Use of RuPay Cards in Government Scheme

Government of Maharashtra
General Administration Department (IT)
Government resolution, No.: MH-904/2/2012-DIT-MH-1
Date: 07th January, 2015

Introduction:

Department of Electronics and Information Technology (DEITY), Government of India as part of National e-Governance Plan is in the process of implementing end-to-end transactional experience for a citizen using e-Governance infrastructure which includes accessing various services through Common Service Centres and online payments using internet based payment gateway. DEITY has appointed NSDL database Management Limited (NDML) to provide payment gateway services, for various citizen services provided by Centre and State Governments, through National Payment Services Platform (NPSP) which is currently being implemented with various Central & State Government Departments.

2. National Payments Corporation of India (NPCI) was formed by RBI to have a nation-wide uniform & standard business process for all retail payment systems. RuPay, payment scheme was launched by NPCI to offer a domestic, open-loop, multilateral system which will allow all Indian banks and financial institutions in India to participate in electronic payments.

3. With the RuPay, all the transaction happens domestically. Thus the cost associated with each transaction is low and remains within the country. The amount of e-Transactions by Government of Maharashtra itself is more than Rs. 80,000/- Crores annually. Further it will grow significantly in coming days as more and more services are e-Delivered. Thus using RuPay instead of Master/Visa/AMEX etc. makes a strong case for saving costs and ensuring the amount remains within the country.

4. Jan Dhan Yojana is also promoting Financial Inclusion of the poor people in a big way by opening their bank accounts and linking with RuPay card.

Government Resolution:

a) Wherever the Government Departments, Local Bodies and State Government Undertakings tie up with banks to issue debit/credit/ATM cards

RuPay Implementation Guidebook

Version 1.0 – 27 April 2012

A. Objective of the document

This document provides the guidelines for enrolment of the new debit card program of NPCI. It explains the card features, implementation planning considerations and the steps required for issuers to issue the debit card. The document also contains the details that go into a cardholder usage manual.

This document is intended for all the issuers issuing debit cards.

B. References and publications

The list of manuals which have been referenced in this document are given as under:

1. Member Certification Guidebook
2. RuPay Product Manual
3. RuPay Card Marks & Specifications
4. RuPay Enterprise Risk Management Document

1. Introduction

National Payments Corporation of India (NPCI): NPCI has been formed to consolidate and integrate the multiple systems with varying service levels into nation-wide uniform and standard business process for all retail payment systems. NPCI facilitates an affordable payment mechanism to benefit the common man across the country and help grow the retail payments in India

RuPay: RuPay is a brand of NPCI under which it operates the card scheme and this document is published by NPCI for its RuPay card scheme

The terms NPCI and RuPay have been used interchangeably in this document and refer to the card scheme entity promoted by NPCI. NPCI owns the RuPay card scheme and NPCI is the decision maker with reference to all matters

2. RuPay Debit Card Product Overview

The RuPay debit cards can be used for ATM, POS, IVR and for online e-commerce transactions. The card will have all the product features as highlighted in the Product Features section as the minimum features. The issuer can add other features on the card with approval from NPCI.

3. Issuer Requirements

The requirements for the debit card are designed to ensure that the cardholders receive maximum value from RuPay debit card. Debit card issuers are required to certify their compliance with NPCI prior to the launch of the product as per the guidelines mentioned in the Member Certification Guidebook

NPCI can audit the issuing members at any time for compliance to ensure adherence to the compliance guidelines on various areas laid down by NPCI.

3.1. Card Name

All RuPay debit card Issuers must use the name of the RuPay debit card. The name of the RuPay debit card must appear on:

a) All plastics
b) All statements & communications to the cardholder like promotions, campaigns, newsletters, usage guide, and statements related to card program

The RuPay debit card name may be used in conjunction with the issuer's name on all such communications.

3.2. Card Design

a) Issuers must comply with the design, brand and other guidelines as specified in the RuPay Card Marks & Specifications Document
b) The issuers customer service number must be printed on the back of the card
c) All card designs must be approved by NPCI prior to sending the same for production

3.3. Reporting

All debit card issuers must do the basic reporting to NPCI like the number of cards issued, number of cities covered, number of transactions, value of transactions, campaigns history, and activation of the debit cards on POS machines & ATMs. This reporting should be done by the issuer on a quarterly basis. The report can be sent over an email to the associated relationship manager or product manager of NPCI. The details of the parameters for reporting are as under:

Parameters	Details (product-wise)
Number of cards issued	Classic Gold Platinum
Number of transactions	Classic Gold Platinum
Volume of transactions	Classic Gold Platinum
Activation rate	Classic Gold Platinum

3.4. Customer Service

a) Issuers must provide a customer service number to all its cardholders. The same needs to be mentioned on the card, usage guide, website, promotional campaigns and any other mode of communication.

b) Any change in the customer service number must be promptly communicated to the cardholders at least 45 days in advance of the change.

3.5. Bank Identification Number (BIN)

a) For the RuPay debit card issued, the issuer must use the unique BIN assigned by NPCI. In case the issuer requires a new BIN, then the issuer needs to submit its request to NPCI for assigning of a new BIN to the member.

3.6. Marketing materials

a) Issuers must submit samples of all their marketing communications, terms & conditions, website content, and disclosures to NPCI for approval prior to publishing the same. The same should be submitted to NPCI for approval at least 30 days prior to publishing the materials

b) NPCI's review of marketing and other materials is only for the purpose of checking if they do not violate any compliance or pose any risk to the brand of NPCI. All the legal compliance of the materials is to be done by the issuer

3.7. Fraud Protection Services

NPCI will help the issuers with the risk management set-up (assistance for possible risk areas and sharing of risk controls for their systems) and to support the RuPay debit card program. NPCI will provide the issuing members with risk management program that comprise of tools like:

a) Fraud detection during authorization
b) Velocity checks
c) Online monitoring & referrals

The details of the fraud & risk management tool can be obtained from NPCI on request. The security measures are further elaborated in the RuPay enterprise risk management document.

All issuers must mandatorily report all fraudulent transactions within 10 days of detection of the fraud. Some of the fraudulent transactions are mentioned under:

a) Lost card: Transactions generated on an account number for a card that is reported as lost
b) Stolen card: Transactions generated on an account number for a card that is reported as stolen
c) Card not received: Transactions generated by a card that the rightful owner claims not to have received
d) Fraudulent application: Transactions generated by a card that has been issued due to a fraudulent card application
e) Skimming: Skimming is the theft of card information used in an otherwise legitimate transaction. The details can be procured using basic methods such as photocopying receipts or more advanced methods such as using a small electronic device (skimmer) to swipe and store hundreds of victims' card numbers
f) Phishing: Phishing is a way of attempting to acquire information such as usernames, passwords and card details by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting card holders

3.8. Product Features

RuPay debit card will be accepted across all channels like ATM, POS, IVR, MOTO and E-commerce. Further details on the product features can be obtained from the RuPay Product Manual

3.9. Pricing

a) **NPCI pricing to issuers:** The pricing to the issuers for this product will be maintained as per the member agreement and the pricing slab. The major fee types that will be charged includes:

   a. Assessment Fees
   b. Authorization Charges
   c. Transaction Processing Fees

   Besides the above, there are other fees that could be charged to the issuers

b) **Issuer pricing to cardholders:** The issuer annual and renewal fees to the cardholder is at the discretion of the issuer.

c) **Interchange:** The interchange for the debit card as prescribed by NPCI will apply for this product.

d) **Cost of the card:** The cost of the plastic has to be borne by the issuer and NPCI will not bear any cost. The card should be manufactured as per NPCI standards (mentioned in the Card Marks and Specifications Document) and from authorized NPCI vendor. The issuer needs to inform NPCI about the selection of its card manufacturer.

Further details about the pricing are mentioned in the RuPay Product manual.

3.10. Authorization Approval

The issuer should have a 99% authorization approval rate for all the merchant transactions on a monthly basis except cash at POS transactions and cash back transactions. NPCI will review the issuer authorization approval rate on a regular basis and take required action (penalties, termination of membership) as appropriate.

3.11. Legal & Regulatory Compliance

a) It is the primary and sole responsibility of the issuer to ensure that all its card programs, customer relationships, terms & conditions are in compliance with all applicable government law, RBI guidelines, NPCI guidelines and other regulatory guidelines.

b) Issuers are responsible for ensuring compliance with the anti-money laundering policies as per The Prevention of Money Laundering Act, 2002, its amendments and any other related guidelines on the Anti-Money Laundering

c) Issuers are responsible for ensuring compliance with any privacy related regulations of the government which includes sharing of cardholder information with any third party.

d) Issuers are responsible for payment of all government taxes related to the card program.

3.12. Certifications

The issuers must submit a written document that all its systems related to the implementation of RuPay debit card have been certified and are in compliance with NPCI requirements.

3.13. Audit

NPCI or any organization designated by NPCI may audit the system, records and procedures or facilities of the issuer (or TPPs) at any given point of time.

4. Implementation

This section provides the guidelines for setting up the different teams required while enrolling for the RuPay card product. This information can be used to help formulate an implementation project and evaluate the impact of a RuPay debit card on the member. This section outlines some of the steps that can help the issuers for implementing the card program.

4.1. Establishing a project team

The issuer may set-up a project team which will champion the implementation plan and manage the project from the issuer's end in conjunction with NPCI. NPCI mentions below a typical project implementation team structure, however the issuer can have its own implementation team.

a) **Project manager:** The Project manager is responsible for the overall project and managing the timelines involved in completion of the project including the key milestones

b) **Audit:** The representative from the audit team ensures that the requirements meet the issuer's operational standards and the service level agreements.

c) **Product/Business team:** The Product team is the central team which is responsible for launch of the card and supporting the branch / sales team centrally in terms of new account processing, new forms and query management

d) **Customer Service team:** The customer service team will be responsible for handling the customer queries and complaints regarding the RuPay debit card.

e) **Finance team:** The Finance team will review the basic cost and revenue streams and help the product or business in enhancing the net profit from this program

f) **Legal team:** The legal team will advise and ensure compliance with all applicable laws and regulations

g) **Risk Team:** The risk and fraud management team will help in establishing fraud prevention mechanism, transaction monitoring, risk engine and risk scoring, investigate suspected fraudulent activity, and on-field investigation

h) **Operations:** The issuer must have an operations team to manage the entire back-end processing with regards to dispute management, settlement of funds and chargeback

i) **Training:** The issuer must have a training team to educate all the concerned officials/teams

5. Roll-out of RuPay Debit Card

A launch strategy defines the issuer's approach to the product rollout. The launch will typically have several stages to ensure that all support functions are in production mode. This section gives a brief of the launch plan of the RuPay debit card.

5.1. Roll-out strategy

The issuer must have a defined launch strategy for the roll-out of the RuPay debit card. The plan will have several stages to ensure that all functions are in place during the roll out.

The issuer should do a pilot launch in few select cities for few select customers to test the systems and ensure all the product features are working as desired. The pilot launch may be done at least 4-6 weeks prior to actual launch to resolve any issues that may arise within that specific point of time. The launch will help the issuer to resolve any issues that may be seen before launching the same on a mass scale.

5.2. Target Segment

The issuer should identify the target customer segment for the RuPay debit cards. The issuer should issue the cards to both the new and the existing card customers. The existing debit card customers can be re-carded with RuPay card at the time of their renewals. RuPay cards can also be issued to customers who have reported to the bank for lost, stolen, expired cards or cards that need replacement.

The potential target segments of the issuers can be, but not limited to, the following:

5.2.1. New / untapped customer segments

a) Customers from mass-market and entry level consumer cards
b) Account holders of Regional Rural Banks (RRBs) / Urban Co-Operative Banks (UCBs)
c) Customers from Metros and Tier 1 locations

5.2.2. Existing customer segments in urban locations

a) Salary account holders
b) Zero balance savings account holders
c) No-frill account holders
d) Classic/silver & gold debit / credit card holders
e) Select premium customers

The issuers can start issuing the RuPay debit cards to their high-end customers and customers of Tier 1 cities, once these debit cards are loaded with new features network level zero liability, cash back, higher insurance coverage, emergency card replacement program, etc.

5.3. Marketing Strategies

The issuer should have a well-defined marketing strategy to market the new product and ensure competitive positioning in the market

a) **Positioning:** The issuer needs to decide upon the positioning of the RuPay Debit card - "top of the wallet" card. The positioning will largely be determined by the segmentation strategy of the issuer

b) **Branding:** The issuer needs to take all the necessary steps in terms of marketing communication through all means & channels to promote RuPay brand to the customers.

c) **Pricing:** The issuer needs to decide on the annual and renewal fees for this product to its customers and should be based on the positioning as decided by the issuer.

d) **Packaging:** The packaging of the RuPay debit card determines how the card is presented to the customers. The same includes physical design, card cover, usage guides, as well any other marketing communication accompanying the card. The member needs to obtain necessary approval from NPCI for the same at least 45 days prior to the card roll out and pilot launch

e) **Activation:** The issuers must plan to bring as many customers as possible to use their debit cards on POS machines to activate the cards.

f) **Promotion:** The issuer needs to undertake various types of promotional activities, both above-the line (ATL) and below-the-line (BTL) campaigns to reach out to its customers. ATL is a type of advertising through media such as television, cinema, radio, print, and Out-of-home to promote brands or convey a specific offer. This type of communication is conventional in its nature and is considered impersonal to customers. BTL uses unconventional brand-building and promotional strategies, such as direct mail, sales promotions, telemarketing and printed media (for example brochures, and usually involves no motion graphics). It is much more effective than when the target group is very large and difficult to define.

5.4. Issuer Benefits

The issuers can add additional features and services to the existing card features. The additional features can range from services like reward points, cash back at select merchants, reversal of issuance fee post activation and promotional campaigns to incentivize the customers to use the card at POS machines.

5.5. Branch Channel Involvement

The Branch channel plays a critical role in improving the revenue from the Debit Card portfolio of a bank. A better equipped and well informed branch employee can add value to the customer engagement by introducing a customer to the Debit card value proposition. A branch employee can take approximately 2-3 minutes of time during the account opening activity to appraise the customer regarding the use of Debit Card and benefits associated with it. The initial time period of account opening with a bank is a time where the customer attention is highest and thus a lasting impression can be cast in the customers mind.

