claiming non-receipt or short receipt of cash from ATM since such transactions are conducted by the customer himself/herself. Also, such complaints are resolved in line with RBI guideline on ATM failed transactions.

5. Definitions & Explanations: (for the purpose of this policy)

a) Real loss is defined as financial outgo from customer's account e.g., debit to customer's account or card.
b) Card Not Present (CNP) transactions are defined as transactions that require use of Card specific information (e.g., card number, card expiry date, CVV number, PIN etc.) without card being physically used e.g., e-commerce transactions, wallet transactions.
c) Card present (CP) transactions are defined as transactions that require use of physical card e.g., at ATM, POS, digital form factors etc.
d) Payment transactions are defined as transactions that involve transfer of funds from one account/ wallet to another electronically and do not require card information e.g., NEFT.
e) Unauthorised transaction is defined as debit to customer's account without customer's consent.
f) Consent includes authorization of a debit transaction 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 use of security passwords, input of dynamic password (OTP) or static password, challenge questions or use of Card details (CVV/ Expiry date/PIN) or any other electronic authentication option provided by the Bank.
g) Date & time of reporting is defined as date & time on which customer has submitted a unique complaint (pertaining to unauthorized electronic banking transaction). 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.
h) Notification means an act of the customer reporting unauthorized electronic banking transaction to the bank.
i) Number of days will be computed based on working days.
j) Mode of reporting will be the channel through which customer complaint is received first time by the Bank, independent of multiple reporting of the same unauthorized electronic banking transaction.
k) Loss in foreign currency if any shall be converted to Indian currency for the purpose of this policy as per bank's policies on conversion at card rate net of commission.

6. Points covered under the policy:

Customer shall be compensated in line with this policy in case of loss occurring due to unauthorized electronic banking transaction as below:

a) <u>Zero Liability of customer</u>
   i) Customer shall be entitled to full compensation of real loss in the event of contributory fraud/ negligence/ deficiency on the part of the bank (irrespective of whether or not the transaction is reported by the customer)
   ii) Customer has Zero Liability in all cases of 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 transactions.

b) <u>Limited Liability of customer</u>
   i) Liability in case of financial losses due to unauthorized electronic transactions where responsibility for such transaction lies neither with the bank nor with the customer, but lies elsewhere in the system AND
   ii) there is a delay on the part of customer in notifying/reporting to the Bank beyond 3 working days and less than or equal to 7 working days (after receiving the intimation from the Bank), the per transaction

liability of the customer shall be limited to transaction value or the amount mentioned in Annexure -1 whichever is lower.

c) Complete Liability of customer

i) Customer shall bear the entire loss in cases where the loss is due to negligence by the customer, e.g. where the customer has shared payment credentials or Account/Transaction details, viz. Internet Banking user Id & PIN, Debit/Credit Card PIN/OTP or due to improper protection on customer devices like mobile / laptop/ desktop leading to malware / Trojan or Phishing / Vishing attack. This could also be due to SIM deactivation by the fraudster.

Under such situations, the customer will bear the entire loss until the customer reports unauthorised transaction to the bank. Any loss occurring after reporting of unauthorised transaction shall be borne by the bank.

ii) In cases where the responsibility for unauthorized electronic banking transaction lies neither with the Bank nor with the customer, but lies elsewhere in the system and when there is a delay on the part of the customer in reporting to the Bank beyond 7 working days, the customer would be completely liable for all such transactions.

d) Other Points

i) The Bank shall afford shadow credit to the customer account within 10 working days from the date of reporting in all cases as per above statements. In case the Bank is unable to resolve the complaint / determine customer liability within 90 days of reporting date, the Bank shall credit the customer with compensation value as specified in this policy. Customer will be given value dated credit (based on date of unauthorized transaction) when customer becomes eligible to be compensated. In case of debit card/ bank account, the customer shall not suffer loss of interest and in case of credit card; customer shall not bear any additional burden of interest for such credit.

ii) Customer would not be entitled to compensation of loss if any, in case customer does not agree to get the card blocked, NetBanking ID blocked, enable debit block on his/her account or does not co-operate with the Bank by providing necessary documents including but not limited to copy of police complaint and cardholder dispute form complete in all respects.

iii) Compensation would be limited to real loss after deduction of reversals or recoveries received by the customer.

