Policy on Customer Protection for Unauthorized Electronic Banking Transactions

BNP Paribas complies with Internet Banking Guidelines issued by Reserve Bank of India (RBI) from time to time.

This policy is based on the RBI Circular reference: DBR.No.Leg.BC.78/09.07.005/2017-18 dated July 6, 2017 outlining guidelines on 'Customer Protection – Limiting Liability of Customers in Unauthorized Electronic Banking Transactions' (the "**RBI Guidelines**") and seeks to lay down the manner in which the Bank will handle customer complaints pertaining to unauthorized transactions.

Definitions

In this policy:

'Bank' means BNP Paribas.

'Customer' means any customer, entity banking with BNP Paribas.

'Online Payment' means a payment instruction initiated by a Customer electronically on the electronic banking channel/platform or the mobile app of the Bank.

'Unauthorized Transaction' would mean an Online Payment instruction that has not been initiated/authorised by the Customer.

Safeguarding Customer's details

The Bank on an on-going basis makes efforts to safeguard its customers and their information by putting in place robust systems which are upgraded from time to time. The Bank has also put in place additional measures such as dual factor authentication, access controls, transaction limits, email alerts and transaction reports etc. to further mitigate security concerns arising out of electronic transactions.

We encourage Customers to refer security tips for safe internet banking and mobile banking experience that have been provided in Annexure 1

In accordance with the RBI Guidelines, the following measures will be adopted by the Bank in connection with instances of Unauthorised Transactions reported to the Bank:

A. Reporting of Unauthorized Transactions by Customers to the Bank

i. The Customers must notify the Bank of any Unauthorized Transaction at the earliest after its occurrence. It is to be noted that longer the time taken to notify the Bank, the higher will be the risk of loss to the Bank / Customer.

Customers should promptly notify the bank of an Unauthorized Transaction at : **india.ebsupport@asia.bnpparibas.com.**

ii. Additionally, the Customer should promptly notify the concerned relationship manager at the Bank to enable faster escalation procedure

iii.

iv. On receipt of intimation of an Unauthorized Transaction from the Customer, the Bank will take immediate steps to the extent possible, to prevent further Unauthorized Transactions in the account

v. All grievance redressal will be done in line with the BCSBI Code (Banking Codes And Standards Board Of India) available on https://www.bnpparibas.co.in

B. The Customer will be compensated by the Bank for any consequential financial loss as per the below guidelines:

- **Zero Liability of Customer**

A Customer's entitlement to zero liability shall arise where the Unauthorised 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 3 working days of receiving the communication from the Bank regarding the Unauthorised Transaction.

- **Limited Liability of a Customer**

A Customer shall be liable for the loss occurring due to Unauthorized Transactions in the following cases:

i. In cases where the loss is due to negligence by a Customer, such as where the Customer has shared user credentials, the Customer will bear the entire loss until the Customer reports the Unauthorized Transaction to the Bank. Any loss occurring after the reporting of the Unauthorized Transaction shall be borne by the Bank.

ii. In cases where the responsibility for the Unauthorized 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 lower of the transaction value or the amount as mentioned in table below.

No.	Time taken to report the Unauthorised Transaction from the date of receiving the communication from the Bank	Customer's Liability (in INR)
1.	Within 3 working days	Zero liability
2.	Within 4 to 7 working days (Current Accounts/Savings Account/Cash Credit/ Overdraft Accounts/Trade Transactions with annual average balance / limit up to INR.25 lakh)	The transaction value or INR 10,000, whichever is lower
3.	Within 4 to 7 working days (All Other Current/Savings/ Cash credit/ Overdraft Accounts/ Trade Transactions)	The transaction value or INR 25,000, whichever is lower
4.	Beyond 7 working days	Customer's liability will be determined on a case by case basis by the business head(s) of the Bank taking an overall view of RBI guidelines, Customer background and circumstances of the occurrence

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

C. **Reversal timeline in case of liability and reporting**

On being notified by the Customer, the Bank shall credit (shadow reversal) the amount involved in the Unauthorized 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 sole discretion decide to waive off any Customer liability in case of Unauthorized Transactions even in cases involving the Customer's negligence. The credit shall be value dated to be as of the date of the Unauthorized Transaction.

Further, the Bank shall ensure that:

i. Communication from the Bank is sent to the email IDs of Customers registered with the Bank. In case of any discrepancies / deficiencies, the Customer should notify the bank not later than 3 working days from receipt of information from the Bank

ii. A complaint is resolved and liability of the Customer, if any, is established within a maximum period of 90 days from the date of receipt of the complaint, and the Customer is compensated as per provisions outlined above.
iii. Where the Bank is unable to resolve the complaint or determine the Customer liability, if any, within the aforementioned period of 90 days, the compensation as prescribed above will be paid to the Customer;
iv. The Customer does not suffer loss of interest or does not bear any additional burden of interest.
v. The Bank shall not only inform its existing clients of such a policy but also inform the client of security tips for safe internet banking and mobile banking experience from time to time
vi. Incident reports are reviewed on a quarterly basis by the Operational Risk / Permanent Control team(s) and corrective steps are taken as applicable. Thereafter, the report will be further presented in the Management Committee meeting
vii. The Standing Committee on Customer Service in the Bank shall review the Unauthorized 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.
viii. All such transactions shall be reviewed by the Bank's internal auditors.
ix. Any system / IT security related changes shall be tabled in the quarterly IT Steering Committee. The standard operating procedures are updated from time to time with regard to safety and security of electronic banking transactions

This policy shall continue to hold good unless otherwise a review is warranted for change in regulatory directives or as the Bank's Committee may deem fit. The policy will be made available on the Bank's website (https://www.bnpparibas.co.in)

Annexure 1

- Avoid accessing your Internet banking account from a cyber cafe. If you happen to do so, we recommend changing your password from your own computer as soon as possible

- Every time you complete your online banking session, log-off. It is important to not just close your browser as anyone who access your computer may be able to log onto your Internet banking account.

- You should use a strong password for all secure websites you access. The password should be difficult for others to guess. We suggest using at minimum 8 characters using a mixture of letters, numbers and symbols.

- Never share your Internet Banking login credentials/passwords with others including any third party vendor as it can have financial/data confidentiality impacts. This also includes someone claiming to be a Bank employee. BNP Paribas will never ask you for your password.

- When accessing the online banking website, here are a few checks that you should make before entering in your password:

    i. The URL should start with 'https://' which means that it is a secure connection.

    ii. It is always best practice to type the website's address in the browser. You may be sent fraud emails that appear to go to your online bank but actually send you to a website designed to steal your information.

- Make sure you protect your mobile device with up-to-date internet security software.

- Only use official mobile banking apps provided by your bank (e.g. BNP Paribas mobile banking solution BankSmart) and only download apps from the official app store.

- Set up a strong password or PIN to lock your mobile handset. The password should be difficult for others to guess.

- Never share your security details with others and never store them on your mobile device in a way that might be recognized by someone else.

- Never share your mobile banking passwords, PIN with others. This includes someone claiming to be a Bank employee. BNP Paribas will never ask you for your passwords.

- Every time you complete your online banking session, log-off

Please note that BNP Paribas will never send e-mails that ask for confidential information. If you receive an e-mail requesting your Internet banking security details like PIN or password, please do not respond, and report all such incidents to india.ebsupport@asia.bnpparibas.com