This section will assist to build awareness amongst your channel staff regarding the Debit Card product and how to effectively communicate the product features to the customer to drive Debit card revenue

5.5.1. Critical Activities

- Engage with the customer at the time of account opening
- Focus on Debit card during account opening
- Emphasize on the benefits of the Debit card

5.5.2. What the Card Product Manager at a bank must do?

- Highlight the key features of the Debit Card in all customer communication
- Train the frontline staff on effective communication of the Debit card features to customers
- Create an “Experience Yourself” campaign for staff to create a firsthand understanding of the product features. A well informed and a convinced staff will communicate effectively to customer.
- Provide reference material to staff for Quick Reference
- Provide tools to branch staff to use as props during customer interaction
- Have a customer follow-up calling to be done to induce memory recall and seek customer feedback if they have already
- Have a FAQ reference sheet handy
- Introduce a Rewards program at an appropriate time to further boost activation and usage of Debit cards

5.6. Continuous Evaluation

Post launching the product, the issuer should track the performance of the product. This would allow the issuer to evaluate the success and the failure or lapses of the product and the same can be identified and resolved at the earliest. The issuers can evaluate the below criteria to track product performance on an ongoing basis. The performance should be reported to NPCI on a quarterly basis as per the parameters mentioned below:

Evaluation Parameter	Criteria	Mandatory/Optional
Number of transactions	• POS transactions • ATM transactions • IVR transaction • Online e-commerce transactions	Mandatory
Volume of transactions (in Rs)	• POS transactions • ATM transactions • IVR transaction • Online e-commerce transactions	Mandatory
Revenue	• Issuance income • Interchange income • Any other income	Optional
Costs	• Systems development • Marketing expenses • Transaction processing • Net fraud losses	Optional
Profitability	• Net revenue less net cost	Optional
Authorization	• Number of transactions authorized • Number of transactions declined • Reasons for declined transactions	Mandatory
Customer service	• Number of queries • Number of complaints • Number of disputes	Mandatory

6. Know Your Debit Card

6.1. Front

<<Insert front Image of XXX Banks Debit Card>>>

a) **Debit card number:** This is the exclusive 16-digit or 19-digit card number. The cardholder needs to quote this number in all communication / correspondence with the issuing Bank

b) **Cardholder name:** Only the cardholder is authorised to use the Debit card issued to the cardholder by the issuing bank. The cardholder needs to check that his/her card has been correctly indent printed

c) **Valid Thru (MM/YY):** The Debit card is valid until the last day of the month of the year indicated on the Debit card.

d) **RuPay logo and hologram:** Any merchant establishment displaying the RuPay logo will accept the Debit card. The hologram is a security feature of the card that helps merchant identify if a card is counterfeit

e) **Electronic usage sign:** This sign indicates that the RuPay Debit card can only be used for online transactions which include card present or card not present transactions. These transactions include electronic point of sale transactions, online IVR transactions and e-commerce transactions with two factor authentication. The Debit card cannot not be used for any offline transactions which include "paper imprint" transactions or mail order transactions

f) **Card Variant:** This indicates if the Debit Card is either a Classic or Gold variant

g) **Domestic/International Debit Card:** This indicates the geographical area(s) of acceptance of the Debit Card. If the sign reads "Domestic Debit/ATM Card" the Debit card can only be used domestically and will not function internationally. Alternatively if the sign reads "International Debit/ATM Card", the Debit card can be used both domestically and internationally.

6.2. Back

<<Insert rear Image of XXX Banks Debit Card>>>

a) **Magnetic strip:** Important information pertaining to the Debit card is encoded on the magnetic strip. The magnetic strip needs to be protected from scratches or exposure to magnets or magnetic fields as it could damage/corrupt the data stored on the magnetic strip. Damaged magnetic strip can result in non-acceptance of the Debit card at merchant establishments.

b) **Signature Panel:** This panel needs to be signed immediately by the cardholder on receipt of the Debit card. The signature should be done with a non-erasable ball point pen (preferably in black permanent ink). The signature has to be identical to the one that will be used to sign the charge slips at merchant outlets. Merchants are required to compare the signature on the charge slip to the one on the back of the card and make sure that it belongs to the cardholder. This requirement helps to minimize fraud and chargebacks.

c) **Customer Service Number:** The card holder can call its issuing Bank at any time on -_____for any queries or should he/she require assistance, including assistance on loss, theft or unauthorised transactions regarding the Debit Card.

d) **Card Verification Data 2 (CVD2):** This is a security feature that protects the card against counterfeit. This number is used by the cardholder to authenticate online card not present transactions which include e-commerce transactions and online IVR transactions.

7. Important Information on Usage of the Debit card

7.1. Activation

A Personal Identification Number (PIN) will be issued to the cardholder separately for using the Debit card at ATMs and/or merchant establishments. In many cases, the Debit card is sent to the cardholder inactive for use at merchant locations. The cardholder should ensure that he/she has received the PIN before trying to activate the Debit card. To activate the Debit card, the cardholder will need to do either of the following:

a) Use the Debit card at an ATM, by entering the PIN.
b) If applicable and offered by the issuing bank, make a PIN verified call to the issuing Bank's Phonebanking/ Customer Service representatives to confirm receipt of the card and PIN. On confirmation the Debit card will be activated.

7.2. Merchant Outlet Transactions

The cardholder should follow the below simple steps while shopping at a merchant establishment.

a) Look for a RuPay sign at the point-of-sale merchant establishment. The merchant must have an electronic point-of-sale card swiping terminal
b) Present the Debit card after making a purchase
c) The Debit card will be swiped by the merchant for authorisation
d) After a successful authorisation, the cardholder account will be subsequently debited for the transacted amount
e) A chargeslip will be generated
f) Check and sign the chargeslip. The signature must match that on the reverse of the Debit card
g) Ensure that the Debit card is returned to the cardholder

As a Savings/Current account holder, the cardholder will be able to purchase items worth up to `.XXXX per day on the Debit card. When using the Debit card at a merchant establishment, the purchase amount will always be debited to the designated Primary account of the Debit card.

7.3. ATM Usage

The cardholder can use the Debit card at any ATM displaying the RuPay logo. This allows the cardholder 24/7 access to the account linked to the Debit card.

Some of the operations that can be performed at ATM's of the Issuing Bank include:

a) Effect a cash withdrawal
b) Obtain a mini account statement for the last 10 transactions
c) View the available account balance
d) Request account statements
e) Transfer funds between accounts
f) Change PIN
g) Request a chequebook

h) Deposit cash/cheque

i) Mobile refill

Please note:

At other bank RuPay ATM (ie. an ATM belonging to a bank other than the issuing bank), the cardholder may only be able to perform limited transactions including cash withdrawal and balance enquiry transactions. Daily ATM cash withdrawal limits will apply. As a Savings/Current accountholder the cardholder can withdraw up to `.XXXXX per day for the Debit Card.

7.3.1. ATM Charges

Every Debit Cardholder is permitted 5 free transactions per month at any other Bank ATMs including Financial as well as Non-Financial transactions. Financial transactions include cash withdrawals while Non-Financial transactions include Balance Inquiry, Pin Change & Mini Statement

If the cardholder exceeds 5 transactions per month at any other banks' ATMs, a charge of INR 20/- (including taxes) per financial transaction and INR. 8.50/- (excluding taxes) per non-financial transaction will be levied on the cardholder

As per RBI guidelines, if there is any failure in the ATM transactions and the cardholder account is wrongly debited, the issuing bank will have to credit such wrongly debited amounts within a period of 7 working days from the date of the complaint. The Bank will pay INR100/- per day beyond 7 working days only if the complaint is lodged within 30 days of the date of the transaction.

8. Important Information on Care of the Debit card

8.1. General Do's & Don'ts for card holders

a) As soon as the cardholder receives the consignment carrying the debit card, he/she should ensure that the card in the envelope has his/her name, and that it is spelt accurately. If there is any error, the same should be informed to the issuing bank immediately

b) Once the debit card is received, the cardholder should immediately sign on the designated signature panel on the reverse of the card. This helps in comparing the cardholder's signature when payments are made at merchant locations such as shops, hotels etc. Unsigned cards may be misused for fraudulent transactions. The cardholder needs to ensure that a valid signature is affixed. For example, "please see ID" is not a valid signature

c) On loss of a debit card, the cardholder should report the same to the issuing bank immediately

d) When disposing off a debit card at the time of renewal/ up gradation/ cancellation, the cardholder should cut it in four pieces diagonally across the magnetic stripe and discard. This will ensure that the card cannot be misused for counterfeit / skimming

e) The Debit card should be kept in a safe place like the wallet or purse, where the cardholder can quickly notice if it is goes missing. It is often too late by the time cardholders realize that the card is missing

f) The cardholder should check his/her card/s periodically to make sure none are missing

g) If the cardholder receives a change of address confirmation and no such request was made, he/she should contact the issuing bank immediately

h) Items with personal information should be kept in a safe place. List of all debit cards, account numbers expiry dates, and the customer service phone numbers should be saved in a secure place so that the cardholder can quickly contact the bank's customer care in case the card/s are lost or stolen

i) The cardholder should inform the issuing bank immediately about any change in his/her mailing address to ensure correct delivery of Card/ PIN in case of subsequent reissue of the debit card

j) The cardholder should not use a replacement card before the Primary card is blocked

k) The cardholder should register/update his/her mobile number with the issuing bank. This will ensure that all transaction alerts are received by the cardholder. This will help in identifying frauds and duplicate transaction as soon as they occur

l) On receipt of the PIN mailer, the cardholder should memorize the PIN and destroy the PIN mailer. The PIN is an important validation of the cardholder's identity. The use of PIN along with card is considered as an authentic signature. The PIN should always be kept a well-guarded secret

m) The Debit card should not be exposed to excessive heat, x-ray or a strong magnetic field. This could cause the magnetic strip data on the Debit card to get corrupted, rendering the card unusable

n) The cardholder should never disclose his/her Debit card PIN to anybody, not even to the Bank's representative

o) In case the cardholder does not recognize a transaction, the same should be reported instantly to the issuing bank

p) The cardholder should not hand-over copies or original documents containing his/her personal data like birth date, PAN number, financials and address proof to any unknown person.

q) The cardholder should never sign a blank application form, that is to be filled in by an agent or a Bank representative at a later time

r) The cardholder should never give a photocopy of the back of the Debit card to anyone for any reason, even if it is an application for a new card

s) The cardholder should never reveal financial or personal information unless he/she has initiated contact. Thieves usually pose as representatives of banks, Internet service providers, and government agencies as a way to get cardholders to divulge personal or financial data that can be used to commit payment card fraud. These types of scams, such as "pretexting" and "phishing," can be perpetrated in person, over the phone, on the Internet, and through e-mail

t) The cardholder should never lend his/her Debit card to anyone and should be well aware of those who have access to his/her cards. If the debit card is borrowed by a family member (spouse, child, parent), with or without the cardholders knowledge, he/she is responsible for their purchase or cash withdrawal

u) The cardholder should never respond to phishing e-mails that falsely claim to be from a bank and ask to disclose personal and bank related confidential details. The Bank will never ask cardholders to send their personal banking details

v) The cardholder should open and respond only to emails that pass some basic tests, such as:-

   i. Is the email from somebody that the cardholder knows?
   ii. Has the cardholder received emails from this sender before?
   iii. Is the cardholder expecting email with an attachment from this sender?
   iv. Does email from this sender with the contents described in the subject line and the name of the attachment make sense?

w) In case the cardholder needs his/her Debit card to be re-issued or terminated, The cardholder needs to send a written request to the address as specified by the issuing bank

8.2. Do's and Don'ts for usage on Point of Sale

a) When the debit card is used for purchases at POS, the cardholder should ensure that it is swiped in the cardholders presence and not swiped on multiple devices

b) The cardholder should ensure that the card number, card-expiry date and the three-digit security code on the back of the card (known as CVD2 number) are not captured in writing anywhere. This can be done if the cardholder ensures the card is swiped in in his/her presence

c) While making point of sale transactions, the cardholder should make sure that the charge slip is complete before signing, it should be totaled correctly

d) The cardholder should ensure that the chargeslip clearly mentions the purchase and cash amount separately, if the transaction conducted was purchase with cash back. The total purchase amount should be the amount including both the purchase and cash amount, while that cash amount should also be displayed separately

e) The cardholder should ensure that for a Cash at POS transaction, the transaction amount and the cash amount are the same

f) The cardholder should ensure that an additional 'Tip' component is displayed on the chargeslip only for transactions that have been conducted at hotels or restaurants. No 'Tips' should be provided at other merchant establishments

g) The cardholder should ensure that he/she conducts any POS transaction in complete privacy, beware of "shoulder surfing." The cardholder should shield his/her PIN from onlookers by using his/her body

h) The cardholder should destroy and dispose of copies of receipts, airline tickets, travel itineraries and anything document that displays his/her card number

i) The cardholder should ensure that the card received from the merchant after a transaction is indeed his/her own, before putting it in the wallet. Cards may get exchanged at crowded merchant locations like service stations and malls or super markets

j) If the card is swiped twice and the same is ascertained at that same very moment, the cardholder should request the merchant to Void one of the transactions and provide him/her with the Void receipt. The slip should be retained by the cardholder until the credit for the duplicate transactions is received. Alternatively if a duplicate transaction is identified by the cardholder at a later time, the cardholder should attempt to get a refund from the respective merchant. If this attempt is not successful then the same should be reported to the issuer bank, who in turn will raise a chargeback with the appropriate reason code

k) Vide RBI Circular DPSS. CO. PD 2224/02.14.003/2010-2011 Dated March 29, 2011, all banks have been advised to put in place a system of online alerts for all types of transactions irrespective of the amount, involving usage of cards at various channels. This measure is expected to encourage further usage of cards at various delivery channels. This was to be

implemented latest by June 30, 2011. In case a cardholder is not receiving alerts for his transactions he should immediately contact the issuing bank to remedy the same.

