TranServ Private Limited

(CIN: U93090MH2010PLC211328)

CUSTOMER PROTECTION POLICY

Limiting Liability of Customers in Unauthorized Transactions

(Reviewed and Adopted by the Board as on 21/10/2019)

Background

Increase in transactions using prepaid payment instruments (PPIs) has multiplied the associated risks and hence Customer Protection against unauthorized electronic payment transactions has assumed greater importance. The Reserve Bank of India (RBI) vide its circular RBI/2018- 19/101/DPSS.CO. PD.No. 1417 /02.14.006/2018-19 has laid down the provisions for determining the customers' liability in unauthorized electronic payment transactions resulting in debit to their wallet/cards.

Objective

RBI requires PPI issuers to formulate a policy covering aspects of customer protection, including the mechanism of creating customer awareness on the risks and responsibilities, and customer liability arising in specific scenarios of unauthorised electronic transactions.

The objective of this policy is to provide a comprehensive guideline to protect customers in case of any unauthorised transactions undertaken using the Dhani Pay PPIs issued by Transerv.

Categories of transactions:

Electronic payment transactions using Dhani Pay PPIs are divided into two categories:

I. Remote / Online payment transactions (transactions that do not require physical PPIs to be presented at the point of transactions e.g. wallets, card not present (CNP) transactions, etc.).
II. Face-to-face / Proximity payment transactions (transactions which require the physical PPIs such as cards or mobile phones to be present at the point of transactions e.g. transactions at Point of Sale, transactions done via mobile app etc.)

Roles & Responsibilities of TranServ

i. TranServ will ensure that the Customer protection policy is available on the website as well the mobile app for reference by customers.

ii. TranServ will conduct awareness on carrying out safe electronic transactions by sending emails to customer on non-disclosure of sensitive information e.g. password, PIN, OTP, date of birth, etc.

iii. TranServ will ensure SMS alerts and email alerts for all payment transactions mentioning the contact details
to report unauthorised transactions or notify objections.

iv. TranServ will advise customers to notify any unauthorised transaction at the earliest to avoid the risk of loss due to delay in informing TranServ.

v. TranServ will facilitate 24X7 access via website/sms/e-mail for customers to report any unauthorized transactions. TranServ will also provide an option on mobile app/home page to report any such transaction.

vi. TranServ will ensure immediate response as acknowledgement to the complaint lodged. The systems will record the date and time of receipt of complaint.

vii. TranServ will also ensure that no transaction is conducted post lodging of complaint of an unauthorized transaction by the customer until the complaint has been resolved.

viii. Within 10 days of the lodging the complaint TranServ will pass a notional credit as per the
applicable customer liability. TranServ will within 90 days resolve the complaint and pay to the customer eligible amount.

ix. In case of non-resolution to determine customer liability within 90 days the customer will become eligible for the compensation.

x. During the investigation, if it is found that the customer has falsely claimed or disputed a valid transaction, TranServ reserves the right to cancel the notional credit and take preventive action including blocking of wallet/card.

Obligations of Customer

a) Customer should 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 TranServ.

b) Customer should co-operate with TranServ investigating team and provide all assistance.

c) Customer must not share sensitive information (such as Card details & PIN, CVV, user Id & password, OTP, transaction PIN, challenge questions) with any entity, including TranServ staff.

d) Customer must set transaction limits to ensure minimized exposure.

e) Customer must protect their device as per best practices including updation of latest antivirus software on the device (Device includes smart phone, feature phone, laptop, desktop and Tab) Customer must verify transaction details from time to time from the account statement and raise query with TranServ as soon as possible in case of any mismatch

f) Customer will go through various instructions and awareness communication sent by TranServ.

Liability of a Customer

a) Zero Liability of the customer:

A customer's entitlement to zero liability will arise where the unauthorized transaction occurs in the following events:

- Contributory fraud/ negligence/ deficiency on the part of TranServ (irrespective of whether or not the transaction is reported by the customer).
- Third party breach where the deficiency lies neither with TranServ nor with the customer but lies elsewhere in the system, and the customer notifies TranServ within three (3) days[1] of receipt of transaction communication.
- Any loss occurring after the reporting of unauthorized transaction.

b) Limited Liability of the customer:

A Customer Liability for the loss occurring due to unauthorized transaction where the deficiency lies neither with TranServ nor with the customer but lies elsewhere in the system (*Third Party Breaches*), and the customer notifies TranServ after three (3) days and within seven (7) days of receipt of transaction communication will be equal to transaction value or Rs.10,000 per transaction, whichever is lower.

Complete Liability of the customer:

Customer will 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. user Id & PIN, 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
- the deficiency lies neither with TranServ nor with the customer but lies elsewhere in the system, and the customer notifies TranServ after seven (7) days of receipt of transaction communication. Company may also, at their discretion, decide to waive off any customer liability in case of unauthorised electronic payment transactions even in cases of customer negligence.

Proof of Customer Liability

TranServ has a process of second factor authentication for all card transactions, as regulated by the RBI. TranServ has onus to prove that all logs / proofs / reports for confirming two factor authentications is available. Any unauthorized 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

[1] Number of days mentioned will be counted excluding the date of receiving communication for transaction Customer Protection Policy

in effecting the transaction.

Reporting and Monitoring

TranServ will put in place a mechanism for reporting the customer liability cases to the Board or its Committee. The reporting will inter-alia, include volume/ number of cases and the aggregate value involved and distribution across various categories of case. Additionally, TranServ will put in place a mechanism to enable review of such transactions and examine the effectiveness of the measures taken. Company to given an option to generate / receive account statements for at least past 6 months. The account statement shall, at the minimum, provide details such as date of transaction, debit / credit amount, net balance and description of transaction. Additionally, company shall provide transaction history for at least 10 transactions.

Review of the Policy

The Policy will be reviewed annually by the Board, or as and when required, including in cases of changes in the business or regulatory environment.