7. Third Party Breach

The following would be considered as Third-party breach where deficiency lies neither with the Bank nor with the customer but elsewhere in the system:

a) Identity Theft
b) Skimming / cloning
c) External frauds / compromise of other systems, e.g., ATMs / mail servers etc. being compromised

8. Roles & Responsibilities of the Bank:

a) The Bank shall ensure that the Customer protection policy is available on the Bank's website as well as at Bank's branches for the reference by customers. The Bank shall also ensure that existing customers are individually informed about the bank's policy.

b) The Bank will conduct awareness on carrying out safe electronic banking transactions to its customers and staff. Information of Safe Banking practices will be made available through campaigns on any or all of the following - website, emails, ATMs, Phone Banking, Net Banking, Mobile Banking etc. Such information will

include rights and obligation of the customers as well as non-disclosure of sensitive information e.g., accounts/ cards details, password, PIN, OTP, date of birth, etc.

c) The Bank shall communicate to its customers in getting their mobile numbers registered with the bank to receive SMS alerts. The Bank will send SMS alerts to all valid registered mobile numbers for all debit electronic banking transactions. The Bank may, depending on the system functionality, also send alert by email where email Id has been registered with the Bank.

d) The Bank will enable various modes for reporting of unauthorized electronic banking transaction(s) by customers. These may include SMS, email, website, toll free number, IVR, Phone Banking or through its branches. The Bank will also enable specific space on its home page where customers can report unauthorized electronic banking transaction.

e) The Bank shall respond to customer's notification of unauthorized electronic banking transaction(s) with acknowledgement specifying complaint number. On receipt of customer's notification, the Bank will take immediate steps to prevent further unauthorized electronic banking transactions in the account or card etc.

f) The Bank shall ensure that all such complaints are resolved and liability of customer, if any, established within a maximum of 90 days from the date of receipt of complaint, failing which, bank would pay compensation as described in Annexures 1.

g) During investigation, in case it is detected that the customer has falsely claimed or disputed a valid transaction, the bank reserves its right to take due preventive action of the same including closing the account or blocking card limits.

h) The Bank may restrict customer from conducting electronic banking transaction(s) other than ATM transaction(s) in case of non-availability of customer's mobile number.

i) This policy should be read in conjunction with Grievance Redressal Policy of the Bank. Clauses from the Bank's Grievance Redressal Policy shall form a part of this policy which are not specifically addressed in this policy. The Grievance Redressal Policy is available on the bank's website.

j) The Bank may use documents such as audit trail/logs, and any other admissible evidence needed for investigation / requirements in line with this policy

9. Rights & Obligations of the Customer

a) Customer is entitled to
   i) SMS alerts on valid registered mobile number for all financial electronic debit transactions
   ii) Email alerts where valid email ID is registered with the Bank
   iii) Register complaint through multiple modes – as specified in above point 8 d) relating to Roles & Responsibilities of the Bank.
   iv) Intimation at valid registered email/ mobile number with complaint number
   v) Receive compensation in line with this policy document where applicable. This would include getting shadow credit within 10 working days from reporting date and final credit within 90 days of reporting date subject to customer fulfilling obligations detailed herein and with customer liability being limited as specified in Annexure-1

b) Customer is bound by following obligations with respect to banking activities:

   i) Customer shall mandatorily register valid mobile number with the Bank.
   ii) Customer shall immediately update his /her registered contact details as soon as such details are changed. Bank will only reach out to customer at the last known email/ mobile number registered with the bank. Any failure of customer to update the Bank with changes due to loss of mobile handset/change of mobile number or any other reason/act by customer leading to transaction alerts/OTP not reaching customer shall be considered as customer negligence. Any unauthorized transaction arising out of this delay shall be treated as customer liability.
   iii) Customer should provide all necessary documentation – customer dispute form, proof of transaction success/ failure and should also file a police complaint (wherever applicable) and provide copy of the same to the Bank.