8.3. Do's and Don'ts for usage at ATM's

a) The cardholder should ensure that he/she conducts any ATM transaction in complete privacy, beware of "shoulder surfing." The cardholder should shield his/her PIN from onlookers by using his/her body

b) If the Debit card is held back by the ATM, the cardholder should inform the concerned call center/Branch personnel immediately

c) Before using an ATM, the cardholder should ensure that there are no strange objects in the insertion panel of the ATM

d) The cardholder should remember to take back the Debit Card after completing the ATM transaction

e) If the cardholder spots any suspicious looking people at or around any ATM, the security guard should be informed immediately

f) The cardholder should change his/her ATM PIN at regular intervals

g) The cardholder should never choose a PIN that is obvious. Birth date, wedding anniversary, phone number, and address pin code are obvious picks. Instead, the cardholder should think of numbers unrelated to major events and addresses in his/her life to create a PIN

h) The cardholder should never disclose his/her Debit Card Number and / or ATM PIN to anyone

i) The cardholder should never hand over the debit card to anyone, even if he/she claims to be a representative of the Bank

j) The cardholder should not get carried away by strangers who try to help him/her use the ATM machine

k) The cardholder should not write the ATM PIN on the card or on a paper/case which is carried along with the card

8.4. Do's and Don'ts for usage on E-Commerce websites

a) The cardholder should preferably transact on sites which mandate validation of CVD2 value (the last 3 digits after the card number, mentioned on the signature panel at the back of the card) or at websites that are certified by RuPay

b) The cardholder should be careful when providing personal information online. He/She should never give out personal or account information to anyone that they do not trust.

c) The cardholder should verify a business's legitimacy by visiting its web site, calling a phone number obtained from a trusted source, and/or checking with a reliable resource

d) The cardholder should keep his/her passwords a secret. Some online stores require the cardholder to register with them via a username and password before buying. Online

passwords should be kept secret from outside parties the same way as how an ATM PIN is protected

e) The cardholder should look for signs of security. Identify security clues such as a lock image at the bottom of the browser, or a URL that begins with https://. These signs indicate that only the cardholder and the merchant can view the payment information and that a site employs' an encryption technology during the transmission of sensitive data

f) The cardholder should keep a record of his/her online transactions. A record of all order confirmations should be saved carefully. If required a printed copy of the same should be retained

g) On completion of an ecommerce transaction, the cardholder should remember to log-off by clicking on the "log-off" option, close the browser and lock the computer if it is left idle

h) In case the cardholder uses his/her Debit Card for online transactions in Internet cafes or public-use computers, the cardholder should erase the history of websites visited/accessed. Also some internet browsers offer to remember usernames and passwords; the cardholder should ensure that when prompted by such browsers, the request is rejected / denied

i) The cardholder should never send payment information via email. Information that travels over the Internet (such as email) is not fully protected from being read by outside parties. Most reputed merchant sites use encryption technologies that will protect cardholder private data from being accessed by others when conducting an online transaction

j) Do not provide any financial/ personal/ Debit Card related information to the unknown internet site or respond to any email seeking such information

k) Avoid accessing Internet banking account on unsecure public computers (e.g. internet cafes)

RuPay Operating Regulations

Version 1.0 – 27 April 2012

Table of Contents

1 Introduction

1.1 Objective of the RuPay Operating Regulations

The RuPay Operating Regulations have been designed to provide a convenient, safe and reliable payment experience while minimizing risk. The RuPay Operating Regulations represent a binding contract between NPCI and all its members associated with the RuPay card scheme. The operating regulations do not constitute a third-party beneficiary contract as to any entity or person, nor do they constitute a contract, promise or representation, or confer any rights, privileges, or claims of any kind as to any third parties.

The RuPay Operating Regulations is a comprehensive document detailing the operating regulations set by NPCI. This manual provides description of the rules and requirements for the RuPay card business. This document attempts to provide operating guidelines that all the participating members must comply with when conducting RuPay card issuing and acquiring business.

1.2 Concerned Parties

The different parties who may find the document relevant include, but are not restricted to:

NPCI: National Payments Corporation of India (NPCI) has been formed to consolidate and integrate the multiple systems with varying service levels into nation-wide uniform and standard business process for all retail payment systems. NPCI facilitates an affordable payment mechanism to benefit the common man across the country and help grow the retail payments in India.

RuPay Scheme: RuPay is a brand of NPCI under which it operates the card scheme and this document is published by NPCI for its RuPay card scheme. RuPay has been conceived to fulfill RBI's vision to offer a domestic, open-loop, multilateral system which will allows various institutions to participate in the electronic payments.

NOTE: The terms NPCI and RuPay have been used interchangeably in this document and refer to the card scheme entity promoted by NPCI. NPCI owns the RuPay card scheme and NPCI is the decision maker with reference to all matters

"Member" means an Acquiring Member, Issuing Member, Acquiring and Issuing Member, Principal Member, Associate Member, and / or Sponsor as the context may require;

"Membership" means Principal Membership or Associate Membership as the context may require;

"Principal Member" means a Member who is granted with a Principal Membership by NPCI for the RuPay Card Scheme;

"Principal Membership" means a membership which is granted by NPCI for the RuPay Card Scheme to the Bank in India or any of its subsidiary or joint venture entity formed by the Bank with other entities;

"Issuing Member" means the Member acting in its capacity as an issuer of Cards to its customers for allowing them to transact with the Merchant and lastly making payment to the Acquiring Member.

"Acquiring Member" means a Member acting in its capacity as an acquirer of payment from the Issuing Member on behalf of the Merchant;

"Acquiring and Issuing Member" means a Member who is acting in its capacity both as an Acquiring Member and an Issuing Member;

"Associate Member" means a Member who is granted with an Associate Membership by NPCI for the RuPay Card Scheme;

"Associate Membership" means a membership which is granted by NPCI for the RuPay Card Scheme to a Member which is a bank or any Person who may or may not be a bank included in the second schedule to the Reserve Bank of India Act, 1934 Bank

"Merchant" means any commercial establishment that accepts monetary transactions made through the RuPay Network;

1.3 Related Publications

Documents referenced in the RuPay Operating regulations have the same authority as the RuPay Operating Regulations. They are binding upon the participants of the RuPay card scheme. The RuPay Operating Regulations govern in case of any contradiction or inconsistency, unless granted a waiver by NPCI. The list of related publications is as mentioned below

1) RuPay Card Marks and Specifications
2) RuPay Dispute Management Rules and Regulations
3) RuPay IIN Maintenance Manual
4) RuPay Global Clearing and Settlement (RGCS) Manual
5) RuPay Settlement Guarantee Document
6) RuPay Working Group Document
7) RuPay Enterprise Risk Management Document
8) RuPay Issuer Implementation Guidebook
9) Member Certification Guidebook
10) RuPay Acquirer Manual
11) Vendor Management Guidebook
12) Third Party Guidelines for Certification and Enrolment
13) Third Party Compliance
14) Member Agreement
15) Sponsorship Agreement
16) RuPay Bylaws
17) RuPay Brand Manual

18) RuPay Product Manual
19) RuPay - PoS Switching Interface Specifications
20) RuPay - RGCS Technical and Message Specifications

The above publications can be found in NPCI Online.

1.4 Confidentiality of this Document

This document is for restricted use, copy and distribution. No part of this document may be reproduced, modified and copied in any form by any means without prior written authorization of NPCI.

1.5 Organization of this document

Chapter Name	Description
RuPay Operating Regulations – Governance	The chapter outlines the manner in which participants of the RuPay card scheme are required to use the operating regulations; the extensions to the operating regulations; the rules governing the confidentiality of NPCI publications; Governance principles for certification and compliance; Operating regulations compliance, enforcement and right of termination of merchant or agents and other general requirements.
RuPay Card Scheme Membership	This chapter describes various types of RuPay card scheme membership, procedure for obtaining and terminating a membership, sponsorship requirements, compliance and certification requirements, liabilities of these members and guidelines for third party processors and vendor management.
The RuPay Brand	This chapter describes how RuPay Brand is to be positioned and provides guidelines on the use of RuPay marks, restrictions on use of marks, presence of other marks, use of marks for promotions, rules to be complied with by members for usage of NPCI brand and marks and the compliance required with these rules.
RuPay Product & Services	This chapter contains guidelines and information for any member participating in the NPCI scheme as an issuer. It outlines the requirements, issuance procedures and other service standards to be followed by an issuing member.
RuPay Card Acceptance	This chapter specifies the requirements applying to an acquirer in on-boarding, training and risk control of merchants. The chapter also outlines the regulations related to terminals, transaction processing and receipts.
RuPay Transaction Processing	This chapter explains the rules and regulations defined by NPCI for its participants to authorize, clear, and settle transactions in NPCInet. Further, NPCI has defined responsibility of acquirers and issuer with respect to transaction processing.
RuPay Risk Management	This chapter outlines security requirements and guidelines and specifies responsibilities for NPCI members regarding fraud, risk management

Chapter Name	Description
	and security of the NPCI system
RuPay Dispute Management	This chapter outline the dispute cycle that each member can resort to for resolution of transaction/cardholder disputes. The rights and limitations for each of the members are clearly defined.
RuPay Pricing, Fees and Interchange	This section contains guidelines and information for issuing or acquiring member participating in the NPCI scheme. It outlines the requirements, procedures and other service standards to be followed by a member for pricing, fees and interchange setup for RuPay brand products.

1.6 Contact for Feedback

Members may forward comments, suggestions, or questions to RuPay in regard to the RuPay Operating Regulations via e-mail to rupay@npci.org.in

2 RuPay Operating Regulations - Governance

2.1 Introduction

The chapter outlines the manner in which participants of the RuPay card scheme are required to use the operating regulations; the extensions to the operating regulations; the rules governing the confidentiality of NPCI publications; Operating regulations compliance, enforcement and right of termination of merchant or agents and other general requirements.

2.2 Key Principles

1) NPCI defines the RuPay Operating Regulations and RuPay Bylaws to support the use of NPCI products and services and to protect NPCI systems and the RuPay brand. Depending on technological developments, feedback received, market trends and opportunities available the RuPay Operating Regulations and RuPay Bylaws are amended, modified, deleted or otherwise changed by NPCI from time to time.
2) Members/Vendors of the RuPay card scheme are bound by the rules and regulations set in the RuPay Operating Regulations and all the documents referred to in this manual. Members may refer to 'Related Publications' section in the introduction for a complete list of publications.
3) NPCI has set up the RuPay compliance committee, to ensure constant monitoring and governance to ensure that the rules and regulations set up by NPCI are complied with by all members, vendors and associated entities. The monitoring is done for but not limited to product, brand and technical requirements, merchant acceptance procedures, and industry-wide standards.
4) In the event of any conflict between the RuPay Operating Regulations and any applicable Indian laws or regulations, the requirements of such law or regulation will preside over the operating regulations.
5) NPCI may grant variances or temporary waivers of the operating regulations under certain unique, emergency circumstances as described in the Section 'Variances to RuPay Operating or Dispute guidelines.'

2.3 Use of RuPay Bylaws and RuPay Operating Regulations

Members of the RuPay card scheme are expected to adhere to the RuPay Bylaws and Operating Regulations set by NPCI. The RuPay Bylaws specify the standards that members must comply with, unless NPCI specifically grants a waiver. The RuPay Bylaws document is a comprehensive document containing the articles laid down by NPCI for its members. The document contains rules regarding the following aspects:

1) Offices and Governance
2) Membership
3) Fees
4) Indemnification
5) Relations between the members within the scheme
6) Relations between the members of the scheme and cardholders
7) Relations between the members of the scheme and the merchants
8) Security
9) Violation of RuPay Bylaws

10) Documents & Audits

For further details on each of the above topics, members must refer the RuPay Bylaws.

Compliance with RuPay Operating Regulations
As specified in the RuPay Member Agreement between the members and NPCI (i.e., the Application for Membership), every member must comply with the rules and regulations laid down by NPCI in the RuPay Bylaws and RuPay Operating Regulations and all its publications.

2.4 Confidentiality of NPCI Publications

The RuPay Operating Regulations must be used only for the purpose of compliance to the RuPay card scheme or for review. Members of the RuPay card scheme are expected to treat the information provided by NPCI with confidentiality with at least the degree of care with which a member treats its own confidential and proprietary information and also ensure that the regulations regarding the confidentiality of the materials are strictly adhered with.

11) The members shall not publish, disclose, or distribute to any person or organization any confidential or proprietary matters of NPCI, including, but not limited to, documents, ideas, products and data without prior written consent of NPCI. The member shall disclose confidential or proprietary knowledge of NPCI only under specific Non-Disclosure Agreements.
12) NPCI shall not publish, disclose, convey or distribute to any person or organization any confidential or proprietary matters of any member, including, but not limited to, documents, ideas, products and data, without prior written consent of that member, unless, with respect to data, the data are aggregated or presented so as to not disclose the data of any specific member.

2.5 Changes to the RuPay Operating Regulations

The RuPay Operating Regulations are updated regularly. All concerned parties are responsible for obtaining and referring to the most current version and content of the RuPay Operating Regulations at all times.

NPCI will communicate the changes that have been approved but are yet not incorporated in the RuPay Operating Regulations through member letters. These communications have the same authority as the RuPay Operating Regulations. Unless an effective date is specified in the release all changes are effective on the Member letter date.

2.6 Operating Regulations for Compliance and Enforcement

The Member Certification Guidebook provides an indicative list of the formation and role of the compliance committee, the types of compliance that must be adhered to by the members, the penalties in case of non-compliance, and the waivers and appeals.
Members of the RuPay card scheme are expected to comply with the rules set by NPCI.

2.6.1 NPCI's Right to Monitor, Audit, Inspect, or Investigate

Each member, agent, vendor and third party entity undertakes to accept an audit and an inspection either by NPCI itself or by an appointed agent. This audit or inspection could be conducted by NPCI either with prior notice or as a surprise checks if there is a requirement.

2.6.2 Compliance Committee

The RuPay Compliance Committee is a monitoring body which governs the adherence of the rules and regulations outlined in this manual. The committee comprises of members from NPCI as well as from the core member banks. For details regarding the formation and role of the compliance committee, members may refer the RuPay Working Group Document and Member Certification Guidebook.

2.6.3 Types of Compliances

Members of the RuPay card scheme need to adhere to the compliance requirements and maintain the integrity of the NPCI payment system. The compliances, not limited to the following, are brand compliance, certification compliance, merchant management, third party compliance and vendor compliance. Please refer the Member Certification Guidebook and Third Party Guidelines (Compliance) for further details.

2.6.4 Assessing Violations

The members need to be compliant with the guidelines and the certifications at all times as mentioned in the respective documents. NPCI can audit the members at any time for compliance to ensure adherence to the compliance guidelines on various areas laid down by NPCI. NPCI or any organization designated by NPCI may audit the system, records and procedures or facilities of the issuer, acquirers (or TPPs) at any given point of time. The compliance checks may be done once a year or more frequently if required which would cover various areas and in case of non-compliance the associated penalties will be levied as mentioned below.

2.6.4.1 Determination of Violation

NPCI may determine a violation of the RuPay Operating Regulations on the following basis:

1) NPCI will determine whether the violation to the rules and regulations set by NPCI has occurred based on the response it receives to an investigation or any other information it deems fit
2) The member's failure to respond to a notification of investigation and to provide all information requested before the specified date in the notification, may result in a determination that a violation has occurred

2.6.4.2 Notification of Determination

After careful scrutiny, NPCI will determine whether violation(s) have occurred and are continuing. In such a case NPCI will specify a date by which the member must correct the violation(s). If violation(s) are determined to have occurred, the notification will advise the member of the:

1) Details of the violation(s)
2) Fines assessed
3) Date by which a member must correct the violation(s)

4) Right to appeal the determination that a violation has occurred and the fines assessed for such violation

2.6.4.3 Penalty Assessment

If NPCI imposes a penalty on a member, it is the duty of the member, to pay the penalty as per the requirements set by NPCI. A member, under any circumstance, must not represent to its customer that NPCI has imposed the penalty on the customer. If required, NPCI may recover the penalty in the daily settlement of the violating member via a fee collection message. The RuPay compliance committee will be responsible for determining the penalty to be charged to the violating member.

2.6.4.4 Notification Response

A member must respond to and provide all information requested by NPCI for a violation that is under investigation. The member must submit its response and information, within the time period specified, and by the mode specified by NPCI. The notification response is effective when posted, sent, or transmitted by NPCI to the member or its agent.

2.6.5 Fines and Penalties for Violations

2.6.5.1 NPCI Right to levy Penalties

NPCI has the authority to levy penalties on members defaulting on compliance of NPCI published RuPay Operating Regulations, RuPay Bylaws or any of the referred publications.

2.6.5.2 Penalties for General Violations

The RuPay compliance committee will determine the fines and penalties to be charged to member banks for violations of any requirement stated in this manual or any of the referred publications.

2.6.5.3 Certification Compliance Related Penalties

A member that fails to comply with the certification compliance will be assessed by the RuPay compliance committee and appropriate penalties will be imposed on the member or the third party entity by the committee.

2.6.5.4 Brand Compliance Related Penalties

A member that fails to comply with the brand compliance will be assessed by the RuPay compliance committee and appropriate penalties will be imposed on the member or the third party entity by the committee

2.6.5.5 Merchant Management and Third Party Compliance Related Penalties

Any entity that fails to comply with the Merchant & Third Party Compliance will be assessed by the RuPay compliance committee and appropriate penalties will be imposed on NPCI members or the third party entity by the committee. The penalty would be levied on the acquirer / issuer and the same may be passed on to the TPP/TSP by the acquirer/ issuer. NPCI would have the authority to revoke / cancel the licence of third party and deny access to the network either with prior intimation or without prior intimation depending on the gravity of the non compliance observed, and as deemed by the compliance committee.

2.6.5.6 Physical Security Validation Requirements for Card Vendors

The physical security validation compliance mentioned in the Vendor Management Guidebook specifies the physical security requirements and procedures that the card vendors must follow before, during and after card manufacturing, magnetic stripe code encoding, embossing, card personalizing, chip embedding, card storing, and card shipping and mailing.

A member that fails to comply with the RuPay physical security validation compliance will be assessed by the RuPay compliance committee and appropriate penalties will be imposed on the member or the third party entity by the committee.

2.6.5.7 Waivers & Appeals

Any member can appeal against a fine or penalty to the RuPay compliance committee in writing. The member needs to clearly document the reason for requesting a waiver along with all the supporting documents. This appeal should be filed within 30 calendar days post receiving the penalty notice.

Waiver Approval	Approval authority for waiver
Penalty amount - Less than or equal to Rs. 20 lakhs	Compliance committee (headed by chairman)
Penalty amount - More than Rs. 20 lakhs	NPCI Board (with recommendation from chairman of compliance committee)

The RuPay compliance committee, headed by the chairman of the committee, can review the appeal and take a decision on the waiver. The decision to grant waiver will be taken by the committee which needs to be in a quorum. The waiver can be granted to the member only if there is an agreement within the committee by a way of simple majority through voting.

In case the RuPay compliance committee is unable to reach a conclusive decision on the waiver and the votes are split equally without a conclusion, then the chairman has the veto power to take the final decision.

In case of termination of the member due to repeated non-compliance, the member can appeal to the RuPay compliance committee to review their case along with all the supporting documents. The committee will hear the case and based on the facts thereafter make their recommendation. The committee can only recommend for the repeal of the suspension of the member. The decision to reinstate the member will fully lie with NPCI Board.

The decision of the NPCI Board / compliance committee is binding on the member and the members would not have legal recourse in this regard.

2.7 Right of Termination of Merchants or Agents

An acquirer is responsible for ensuring that the merchants comply with the rules and regulations set by NPCI. In case the merchant defaults, NPCI can penalize the acquirer. Acquirers must therefore ensure that they regularly audit the merchants. For details, acquirers must refer the RuPay Acquirer Manual
NPCI may permanently prohibit a merchant, Internet Payment Service Provider (IPSP), or any other entity from participating in the RuPay card scheme for any reasons it deems appropriate, such as:

1) Entering into a merchant agreement under a new name with the intent to circumvent the provisions of the RuPay Operating Regulations
2) Is involved in fraudulent activity
3) Activity that causes the Acquirer to repeatedly violate the RuPay Operating Regulations
4) Any other activity that may result in undue economic hardship or damage to the goodwill of the RuPay card scheme
5) If the merchant is involved in any illegal activity under Indian law
6) If the merchant is involved in any money laundering
7) If the merchant poses a threat to the RuPay brand
8) If the merchant is responsible for a situation which could result in a loss to NPCI or brings the RuPay brand to disrepute
9) Any other reason NPCI deems appropriate

Once a merchant or agent is prohibited by NPCI from participating in the RuPay scheme, every acquirer should terminate its relationship with the merchant

Revocation of Merchant Privileges
If NPCI finds a merchant or agent has violated the rules and regulations set by NPCI, NPCI has the right to revoke merchant privileges. NPCI may fine an acquirer that enters into an agreement with any merchant that NPCI has prohibited from participating in the RuPay scheme.

2.8 Variances to RuPay Operating Regulations or Dispute Guidelines

RuPay management committee may request, amend or revoke variances to the RuPay Operating Regulations or Dispute Guidelines based on business requirements, and or on member banks request.The variances will be officially communicated to all affected members via Member Letter/s.

2.8.1 Variance attempt requests

Request for variance must be submitted to the RuPay management committee for approval.
In case of emergency variance RuPay management committee may take decision without member's request.

2.8.2 Types of Variance requests

RuPay management committee may grant variance or temporary waiver to the RuPay Operating Regulations or Dispute Guidelines to a particular member based on their request or to members of a

particular region. The emergency variance can be given to specific location, member or group of members in the event of natural disaster.

2.8.3 Emergency Variances

RuPay management committee may grant an emergency variance to a member, group of members or members of a particular region if the RuPay member cannot abide by due to conditions beyond its control. The Emergency variances includes situations such as

1) Natural calamities
2) Act of war
3) Government restrictions
4) Political turbulence
5) Breakdown of public infrastructure

2.8.4 Time limit for Emergency Variances

NPCI will communicate timelines to member bank on case to case basis.

3 RuPay Scheme Membership

NPCI is a section 25 company having its own equity members and has been formed with the below mission:
"To build state-of-the-art world class customer friendly electronic retail payments system available & affordable to all, round the clock".

RuPay is a brand of NPCI under which it operates the card scheme.

3.1 Introduction

This Chapter describes various types of RuPay card scheme membership, procedure for obtaining and terminating a membership, sponsorship requirements, compliance and certification requirements, liabilities of these members. RuPay Bylaws and Member Agreement documents provide further details (including member rights and obligations) for the card scheme members.

3.2 Key Principles

1) Entities that wish to obtain a NPCI membership should meet the guidelines specified in RuPay Bylaws and RuPay Operating Regulations
2) NPCI members include financial institutions that issue RuPay cards to consumers or enrol merchants to accept RuPay cards and third party entities that directly interact with NPCI systems to process transactions
3) NPCI members should accept full responsibility for issuance of card scheme products, acquiring of merchants, settlement of transactions, compliance with RuPay Bylaws, Member Agreement, RuPay Operating Regulations and other compliance documents listed in this document along with external legal/regulatory requirements. Members need to adhere to the compliance requirements and pay associated penalties as defined in Member Certification Guidebook

3.3 General Membership Guidelines

Registration

The RuPay card scheme membership is available to all entities that satisfy the eligible criteria laid down in the RuPay Bylaws. The membership is exclusive and no entity can have more than one membership at any given point of time.

The application for RuPay card scheme membership shall be made to NPCI in the specific format mentioned in Member Agreement and NPCI will evaluate and accept or reject these applications. NPCI reserves the sole right to refuse membership to any applicant without providing the reason / explanation for the same.

The member should be able to perform the functions and obligations required of specific membership (as specified in the RuPay Bylaws Annexure) and should pay the applicable fees to join RuPay card scheme, fees related to issuing, acquiring and processing RuPay cards, fees and charges for towards settlement and

settlement guarantee fund and all fees that may be levied by NPCI from time to time. The details about member pricing is mentioned in the RuPay Product Manual.

Member Agreement

The entities interested in a RuPay card scheme membership should enter into an agreement as specified in Member Agreement. Detailed rules and information related to RuPay card scheme membership are specified in the new member enrolment documents which are listed below:

a) RuPay Membership Agreement
b) RuPay Sponsorship Agreement

The membership shall begin only from the date the applicant is accepted for membership by NPCI. The members will be bound by rules and guidelines as defined in the RuPay Operating Regulations and RuPay Bylaws.

Classes of Membership

There will be two classes of RuPay card scheme membership - Principal membership,and Associate membership as detailed below:

Principal Membership

"Principal Membership" means a membership which is granted by NPCI for the RuPay Card Scheme to the Bank in India or any of its subsidiary or joint venture entity formed by the Bank with other entities;

A Principal member shall have the following rights:

a) Have direct relationship with the card holders of the bank having the marks of RuPay and/or with the merchants to honour these cards having the marks of RuPay
b) Provide authorization services unless exempted by NPCI
c) Provide credit to and collect outstanding money from the cardholders and pay to the acquirers
d) Notify NPCI atleast 90 (Ninety) days in advance of its intention to modify or terminate the RuPay Sponsorship Agreement;
e) Immediately notify NPCI in writing of any termination or material modification of the Service Agreement.

Associate Membership

"Associate Membership" means a membership which is granted by NPCI for the RuPay Card Scheme to a Member which is a bank or any Person who may or may not be a bank included in the second schedule to the Reserve Bank of India Act, 1934Bank;

The Associate membership shall be granted to any bank or non-bank having a sponsorship agreement with any of the Principal members. The Associate will have similar rights as that of a Principal member. The Associate member:

a) Has to be sponsored by a Principal member and a written agreement needs to be drafted for the sponsorship between the two entities

Eligibility

Principal Membership

The membership is exclusive and no entity can have more than one membership at any given point of time. The application for RuPay card scheme membership shall be made to NPCI and NPCI will evaluate and accept or reject these applications. NPCI reserves the sole right to refuse membership to any applicant without providing the reason / explanation for the same.

The membership would have associated functions and obligations and should pay the applicable fees to join RuPay card scheme, fees related to issuing, acquiring and processing RuPay cards, fees and charges towards settlement and settlement guarantee fund and all other fees that may be levied by NPCI from time to time. The details about member pricing, fees and charges is detailed in the RuPay Product Manual.

The eligibility criterion for a Principal Membership is as follows:

a) A Person shall be a Scheduled Bank;
b) A Person shall have a valid banking license from RBI to carry on the banking business;
c) A Person shall have an RBI Settlement Account;
d) The Person shall have a current account with RBI; and
e) The Person shall be registered with RBI as an RTGS member.

Besides the above, NPCI would require the member banks to adhere to other technical, operational and governance criteria as defined from time to time.

Associate Membership

The Associate membership shall be granted to any bank or non-bank having a sponsorship agreement with any of the Principal members. The Associate will have similar rights as that of a Principal member. The Associate member has to be sponsored by a Principal member and a written agreement needs to be drafted for the sponsorship between the two entities. The Associate and Participant applicant who require a sponsorship for participation in the scheme must send the RuPay Sponsorship Agreement duly signed by the authorized official of the sponsor member and the sponsored member. The sponsor member should notify NPCI 90 days in advance in case of change or termination of the sponsorship agreement.
The sponsor member should comply with the RuPay Sponsorship Agreement and

a) Accept full and complete responsibility for the proper performance by the sponsored member of all requirements of the rules & guidelines as may be in force from time to time
b) Immediately notify NPCI in writing of any termination or material modification of its service agreement with the sponsored member
c) Promptly pay the fees and charges associated with the sponsored member to NPCI as required
d) Ensure the sponsored member is compliant with all the guidelines and regulations of NPCI and the violation of any such compliances will lead to penalties and thereafter termination of membership

Sponsorship requirements

The Associate applicant who require a sponsorship for participation in the scheme must send the RuPay Sponsorship Agreement duly signed by the authorized official of the sponsor member and the sponsored member. The sponsor member should notify NPCI 90 days in advance in case of change or termination of the sponsorship agreement.
The sponsor member should comply with the RuPay Sponsorship Agreement and

a) Accept full and complete responsibility for the proper performance by the sponsored member of all requirements of the rules & guidelines as may be in force from time to time
b) Immediately notify NPCI in writing of any termination or material modification of its service agreement with the sponsored member
c) Promptly pay the fees and charges associated with the sponsored member to NPCI as required
d) Ensure the sponsored member is compliant with all the guidelines and regulations of NPCI and the violation of any such compliances will lead to penalties and thereafter termination of membership

Change of Membership type

In case of change of membership type, the member needs to send a written notice thereof notifying about the change 90 days prior to the change to NPCI management committee. The member shall not assume a new membership role unless it has received NPCI's prior written approval.