iv) Customer should co-operate with the Bank's investigating authorities and provide all assistance.
v) Customer must not share sensitive information (such as Account/ Debit/ Credit/ Prepaid Card details & PIN, CVV, NetBanking ID & password, OTP, transaction PIN, Wallet details or challenge questions) with any entity, including bank staff.
vi) Customer must protect his/her device as per best practices specified on the Bank's website, including updation of latest antivirus software on the device (Device includes smart phone, feature phone, laptop, desktop and Tab)
vii) Customer shall abide by the tips and safeguards mentioned on the Bank's website on Secured Banking available at https://www.hdfcbank.com/personal/security
viii) Customer shall go through various instructions and awareness communication sent by the bank on secured banking
ix) Customer must use card controls, including set transaction limits to ensure minimized exposure from time to time and also update overseas travel plans so that bank is aware of the customer whereabouts for transaction confirmation.
x) Customer must verify transaction details from time to time in his/her bank statement and/or all card statement and raise query with the bank as soon as possible in case of any mismatch/ dispute.
xi) Customer shall report unauthorized electronic banking transaction(s) to the Bank at the earliest after occurrence of such transaction. Further longer the time taken in reporting unauthorised transaction to the Bank, higher is the risk of loss to the bank/customer.

10. Notifying the Bank of the unauthorized transaction:

a) Customer shall report unauthorized electronic banking transaction(s) to the Bank at the earliest, with basic details such as Customer ID and/ or Card number (last 4 digits), date & time of transaction and amount of transaction.
b) Customer shall follow bank's reporting process viz.
   i) Notify/ report through the options listed in the section on Roles & responsibilities of Bank (8 d)). In case customer is unable to do so, customer could report through phone banking or at the nearest branch.
   ii) Lodge police complaint and maintain copy of the same and furnish police complaint when sought by bank's authorised personnel.
c) Customer shall authorise the bank to block the Credit/ Debit/ Prepaid card/ NetBanking/ Account(s) / Wallet to reduce likelihood of additional loss
d) Customer to clearly specify the facilities to be blocked failing which the Bank reserves the right to block all modes through which electronic banking transactions can be carried out to protect the customer's interest. Also, revoking these blocks would require explicit consent from customer for each facility.
e) Customer shall share relevant documents as needed for investigation or insurance claim viz. cardholder dispute form, copy of passport in case of international transactions and police complaint (wherever applicable).
f) Fully co-operate and comply with Bank's reasonable requirements towards investigation and provide details of transaction, customer presence, etc.

11. Proof of customer liability:

The Bank has a process of second factor authentication for electronic transactions, as regulated by the Reserve Bank of India. Bank has onus to prove that all logs / proofs / reports for confirming two factor authentication are available. 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.

12. Force Majeure:

The bank shall not be liable to compensate customers for delayed credit if some unforeseen event (including but not limited to civil commotion, sabotage, lockout, strike or other labour disturbances, accident, fires, natural

disasters or other "Acts of God", war, damage to the bank's facilities or of its correspondent bank(s), absence of the usual means of communication or all types of transportation, etc. beyond the control of the bank prevents it from performing its obligations within the specified service delivery parameters.

Annexure -1

Unauthorised Transaction due to Bank's negligence	
Time taken to report the fraudulent transaction from the date of receiving communication from the Bank	**Customer's Maximum Liability (Rs.)**
Customer to report as soon as possible to prevent future losses	Zero Liability
Unauthorised Transaction due to Customer's negligence	
Time taken to report the fraudulent transaction from the date of receiving communication from the Bank	**Customer's Maximum Liability (Rs.)**
Customer to report as soon as possible to prevent future losses	100% liability till it is reported to Bank

Maximum Liability of a Customer in case of unauthorized Electronic Transaction where Responsibility is neither with the Bank nor with the customer but lies elsewhere in the system & customer has reported unauthorized transaction from transaction date within working days specified in following table:		
Type of Account	**Within 3 working days (Rs.)**	**Within 4 to 7 working days (Rs.)**
BSBD Accounts	Zero Liability	5,000
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
Digital Term Loans where disbursement is not done in the Customer's Savings Account		10,000

Any unauthorized electronic banking transaction reported after 7 working days will be treated as 100% customer liability.

---------- End of Document ----------