Transferability of Membership

The membership of RuPay Card Scheme is not transferable or assignable by the Member, whether by sale, consolidation, merger or otherwise without the express written Consent of NPCI.

Provided however, if a Member intends to transfer or assign its membership with NPCI RuPay Card Scheme, such a Member must send such a request in writing to NPCI requesting for transfer of membership. Upon receipt of such request, NPCI will review the same and notify the requesting Member accordingly.

In the event of a consolidation, amalgamation or merger of two or more Members that results in the liquidation of any Member or Members, the surviving Member shall continue to be a Member with all the rights, liabilities, duties and obligations of such dissolving Member's Membership.

Provided however that the surviving Member shall be eligible to be a Member of NPCI Card Scheme and perform the functions and obligations required by Members of the same class as that of the dissolving Member.

In case the member does not want to continue the Membership, then the said Membership needs to be terminated in accordance with the termination provisions provided hereunder.

Compliance

The members are required to provide such information and certification as requested by NPCI from time to time which includes adherence to compliance of the RuPay Bylaws, operating environment, business numbers and the compliance guidelines specified in NPCI compliance documents listed below:

a) Member Certification Guidebook
b) RuPay Acquirer Manual
c) Third Party Compliance
d) Member Service-Level Agreement
e) RuPay Brand Manual

NPCI shall have the right to require any member to produce such written evidence as it deems necessary to determine compliance with these guidelines. Every issuing member should also be bound to the requirements specified in RuPay Card Marks and Specifications.

Member Certification

The applicant banks, both the issuers and the acquirers need to certify themselves in order to start the operations as a NPCI member. These certifications can be related to PCIDSS, online authorization specifications, RuPay Global clearing and Settlement System (RGCS) certification, EDC/POS machine certification, , and any other certification as decided by NPCI from time to time. The applicant banks will be confirmed as full time members of NPCI only post completion of all the required certifications as required by NPCI. The details of the required certifications are specified in Member Certification Guidebook

3.4 Third Party Guidelines

Third Parties are defined as an entity who is engaged to provide RuPay related services directly or indirectly to a Member bank. The third parties are of 2 types:

Third Party Processors (TPP): TPP are defined as Third Party entities operating under the marks of NPCI for Principal / Associate members who either through the way of processing or clearing and settlement and/or by any other way directly interact with NPCI systems and switch.
A Data Storage Entity is engaged in the processing, transmission, or storage of card account data, transaction data, or both.
A Third Party Processor is an independent entity that is contracted by a member to conduct some part of the transaction processing process. The third parties may provide authorization, clearing & settlement, or any other payment related processing services for merchants or member banks

Third Party Service Providers (TSP): TSP are Third Party entities that do not touch the switch of RuPay but provide other services like data storage, data transmission, processing cardholder data. The various types of TSPs are Independent Sales Organizations, personalization and dispatch bureaus, cardholder solicitation

Third Party registration

The Third Party must inform NPCI of its interest in order to initiate the enrolment process. The Third Parties interested in a RuPay card scheme membership should enter into an agreement as specified in Third Party Compliance document. Detailed rules and information related to RuPay card scheme membership are specified in the new member enrolment documents which are listed below:

A Third Party should also submit for evaluation a letter of recommendation from the sponsor, copy of their most recent audited financial statements (previous three years), previous experience details and a brief history of the organization and promoters profiles. The procedure for enrolment of Third party processors is detailed in Third Party Enrolment and Certification document.

A Third Party must apply to be registered and get empanelled by NPCI before commencing its services.. The Third Parties can start their operations only post completing the necessary registrations and certifications with NPCI.

NPCI will not disclose any confidential information furnished to it by a member or the Third Party, except to the same Member or Third Party supplying the information, or as part of a general statistical compilation that does not reveal individual Member or the Third Party data, or as may be required by any court process or governmental agency having or asserting jurisdiction over NPCI.

Third Party agreement

A member and its Third Party must enter into a written agreement describing the services that the Third Party is to provide. The Third Party agreement must be updated from time to time as appropriate to reflect the services that the Third Party provides and may not contradict, or be inconsistent with the guidelines.
The member should have an agreement in writing with all new Third Parties.

The agreement must capture the member's responsibility, operating policies and must not include any clause that limits or attempts to limit the Principal or Associate member's responsibility or shift the responsibility to the Third Party for all the action / activities related to RuPay card scheme operations.

On the effective date of the termination or expiration of the agreement(s), or upon notice by NPCI or upon expiration or de-registration of the Third Party, the Third Party must immediately cease all use of NPCI marks and systems. The member is responsible to ensure that the Third Party ceases to use the marks of NPCI and surrenders all NPCI related materials and associated information to the member or NPCI failing which the member shall be held responsible and all procedures legal and non legal shall be directed towards the member, depending upon the severity of misuse of marks and system.

The member must verify if the Third Party has an existing business and business model, has required controls, both financial and operational, to conduct the business on an ongoing basis and complies with all the applicable laws before signing up the Third Party. The list of checks the member must undertake to verify the Third Party credentials is specified in section 'Pre-requisites while entering into an agreement with the participant' of Third Party Compliance.

Checks and Controls

1) The Principal and Associate member are entirely responsible and must themselves manage and direct all aspects of services performed by the Third Party member and establish and enforce all management and operating policies applicable in accordance with the guidelines.
2) A member needs to check with NPCI in writing if the selected Third Party has been registered and certified by NPCI before getting into any arrangement with the Third Party. NPCI will send a written confirmation to the member regarding the completion of registration and certification of the Third Party.
3) In case the Third Party is not registered and empanelled, then the member has to ensure that the Third Party is empanelled with NPCI as a Third Party before getting into any agreement / arrangement.
4) A member must not transfer or assign any part or all of such responsibilities or in any way limit its responsibility with regard to its Third Parties.
5) A member must conduct meaningful monitoring to ensure ongoing compliance by the Third Party with the guidelines.
6) In case of any deviations, then the same needs to be reported to NPCI and the member must ensure the Third Party undertakes corrective actions to resolve the deviations.

Use of marks

A Third Party must not use any NPCI or related marks on its own behalf. The Third Party may not suggest or in any manner create an impression that the Third Party is a Principal or Associate member of NPCI.

Transfer of rights

A Third Party must not subcontract, sublicense, assign, license, franchise, or in any other manner extend or transfer to any third party any rights or obligation the Third Party may have in connection with providing the service to a member. Any such transfer is not permitted by NPCI to process RuPay card transactions.

Confidentiality

A Third Party must comply with the confidentiality rules specified in Third Party Compliance Guidelines.

Data Security

A Third Party must comply with all standards and regulations pertaining to the storage and/or safeguarding and/or transmission of account and customer data. The Third Party must ensure their systems are secure against any frauds or network attacks or any such security related risks. If a Third Party believes that there has been an unauthorized access to cardholder's data, then the Third Party should immediately inform the member and the member should submit a report on the same to NPCI. The member should give details on the lapse and the remedial action plan to counter it.

Adherence to Service Level Agreements

Third party entities must comply with the service level rules specified in Third Party Service-Level document.

Adherence to Third Party Compliance

Third party entities must comply with the guidelines for access to NPCI system and software, and also the components and the data environment that interfaces with NPCI switch and systems as specified in Third Party Compliance Guidelines.

Indemnification

The Third Party must indemnify under any and all circumstances, and hold harmless National Payments Corporation of India and each of the directors, officers, employees and agents of NPCI from any actual or threatened claim, demand, obligation, loss, cost, liability and/or expense(including, without limitation, actual attorneys' fees, costs of investigation, and disbursements) resulting from and/or arising in connection with, any act or omission of the indemnifying member, its subsidiaries, or any person associated with the indemnifying member or its subsidiaries.

Audits

NPCI or any designated agency appointed by NPCI may conduct one or more regular or periodic financial and procedural audits of the Member and its Third Party or both, at any time and from time to time for the purpose of determining compliance with the guidelines and rules. The Third Party bears all costs of any such audit or audits. The Member and its Third Party each must fully cooperate with and promptly supply NPCI with all information and material upon request. Such audits can be conducted by NPCI either with prior notice or as surprise checks if there is a requirement.

Penalties

A Third Party that fails to comply with the Merchant Management and Third Party Compliance will be assessed by the RuPay compliance committee and appropriate penalties will be imposed on the NPCI member. Descriptions of these penalties are specified in Member Certification Guidebook

3.5 Termination of Membership

The Membership of a Member shall stand terminated and except as otherwise provided herein, all the rights and obligations between the Parties shall stand cancelled and revoked on the happening of any of the following events namely:-

a) termination of a Member's Membership by NPCI without any reason whatsoever by NPCI serving a prior written notice, as NPCI may deem fit, to the Member clearly stating the termination of that Member;

b) any Member serving a written notice to NPCI at least 180 days prior to the date from which its Membership needs to be terminated by providing reasons for termination as well as a declaration for making all payments due and payable by the Member to NPCI and that such termination has been approved by NPCI[1];

[1] DG Comment: Member cannot terminate unless the same is accepted by NPCI.

c) any Member becoming or is likely to become Insolvent[2];
d) any Member not issuing or accepting Cards for more than 2 (two) years;
e) a Sponsor withdrawing its sponsorship of an Associate Member;
f) Directions issued by any regulatory authority against the Member.

G. Consequences of Termination

a) The Member shall, from the date of termination, cease to issue Cards in its own name or appear on such Cards or elsewhere as the owner or issuer thereof;
b) The Member may re-issue cards to its customers on a network other than the RuPay Network by replacing the Cards issued to them;
c) The Member shall return to NPCI all media, Documentation and other materials including those pertaining to the RuPay mark and Confidential Information and certify in writing to NPCI that they have been destroyed as directed. The Member shall also cause all software related material to be erased from the Members Computer and shall certify to NPCI that the same has been done;
d) The Member shall make all payments accrued but not paid until the date on which such event of termination occurs and also make all such payments which would have been required to be paid, if no event of termination would have occurred on the date of termination;
e) The Member will not be eligible for any refund of any excess Fee(s) lying with NPCI after adjusting the amounts payable by the Member to NPCI;
f) The Member must issue necessary directions / notifications to the Card Holders, Merchants, Vendors, Associate and Participant Members who were sponsored by it of such termination at least [30] days prior to the date of termination and the Member shall not enter into a direct contractual relationship with any Person for the issuance of Cards from such date;
g) The Member must refrain from misrepresenting to any Persons that it continues to be a Member of NPCI RuPay Card Scheme and must indemnify and keep indemnified, NPCI of, from and against any loss or damage caused to it as a result of such misrepresentation;
h) The Member must fulfill all its obligations pertaining to each transaction executed through it and this provision shall survive the termination of its Membership with NPCI.

Provided however, any obligation of the Member arising out of or in connection with any transactions executed on the RuPay Network and which shall accrue prior to the date of termination but not concluded on or before the date of termination, such Member shall conclude such transactions and perform its

[2] DG Comment: Please refer to the definition of the term Insolvent as the same is very exhaustive.

obligations in accordance with the provisions contained in the Transaction Documents as though the same were consummated prior to the termination of its Membership with NPCI.

A terminated member shall maintain confidentiality of RuPay information as specified in Clause G below. The terminated member should indemnify RuPay from any falsely projected image of RuPay and can be penalized for projecting association with RuPay in spite of the termination.

Wind Down: NPCI may, during the Wind Down Period, permit an outgoing Member and its existing Card Holders to transact on the RuPay Network. For this purpose, the outgoing Member shall furnish such security as may be acceptable to NPCI to secure its obligations for the transactions which have been executed on the RuPay Network during the Wind Down Period. All those transactions which have been executed during the Wind Down Period shall continue to be governed by the applicable Transaction Documents and that the outgoing Member shall be bound by the provisions contained in such Transaction Documents.

Provided however, NPCI reserves its right to reject all or any transactions executed by the existing Card Holders of the outgoing Member on the RuPay Network during the Wind Down Period.

This provision shall not apply to any Member who is becoming or is likely to become Insolvent.

3.6 Liabilities and Indemnifications

NPCI members shall accept full responsibility for issuance of NPCI products, acquiring of merchants, settlement of transactions, compliance with RuPay Bylaws, Member Agreement, RuPay Operating Regulations, RuPay Acquirer Manual and Member Certification Guidebook and external legal/regulatory requirements. Members indemnify NPCI against all claims that arise out of their activities.

3.6.1 General Guidelines

Indemnification

Every Member shall indemnify and keep indemnified, NPCI of, from and against:

a. any loss or damage that it may suffer as a result of a breach by the Member of any of the provisions contained in any of the Transaction Documents or under any law for the time being in force;
b. any demand, claim, action, proceeding or any action which may be made or likely to be made or maintained against NPCI on account of the Member not having complied with any of the provisions contained in any of the Transaction Documents;

c. all prosecutions, claims, costs, charges and expenses with regards to any action or prosecution that may be initiated by or against NPCI in connection with the Member's membership with NPCI;

d. any waiver, forbearance or indulgence granted by the Member shall not affect the liabilities of the Member under any of the Transaction Documents and this indemnity shall bind the Member and its respective representatives, executors, successors and assigns and shall not be determined or affected by the incapacity of the Member;

e. any loss or damage that it may suffer as a result of a breach by a Third Party of any of the provisions contained in any of the Transaction Documents or under any law for the time being in force.

Every Member who is a Sponsor must accept full and complete responsibility for compliance by an Associate Member of all rules and regulations contained in the Transaction Documents formulated by NPCI for the RuPay Card Scheme marketed under the brand 'RuPay' and all other Intellectual Property Rights of NPCI and must indemnify and keep indemnified, NPCI as provided in Rule 6(a) to Rule 6(d) of the By-laws

Liabilities

Notwithstanding anything to the contrary the Member's aggregate liability in connection with obligations undertaken as a part of the card scheme regardless of the form or nature of the action giving rise to such liability (whether in contract or otherwise), shall be at actual and limited to the total value of all fees / charges / amounts due to NPCI and the transaction value that is being processed / cleared by the Member

The Member's liability in case of claims against NPCI resulting from gross misconduct or gross negligence of the Member or its employees, contractors, consortium members, and subcontractors or from infringement of patents, trademarks, copyrights or such other Intellectual Property Rights or breach of confidentiality obligations shall be unlimited.

In no event shall either party be liable for any indirect, incidental or consequential damages or liability, under or in connection with or arising out of this Agreement or the hardware or the software delivered hereunder, howsoever such liability may arise, provided that the claims against customers, users and service providers of NPCI would be considered as a direct claim.

Upon termination, members will not be eligible for any refund of fees from NPCI. The member shall continue to be responsible for any financial or other obligations arising from its membership prior to the termination date. The member shall not indulge in any action that leads to a suggestion that the member is still a part of RuPay card scheme. The member shall be liable to fulfil all obligations incurred as a result of a transaction occurred prior to the termination date. A member notifying NPCI of its intention to terminate shall immediately advise its cardholders, merchants and agents of such action and shall cancel all cardholder, merchant and agent agreements no later than the date on which its termination becomes effective. Any member whose membership is terminated shall thereupon relinquish to NPCI all its rights and privileges in RuPay card scheme and shall immediately discontinue the use of and destroy all printed materials and supplies bearing (i) the name RuPay, (ii) the marks of NPCI, or (iii) any colourable imitations

of the foregoing. A terminated member shall maintain confidentiality of RuPay card scheme information. The terminated member should indemnify NPCI from any falsely projected image of RuPay and can be penalized for projecting association with RuPay card scheme in spite of the termination.

Force Majeure

If at any time during the subsistence of a Member's Membership with NPCI, NPCI or a Member is prevented or delayed from performing any of its obligations hereunder by causes, circumstances or events beyond the control of NPCI or a Member respectively including delays due to floods, fires, accidents, earthquakes, riots, explosions, wars, hostilities, acts of government, or other causes of like character, despite due diligence and reasonable efforts to do so, NPCI or a Member shall be excused from performance hereunder for so long as such causes, circumstances or events continue to prevent or delay such performance.

NPCI Systems Failure

NPCI is not responsible for any claims arising out of:

1) Defect or malfunction of any equipment, facilities, or software used by NPCI to perform authorizations or RGCS services
1) Loss or corruption of any data flowing through RGCS
2) Failure or performance degradation of NPCInet
3) Failure or performance degradation of Central Switch or RGCS system
4) Incorrect interchange reimbursement fees irrespective of whether the cause is due to NPCI error, Issuer error, Acquirer error, system breakdown or software error

Fraud Related Liabilities

The responsibilities of various parties in case of fraud related liabilities are detailed in RuPay Fraud Risk Management document.

Maximum NPCI Liability

NPCI, under any situation will not be liable in total for any individual or related series of claims.

Customer Care Indemnification

Members should indemnify NPCI against all claims arising out of related customer care services.

3.6.2 Issuer Guidelines

IIN use

A member is responsible to NPCI and all other members of NPCI for all claims arising from the use of the assigned IIN. In case of a recalled IIN, an IIN licensee is responsible and liable for any recalled IIN until it is fully deleted from all NPCI systems. In case of IIN transfer, NPCI holds the transferring institution financially liable for all portfolio activities, in addition to payment of all applicable fees, until NPCI acknowledges all required documentation. In case of a portfolio sale/ transfer/merger that result in a

change of IIN licensee, the full liability associated with the acquired IIN lies only with the purchasing or surviving organization.

Marks and Promotions Indemnification

1) Issuers using NPCI marks shall indemnify NPCI against all claims arising out of such an usage
2) Members that refer to any promotional activity of RuPay card scheme should indemnify NPCI against all claims arising out of such a reference

3.6.3 Acquirer Guidelines

PIN security

The Acquirer should ensure that required safeguards for protecting PINs are in place as specified in the Authorization manual. The Acquirer should indemnify the Issuer against any claims resulting from non compliance to these security guidelines.

Merchant Acquisition

Acquirers who use third party processors (Third Party) for acquiring merchants are responsible for ensuring that the Third Party follows the Acquirer guidelines. The liability for the merchant acquisition through Third Party rests with the Acquirer.

3.7 Vendor Management Guidelines

Vendors are those entities that assist the Principal, Associate or the Participant members in fulfilling their obligations to NPCI; these entities do not interact with the NPCI systems / switch in any manner. The vendors could comprise of entities like, but not limited to, card manufacturers, magnetic stripe card personalizer, IC personalizer, IC embedder, IC pre-personalizer, terminal manufacturer.

Vendors are not granted membership status of RuPay scheme and they support and act on behalf of Principal, Associate or Participant members who are members of RuPay scheme.

Members that are supported by vendors should comply with the guidelines specified in Vendor Management Guidebook

On-boarding

The vendor must inform NPCI of its interest in order to initiate the on-boarding process. The vendor should submit copy of their most recent audited financial statements (previous three years), previous experience details and a brief history of the organization and promoters profiles.. The procedure for on-boarding of vendors is detailed in vendor Management Guidebook.

Certification

All certified vendors must adopt the security control processes and security devices specified in security guidelines section 'Vendor Security Compliance' of Vendor Management Guidebook as a minimum protection for card products bearing the RuPay brand. Any divergence from these requirements needs a written approval from the RuPay compliance committee.

Certified vendors may adopt additional controls, as they find appropriate, provided they are in addition to and enhance the procedures mentioned in Vendor Management Guidebook. All additional controls and enhanced systems need to have prior approval of NPCI. The RuPay compliance committee will take the final decision about the Vendor's security control.

An Issuer may use a vendor for the production of card products and related components bearing the ''RuPay'' brand only if the vendor is certified and registered with NPCI to be in compliance with the requirements mentioned in section 'Certification' of Vendor Management Guidebook.

The vendor certification program is managed and overseen by the NPCI. NPCI will choose to appoint any external certification or audit agency for conducting the certification.

The various steps that need to be followed while getting the compliance done are specified in section 'Certification Process' of Vendor Management Guidebook.

A certified vendor must comply with security standards at every given time and must notify NPCI immediately of the following:

a) Change in location of the certified site or extending the existing certified building.
b) Any changes to the security procedures.
c) Change in the company management, structure, and shareholding pattern.
d) Upgrading or replacing major equipment.
e) Establishing joint ventures or agreements with other certified or non-certified Vendors.

In the event any of the above mentioned points occurs, NPCI may require that the vendor may contract with one of the external audit firms accredited by NPCI to perform a follow-up security audit of the vendor site. All the costs related to this activity should be borne by the vendor.

Security Compliance

Vendors will be required to do business operations under various security challenges and hence they are expected to abide by the below security compliance guidelines:

1) Vendors should abide by the security procedures specified in section 'Personnel' of Vendor Management Guidebook which covers all personnel that have access to RuPay card and its products, components and the data environment. The guidelines are related to:
   a) General security procedures
   b) Screening and documentation
   c) Identification access cards/badges
   d) Change of role & attrition management
2) The in-house or contract security personnel must meet the same pre-screening qualifications requirements as personnel that access to RuPay card products, data environment. In the event the security personnel are outsourced, the outside source must maintain liability to cover for any potential losses. Detailed guidelines for security personnel are specified in section 'Security Personnel' of Vendor Management Guidebook

3) Vendors should handle visitors or non-employees (including consultants and maintenance staff from any sub-contractor) as specified in section 'Visitors or Non-employees' of Vendor Management Guidebook
4) Vendor premises guidelines including access controls, security control room, high security areas, locks and keys, shredding room and other safety norms are specified in section 'Vendor premises' of Vendor Management Guidebook
5) Vendors are expected to abide by the guidelines on production processes, returned cards, data handling processes, waste management and security policies specified in section 'Vendor Security Compliance' of Vendor Management Guidebook

Logical Security Compliance for Card Vendors

Vendors should abide by the guidelines specified in section 'Logical Security Compliance for Card Vendors' of Vendor Management Guidebook which covers the below aspects:

a) Key management
b) Networks and systems
c) Data security

Audit Guidelines

NPCI audit guideline is to assess the vendor's financial and business risk. Internal and external audits may be used to review specific information relating to different operations of the vendor. Audits will test financial information for accuracy and validity. Audits will focus on security aspects. The audit will determine various compliances of the vendor:

a) Financial compliance
b) Commercial compliance
c) Legal compliance
d) Vendor premises
e) Personnel
f) Production
g) Security
h) Business continuity plan

Details on audit methodology, audit plan, audit frequency, audit agency criteria and qualification and audit fees are specified in section 'Audit Guidelines' of Vendor Management Guidebook

Penalties

A member whose vendor fails to comply with the RuPay physical security validation compliance will be assessed by the RuPay compliance committee and appropriate penalties will be imposed on the NPCI member. Descriptions of these penalties are specified in *Member Certification Guidebook*

3.8 Ownership of Marks

The member shall accept NPCI's ownership of marks. The member agrees that it will not object or challenge or do anything adverse, either legally or publicly against the NPCI marks. The member will not modify, adopt, register or attempt to modify, adopt or register, any names, trademarks, service marks, trade names, logos, or any word or symbol that is remotely similar to or bears any resemblance to NPCI

marks, as a part of the member's trade name, company name, product names, marks, copyright or otherwise.

At NPCI's request, the member shall immediately withdraw all its rights it may have in any NPCI marks. The member shall agree that all use of NPCI marks by the member shall be for the benefit of NPCI. In case the members requires to launch a card in liaison with any other corporate as a co-branded card, then the member needs to inform NPCI in writing 90 days in advance and take written approval from NPCI. The member needs to adhere to the specifications and guidelines mentioned in the RuPay Card Marks and Specifications document to issue the co-branded card and should ensure the partner corporate also adheres to the specifications and guidelines mentioned in the document.

4 The RuPay Brand

NPCI is a section 25 company having its own equity members and has been formed with the below mission:

"To build state-of-the-art world class customer friendly electronic retail payments system available & affordable to all, round the clock"

RuPay is a brand of NPCI under which it operates the card scheme.

4.1 Introduction

This chapter describes how RuPay Brand is to be positioned and provides guidelines on the use of RuPay marks, restrictions on use of marks, presence of other marks, use of marks for promotions, rules to be complied with by members for usage of NPCI brand and marks and the compliance required with these rules.

4.2 Key Principles

1) Members/Vendors including card manufacturers should comply with RuPay Card Marks and Specifications and RuPay Brand Protection Guidelines and Vendor Management Guidebook document while using the RuPay marks
2) The positioning of RuPay marks on the bank cards (credit, debit and prepaid) should be as specified in RuPay Card Marks and Specifications
3) Members should not use the RuPay brand and / or marks as part of its corporate identity
4) The RuPay marks should not be used other than in relation with NPCI products, promotions, offers, sponsorships, services, processing and acceptance
5) No marks other than the NPCI / RuPay brand mark should be used to indicate acceptance at the point-of-sale

4.3 RuPay Brand Positioning

RuPay will position itself as 'India's domestic card scheme for enabling member banks to issue and acquire electronic payment across all consumer segments at the right price'.

4.4 RuPay Marks

Components

RuPay Marks includes the NPCI/RuPay Logo, Brand Name, RuPay Slogan, RuPay Hologram and other ancillary marks.

Compliance

The use of RuPay marks must comply with the guidelines specified in RuPay Card Marks and Specifications, RuPay Operating Regulations and RuPay Acquirer manual.

4.5 Restrictions on use

4.5.1 Acquirer Guidelines

Protecting brand reputation

Acquirers must ensure that the RuPay marks are not used in any such manner that may bring the brand into disrepute. The use of RuPay marks by the acquirers and merchants on all its communication, posters, signages, websites. including co-branding initiatives should be only after prior intimation and approval of NPCI. There should be no unlicensed usage / misuse of RuPay brand by the acquirers or any other entities associated with the acquirers including merchants, Third Party and vendors.

Acquirers must ensure that all its merchant outlets, agents or e-commerce merchants do not process any illegal transactions including, but not limited to:

1) Purchase of photographs, videos, cartoons, simulation or any other media or activities including but not limited to
   a) Pornography
   b) Rape
   c) Terrorism
   d) Bestiality
2) Goods or services the provision of which is illegal (e.g. drug trafficking)
3) Sales where the amounts charged do not correspond with the value of the goods or services purchased or rendered
4) Cash at merchant outlets excluding Cash at POS
5) Amounts which do not represent a bonafide sale of goods or services at the merchant location
6) Any unlawful activity as defined by constitution of India (Central/ State governments etc)

Adherence to RuPay Merchant and Third Party Processor Compliance

Acquirers must ensure that their operations should comply with RuPay Acquirer Manual

Adherence to RuPay Brand Protection Guidelines

Acquirers must comply with RuPay Acquirer manual. These guidelines specify instances where RuPay brand may be associated with illegal activities or any other activity that may have an adverse impact on RuPay brand.

Some examples of such activities are including, but not limited to the following:

1) Sinful Transactions
2) Sale of counterfeit or trademark infringing services or products
3) Deceptive Marketing Practices

Adherence to RuPay Operating Regulations

Acquirers must ensure that their operations should comply with the guidelines mentioned in this

document.

Notifications
Acquirers will receive notifications from NPCI if their merchants have indulged in any transaction(s) that may lead to the disrepute or damage of RuPay brand. This notification will include timelines for responding to the violation and remediation plan. This may lead to financial implications and eventually termination of membership.

Remediation
Once the acquirer has been identified by NPCI for any violations, the acquirer should immediately take strict action to address the matter on an urgent basis and make sure no further transactions take place through the specific merchant. The acquirer is also expected to submit a detailed report on the remediation and controls implemented to NPCI within the timelines mentioned by NPCI.

Waiver
NPCI reserves all the rights to decide upon the suspension or waiver of penalties due to non-compliance on a case to case basis. The acquirers need to inform NPCI within 10 days post receiving the notification in case they wish to seek waiver of penalty

The waivers are granted at the sole discretion of RuPay compliance committee and will be granted only for the agreed timeframe.

4.5.2 Issuer Guidelines

The RuPay Brand Name can be used on the card only when it is:
1) Part of a product name
2) Used only as a term "RuPay Card" when used in conjunction with an issuer's product name

Trademark Denotation Symbols
Display of a RuPay mark on cards, websites, or printed marketing materials may require the use of a registration symbol (e.g.,™) to denote registered trademark status.

Non-RuPay Marks and Other Language on RuPay cards
Certain trade names, including those of an issuer, an issuer's holding company, or an issuer's agent may appear on a RuPay card as long as it does not interfere with the RuPay brand mark and its standardized background, or with the functional or security features of the card.

With the exception of marks owned by entities deemed to be competitive by NPCI, the following marks and language may appear on RuPay cards:
1) A trade name or mark of a non-issuer (e.g., co-branding partner or affinity entity) can also be placed on the back of a RuPay Card if the issuer trade name or mark is used on the front of the card
2) Words that indicate an account classification, type, service description, or other information associated with the card (e.g., type of bank account, VIP status)
3) Characters that identify an account or provide security identification

Members need to take prior written approval of NPCI to use the marks and language as specified above. Members should not include advertising, promotional or other language on a RuPay Card, unless it is an integral part of the identification of the issuer's organization

With prior written consent from NPCI, a RuPay card may display:

1) Marks associated with proprietary, local, regional, national or multinational services that are not competitive to RuPay
2) Marks that identify the services of the issuer or trade names that identify the issuer, in any colour

Prohibited Use of Marks

1) Issuers should not issue a RuPay card bearing the trade name or mark of any entity that is competitive with RuPay or with a RuPay card scheme program.
2) Issuers should not issue a RuPay card with a trade name or mark that is confusingly similar to a RuPay mark.

Use of Similar Marks

Members should not use any component of the RuPay mark or a mark similar to the RuPay mark for any purpose not related to the RuPay card scheme. If NPCI notifies a member that its trademark is similar to a RuPay mark, the Member must immediately stop using the mark.

Transaction Monitoring

1) Issuers must monitor card usage and transactions at high risk merchants
2) Issuers shall be liable for any transaction authorized by issuers, even if originated at illegal MCCs and for and illegal transactions

4.6 Use of Marks on Cards

Mark placement

The RuPay brand mark must be placed on the RuPay card as follows:

1) RuPay brand mark must be placed and positioned as specified in RuPay Card Marks and Specifications
2) NPCI-approved card manufacturers have the information necessary to incorporate the RuPay brand mark into the card
3) A clear space area, free of text or graphics must be maintained on all sides of the mark as specified in RuPay Card Marks and Specifications

Other elements

The account number, expiration date and cardholder name/identifier must be placed on the card as specified in RuPay Card Marks and Specifications. The account number, expiration date and cardholder name/identifier must not interfere with the card's functional or security features.

The detailed specifications are available in RuPay Card Marks and Specifications

4.7 Member Identification

The Issuer identification must be placed on the RuPay card as follows:

1) The Issuer name and/or logo must appear once, either on the card front or on the back of the card.

2) The Issuer name and/or logo must not be placed over the RuPay brand mark and its clear space area.

Requirements

1) Issuers may use a proprietary program name on the front of the card with or without their name included.
2) If the Issuer name is not included on the front of the card, it must appear on the back of the card
3) A RuPay card cannot be issued bearing the trade name or mark of any entity that is competitive with RuPay or with a RuPay program.

IIN

The IIN is a number used to identify an issuer for authorization, clearing, or settlement processing. Issuers must ensure that the card is pre-printed with the first 4 digits of the IIN. These first 4 digits will also become the first 4 digits of the card permanent account number (PAN) during the personalization process. The details for this are clearly specified in the RuPay Card Marks and Specifications.

4.8 Co-Branding Marks

1) To launch a co-branded card, member needs to inform NPCI in writing 90 days in advance and take written approval from NPCI
2) Members should adhere to the guidelines and specifications mentioned in RuPay Operating Regulations and RuPay Card Marks and Specifications
3) Members should ensure that the co-branding partner also adheres to the guidelines and specifications mentioned in RuPay Operating Regulations and RuPay Card Marks and Specifications

4.9 Use of Marks in Marketing

1) Members should not include advertising, promotional, or other language on a RuPay Card, unless it is an integral part of the identification of the issuer's organization
2) The marks of RuPay must be used only for promotional purpose as a way to indicate acceptance of RuPay cards and not as sponsoring or endorsing the merchant's products unless agreed upon by NPCI in writing.
3) The name 'RuPay' must appear on all statements & communications to the cardholder like promotions, campaigns, newsletters related to RuPay card scheme
4) Issuers should obtain prior approval from NPCI for all marketing materials related to the RuPay card scheme
5) Members should not use the RuPay marks for its promotional activities along with marks of an entity that is competitive with RuPay
6) Acquirers should approve in advance all marketing materials involving RuPay marks used by the merchants
7) Members should not use RuPay marks in a marketing material if there is any chance that it could be mistaken for an actual card
8) Members should not use the RuPay brand name in any classified advertising section

4.10 Audits

NPCI will conduct periodic audits to ensure that all entities authorized to use the RuPay Marks comply with the NPCI guidelines. NPCI will conduct audits to ensure compliance in relation to use of RuPay marks, and all communication related to product and promotions.

A member that fails to comply with the Brand Protection Guidelines as mentioned in RuPay Acquirer Manual will be assessed by the compliance committee and appropriate penalties will be imposed. Descriptions of these penalties are specified in Member Certification guidebook

5 RuPay Products and Services

5.1 Introduction

This section contains guidelines and information for any member participating in the RuPay scheme as an issuer. It outlines the requirements, issuance procedures and other service standards to be followed by an issuing member.

5.2 Key Principles

1) **RuPay Brand Integrity:** All the members of RuPay scheme should agree to comply with technology and operating standards mentioned in the various manuals and documentations published by NPCI from time to time for the RuPay scheme. All members should adhere to card marks & specifications requirements mentioned in RuPay Card Marks & Specifications to ensure the safety and integrity of RuPay brand and its systems.
2) **Seamless transaction processing:** RuPay member should ensure that seamless transaction and data processing are available to all its RuPay cardholders. To meet diverse needs of cardholders in RuPay system, all the members should adhere to the RuPay policies and standard defined in RuPay Product Manual.
3) **Data sharing and reporting:** All RuPay card issuers must provide quarterly reports, in the NPCI format defined in the RuPay Product Manual, to NPCI with details of cards issued, number of cities covered for card issuances, number of transactions, value of On-us and Off-us transactions, and count of active cards on POS and ATM's. The issuers must also submit a confirmation document to NPCI on an annual basis that all its systems related to the implementation of the RuPay debit card have been audited, certified and are in compliance with NPCI requirements and guidelines.
4) **Following the guidelines established by NPCI:** All RuPay card issuers must agree to follow all applicable standards and guidelines established by NPCI with regards the RuPay scheme. RuPay standards and guidelines are to ensure integrity, visibility, recognition and security of the RuPay brand and products.

5.3 Issuer Responsibilities

5.3.1 Confidentiality of cardholder information

RuPay card issuer must only use and share cardholder information with NPCI and with its agents only for the purpose of processing, authorizing, cardholder's transaction and to provide assistance to cardholder.

5.3.2 Issuer disclosure of cardholder liability

RuPay card issuer must disclose the cardholder liability to RuPay cardholder in scenario of unauthorized transactions done on RuPay card.

5.3.3 Card usage notification to cardholder

RuPay card issuer must inform RuPay cardholder about the do's and don'ts of card usage and relevant RuPay and issuer-specific guidelines.

5.3.4 Issuer disclosure of fees and charges

RuPay card issuer must provide written information and details of all applicable fees and charges to the cardholder. Any amendments in fees and charges should be informed to cardholder in advance.

Issuer must provide tariff sheet with details of all applicable fees, charges and details of terms and conditions and any other applicable agreement to the cardholder.

5.3.5 Legal & Regulatory Compliance

1) It is the primary and sole responsibility of the issuer to ensure that all its card programs, customer relationships, terms & conditions are in compliance with all applicable government law, RBI guidelines and other regulatory guidelines
2) Issuers are responsible for ensuring compliance with the anti-money laundering policies as per The Prevention of Money Laundering Act, 2002, its amendments and any other related guidelines on the Anti-Money Laundering
3) Issuers are responsible for ensuring compliance with any privacy related regulations of the government which includes sharing of cardholder information with any third party
4) Issuers are responsible for payment of all applicable Government Taxes related to the card program
5) Issuers are responsible for ensuring compliance with applicable FEMA Guidelines

5.3.6 Audit

NPCI or any organization designated by NPCI may audit the system, records and procedures or facilities of the issuer at any given point of time.

5.3.7 IIN usage

Issuer must apply to NPCI to obtain an IIN and issuer should comply with all the mandatory requirements mentioned in RuPay - IIN maintenance Manual

1) Issuer may assign multiple card programs to the same IIN
2) NPCI reserves the right to reject the issuer's request for an IIN
3) Issuer needs to provide necessary forms and documents to NPCI for IIN activation
4) For each new card variant an issuer must assign a unique IIN account range

The regulations governing IIN assignment, activation, release and management are clearly defined in the RuPay - IIN Maintenance Manual

5.3.8 RuPay card name

All RuPay debit card issuers must ensure the use of the RuPay name on the RuPay card issued. The name RuPay must appear on:

1) All card plastics

2) Communications to the cardholders like promotions, campaigns, newsletters and usage guide, related to RuPay card program

5.3.9 Card shipping and security

RuPay card issuers must ensure compliance with the RuPay and RBI guidelines, including any amendments from time to time, for transportation and shipment of the RuPay cards, PINs and all other RuPay material to the cardholders.

For details on RuPay product guidelines; kindly refer the RuPay Product Manual.

5.4 RuPay Card Issuance Process

The RuPay card issuance process consists of three steps:

5.4.1 Step 1: Pre-issuance

Card design

Issuers must comply with the card design, brand, and technical specification guidelines as specified in RuPay Card Marks & Specifications. The issuer's customer service number must be mentioned on the card. All card designs must be approved by NPCI prior to sending the same for production.

Cardholder acquisition

Cardholder acquisition is a critical step in the card issuance process and thus it is essential that due care and preventive measures against frauds are implemented at this stage. The issuer should follow the guidelines mentioned below to reduce risk of losses due to application frauds

1) Ensure Know Your Customer (KYC) norms are met before issuance of card
2) The issuer should adopt a robust evaluation process and due diligence process at the time of on boarding the customers which could include adequate credit checks, bureau checks, fraud checks, verifications etc. In case there are any specific guidelines published by RBI same should be adopted by members.
3)
4) Decline direct-mail applications that have been substantially altered or submitted by anyone other than the intended party
5) Implement "closed-loop" feedback process involving all members of the payment chain to identify characteristics of fraudulent applications and develop preventative measures for the same
6) All applicable fees and charges details are shared with cardholder

5.4.2 Step 2: Issuance

Card/PIN issuance and distribution

The transportation and delivery of RuPay card and other RuPay card materials must be taken care of appropriately by the issuers.

RuPay may require all cardholders to be distributed a PIN along with the card. The PIN is mandatory for transactions at ATM networks and required at POS terminals.

Issuers should ensure that the PIN is handed over to cardholder in such a way that no person other than the cardholder knows it and is able to access it. The issuer may send the card in de-active mode to prevent fraudulent usage of cards, intercepted midway before reaching the actual cardholder.

Issuers should comply with the RBI guidelines issued from time to time in matters related to issuance and dispatch of Pins. RuPay internal guidelines related to the same have been mentioned in RuPay Issuer Implementation Guidebook.

Cardholder communications:
Issuer must develop effective processes to provide cardholder communication materials to their cardholders.

Cardholder communication materials are important for all RuPay debit products. The following recommendations must be considered while developing the communication materials:

1) Cardholder communication must be a regular exercise and must be increased during promotional offers
2) Cardholder information may be designed to encourage customers to increase usage of RuPay debit cards
3) Cardholder communication must include security precautions that cardholders must exercise to prevent fraud
4) The communication material must include contact details for queries and emergencies

5.4.3 Step 3: Post Issuance

Customer services:
Issuers must provide customer service number/s to all its cardholders. The same needs to be mentioned on the card, usage guide, website, promotional campaigns and any other mode of communication.

Any change in the customer service number must be promptly communicated to the cardholders at least 30 days prior to the change

Issuer must ensure that customer service support is available for the following functions

1) Dispute resolution
2) Card product information
3)
4) Card cancellation

Issuers must ensure that 24*7*365 customer service support is available for the following functions:

1) Fraud Detection
2) Lost/Stolen cards

Transaction processing
RuPay debit card program has developed a support framework to enable transaction processing
The following are the key transaction processes:
1) Authorization processing
1) Clearing and settlement processing

Authorization is a process through which a card issuer approves or declines a card transaction. Before a transaction is presented for clearing and settlement, it needs to be authorized by the issuer.
Issuers must ensure that they have connectivity to the NPCInet and must be aware of the file and message specifications for Clearing and Settlement. The details can be found in the RuPay Global Clearing and settlement Manual

Dispute resolution
To protect cardholder rights, issuing institution can raise dispute on questionable transactions with acquirer through retrieval request/charge back process.
For details on dispute settlement guidelines for different types of issuers; kindly refer the "RuPay Dispute Management Rules and Regulations"

5.5 RuPay Card Features

NPCI offers two unique RuPay card products
1) The RuPay Classic
2) The RuPay Gold

RuPay Gold is a higher variant product offering which the issuer can offer to its customers. This product is targeted at a customer base that maintains higher balances with the issuer and is considered a preferred customer base**.**

For each targeted customer segments, issuers are expected to create a value proposition around the RuPay debit offering. This will help them deliver quality service to their customers. Moreover the issuer can always provide add-on services and benefits to the cardholders to enhance their card usage experience.

The RuPay debit card product features can be viewed in the light of the following major aspects:

Acceptance
The RuPay card is valid for transactions at Point of Sale (POS), Automated Teller Machine (ATM) and E-Commerce (E-Com)

Transaction types
The RuPay card is valid for Purchase, Purchase with Cash Back, Cash at POS, ATM Cash withdrawals, ATM PIN Change, ATM Balance Enquiry transactions and various allied services through ATM's.

Card design features

The RuPay card offers option of 16 or 19 digits Primary Account Number Length to issuers.

For details on RuPay product features; kindly refer the RuPay Product manual.

5.6 RuPay Card Marketing and Positioning

Marketing strategies
The issuer should have a well-defined marketing strategy to market the new product and ensure competitive positioning in the market

Positioning
The issuer needs to decide upon the positioning of the RuPay base Debit card - "top of the wallet" card. The positioning will largely be determined by the segmentation strategy of the issuer

Branding
The issuer needs to take all the necessary steps in terms of marketing & communication through all means & channels to promote RuPay brand to the customers

Pricing
The issuer needs to finalize the annual and renewal fees for this product, based on the positioning and strategy

Packaging
The packaging of the RuPay base debit card determines how the card is presented to the customers. The same includes physical design, card cover, usage guides, as well any other marketing communication accompanying the card. The member needs to obtain necessary approval from NPCI for the same at least 30 days prior to the card roll out and pilot launch

Activation
The issuers must try to ensure maximum activation levels for the RuPay cards issued by them

Promotion
The issuer needs to undertake various types of promotional activities, both above-the line (ATL) and below-the-line (BTL) campaigns to reach out to its prospective customers. ATL is a type of advertising through media such as television, cinema, radio, print, and out-of-home to promote brands or convey a specific offer. This type of communication is conventional in its nature and is considered impersonal to customers. BTL uses unconventional brand-building and promotional strategies, such as direct mail, sales promotions, telemarketing and printed media (for example brochures, and usually involves no motion graphics). It is much more effective than when the target group is very large and difficult to define.

Marketing materials
Issuers must submit samples of all their marketing communications, terms & conditions, website content, and disclosures to NPCI for approval prior to publishing the same. The same should be submitted to NPCI for approval at least 15 days prior to publishing the materials

NPCI's review of marketing and other materials is only for the purpose of checking that they do not violate any compliance or pose any risk to the RuPay brand. The issuer will be responsible to ensure that all legal and compliance-related requirements are satisfied.

Target Segment

The issuer should have a clear policy to identify the target customer segment for the RuPay debit cards. The issuer can issue the cards to both the new and the existing customer card base. NPCI will provide all the guidelines to the issuers for issuance of RuPay card to their prospective customers.

Continuous Evaluation

Post product launch, the issuer should track the performance of the launched product. This would allow the issuer to evaluate the success and the failure or lapses of the product.

For details on RuPay product guidelines; kindly refer the RuPay Product manual.

6 RuPay Card Acceptance

6.1 Introduction

This chapter specifies the requirements that apply to an acquirer in on-boarding, training and risk control of merchants. The chapter also outlines the regulations related to terminals, transaction processing and receipts.

The various compliance points are designed for:

1) Acquirers to know their obligations and responsibilities towards the RuPay payment systems
2) Members to manage and monitor their relationships with merchants, and agents of the merchants
3) Provide guidelines to merchants participating in the RuPay card scheme

6.2 Key Principles

1) **Adherence to technology standards:** RuPay acquiring members must adhere to the PCI PED (Payment Card Industry PIN Entry Device) standards and also in some cases PCI – PAD standards to ensure coherent functioning of systems and uninterrupted secure transaction processing
2) **Accepting RuPay products for payment:** All merchants should accept all types of RuPay cards that are made available from time to time, which includes credit, debit, prepaid and any other form of emerging payment instruments. This would also be applicable to the evolving payment technologies like EMV, near field communication or contactless which should be accepted by the merchant. The merchant should not be preferential to any card scheme and should be scheme neutral.
3) **Merchant's jurisdiction:** An acquirer must only contract with merchants that have a registered office in India.
4) **Entering into a merchant agreement:** An acquirer must sign an agreement with the merchant before it starts to accept RuPay cards.
5) **Merchant Inspection:** The acquirer, through inspection, must ensure that the merchant does not pose a high risk, as defined in the RuPay Acquirer Manual. Acquirers should ensure that there is a strong fraud prevention mechanism while setting up the merchant account.
6) **Merchant training:** The acquirers should take all measures to ensure that their merchants & third party agents are provided with sufficient information & training to understand their roles in the payment system and effectively fulfil their obligations towards the cardholders, other RuPay members, towards the RuPay scheme and NPCI.
7) **No surcharging:** No merchant should impose any surcharge on a RuPay card transaction. There can be variations to this rule and the merchant can contact the relevant acquirer for further details and clarifications, as defined by RuPay from time to time.
8) **RuPay brand protection:** Acquirers and merchants of the RuPay card scheme are expected to follow the guidelines set by NPCI in the RuPay brand protection guidelines for acquirers. In case of non-compliance, the acquirer of merchant will be subject to fines and penalties as outlined in the above mentioned document.

6.3 Acquirer and Merchant Requirements

6.3.1 Relations between the acquirer and the merchants

RuPay acquirers are solely responsible for the affiliation of all merchants. Merchants must remain free to choose with whom they would like to be associated with and may sign a contract with as many acquirers as they so desire.

For this purpose, the merchant who wishes to accept payment must sign a contract with each of the acquirer with whom he wishes to route all or some of its transactions. Each contract between an acquirer and a merchant must include the clauses required by NPCI. The details of these clauses are mentioned in the Merchant & Third Party compliance document for acquirers.

6.3.2 Merchant Enrolment Application

The merchant enrolment application is essential to obtain all the relevant information about the merchant. The relevant contact details of the acquirer must also be shared with the merchant for service/any other issue or support required.

The acquirer should verify the merchant's financial soundness and the risk of fraud before entering into any agreement with the merchant. Hence the acquirer must gather all the relevant information on the merchant's background, business model, location and promoters or owners.

The details gathered by the acquirer needs to be documented and stored for a period of at least 12 months or as stipulated by NPCI from time to time.

The acquirer should take the details of the business, brochures, cancellation policies, URLs, SSL certificates, and the promoters. Acquirers must complete the following checks:

1) Merchant premise inspections
2) Member details
3) Background information
   - Business background
   - Operational background and
   - Business location

An acquirer must verify additional application information for card not present transaction processing merchants. This includes business plans, advertisement details and other marketing materials. Additionally, the acquirer must check whether the applicant is an existing merchant that wants to add a website, or a new merchant. The form should collect additional information like the URL, IP address, details of the customer service, terms & condition of the sale, security guidelines and risk management guidelines which the e-commerce merchant should provide to acquirer.

For additional information regarding merchant application; members may refer the RuPay Acquirer Manual.

6.3.3 Merchant Agreement

6.3.3.1 General Requirements

An acquirer must sign an agreement with the merchant before it commences the service of accepting RuPay card. The merchant agreement must legally bind the acquirer and the merchant. The agreement must be designed to reduce the acquirer's exposure to risk and losses. However the acquirer will be liable for all losses occurred due to any merchant activity.

The agreement should have clear terms of termination and all the regulatory guidelines prescribed by the regulator/governing bodies. The agreement should also clearly state the right of the acquirer to hold funds of the merchant.

The agreement should have, but not limited to, the following mandatory clauses:

1) The contracting merchant should have a registered office in India
2) The merchant shall not disclose card holder information to any third party
3) Merchants and its agents should not retain the track data post the authorization
4) The merchant's liabilities like chargeback & fines should be clearly stated
5) Chargebacks will be directly debited from the merchant's account and the merchant is required to maintain necessary reserves to cover the same
6) Merchants should not levy surcharges on the transactions unless explicitly permitted by NPCI
7) The marks of RuPay must be used only for promotional purpose as a way to indicate acceptance of RuPay cards and not as sponsoring or endorsing the merchant's products unless agreed upon by NPCI in writing
8) The acquirer/NPCI or any entity on behalf of the acquirer/NPCI reserves the right to audit the merchant at any time
9) The acquirer reserves the right to terminate the agreement for any reason at any time

The following rules must be followed by the acquirers before they enter into a legal agreement with their merchant:

1) The acquirers must have in place an agreement for all its merchants, which ensures that a merchant operates under the rules and regulations established by NPCI and the acquirer.
2) The merchant agreement must include the clause that the acquirer is the principal party and the services are extended to the merchants by the acquirer
3) Individual merchants can choose to move their relationship from existing acquirer to another acquirer without obtaining the consent of the existing acquirer. The merchant should inform the acquirer incase of termination of relationship within the specified timelines as set by the acquirer
4) Ownership of the merchant's RuPay card-based transactions rests with the RuPay acquirer with whom the merchant has a signed merchant agreement
5) An acquirer must implement a procedure for formulating and validating merchant agreements. A periodic review (once every quarter) may be done by the acquirer to ensure that the merchant complies with terms contained in the agreement
6) The merchant agreement must provide for the immediate termination of a merchant by the acquirer for any activity that may create a loss to NPCI or may bring the RuPay brand into disrepute

7) The merchant agreement must have a clause emphasizing the importance of compliance with the security requirement including but not limited to database security, data storage & data transfer. Acquirers must educate the merchants on the importance of this obligation and the consequences of failing to protect this information
8) All acquirers and their merchants / Third Parties must follow the Payment Card Industry (PCI) Data Security Standard (DSS)
9) The merchant agreement must include a clause that requires the merchant to inform the acquirer in case of any agent that has access to cardholder data
10) The merchant should have a report of all agents and the same should be shared with the acquirer on a quarterly basis
11) The merchant agreement must state that the acquirer is responsible for providing settlement funds to the merchant within the agreed timelines.

Members must refer the RuPay Acquirer Manual for details regarding the rules and regulations.

6.3.4 Merchant Inspection

The acquirer must determine that there is no significant derogatory background information about any of the merchant's principals. The acquirer may obtain this information through:

a) Credit reports
b) Personal and business financial statements
c) Income tax returns
d) Other information lawfully available to the acquirer

Acquirers should ensure that there is a strong fraud prevention mechanism while setting up the merchant account

Following are the requisites that acquirers must evaluate merchants on, before initiating merchant agreements. The requisites have been segregated in terms of card-present and card not present merchants. Members must refer the RuPay Acquirer Manual for further details.

6.3.4.1 Card-present merchants

In case of card present merchants; the acquirer must ensure that:

1) The merchant's POS devices are certified and capable of processing RuPay card transactions which are PIN based. All RuPay transactions will be PIN-based transactions
2) The acquirer should impart necessary training to the merchant and educate them about risk mitigants
3) The terminals should be able to read and transmit track 1 and track 2 data, but should not retain the same. The POS device should not have any data retention software

6.3.4.2 Card-not-present merchants

In case of card not present merchants; the acquirer must ensure that:

1) The website provides all the necessary information like cancellation policies, privacy policies, refund policies and customer services details to the customers
2) The merchant must be educated regarding the risks and liabilities in the card not present transactions

3) The acquirer should advise the merchant to install strong fraud management process and data security including data storage. Please refer the RuPay fraud risk management document.

6.3.4.3 Merchant Premise Inspections

The acquirer should periodically do a physical verification of the merchant premise, wherever possible. The inspection will allow the acquirer to ascertain if there is any suspicious activity. The acquirer should review/inspect the signage, licenses, employees and security details

6.3.5 Merchant Monitoring

The acquirers should monitor the merchants and the agents of the merchants to identify and investigate high-risk merchants at the earliest. Daily monitoring of the merchant's transactions including presentments and authorization can help in detecting any unusual pattern.

The acquirers must monitor various merchant activities, including but not limited to the below:

1) Monitor merchants and investigate situations where there are a significant number of low-value or high-value transactions compared to the merchant's average transaction value
2) New and inactive merchant activity
3) Unusual refund activity
4) Excessive disputes and high chargebacks

For e-commerce merchants, the acquirers should monitor every page on the merchant's website. This review should consist of a combination of proactive and persistent website analysis. Acquirers should review every page on every website at a pre-determined timeline. This is to ensure that merchants do not process illegal or prohibited transactions. An acquirer must comply with the applicable laws and a transaction must be legal in the jurisdiction of both the cardholder and the merchant. The merchant should also adhere to the security guidelines of using SSL certificates, two-factor authentication and other policies mandated by the regulatory authorities or mandated by NPCI and RBI from time to time.

6.3.5.1 New Merchant Monitoring

The acquirer should have high surveillance in the first few months of signing a new merchant. During this time the merchant should look out for the following suspicious activities and investigate the merchant appropriately:

1) The acquirer should check if the presentments of the merchants vary largely or the merchant has done a large presentment on different days which can give an indication of suspicious activity
2) The acquirer should track the authorization activity of the merchant, for e.g. a sudden spurt in authorization in unusual hours which can indicate a fraud
3) A large variance in the average transaction size
4) An unusual number of declined transactions. It may be an indication of phished card accounts or unused accounts

The acquirer must also review and monitor the agent activities on a quarterly basis

6.3.5.2 Activity Monitoring

The acquirer should compare the merchant's actual processing volumes to the normal weekly activity parameters established for that merchant. The acquirer must generate unusual activity reports if any of the following meets or exceeds 150% of the normal weekly activity and report the same NPCI.

1) Weekly gross sales volume
2) Number of weekly transaction
3) Average transaction amount
4) Number of weekly disputes

6.3.5.3 Merchant Investigation

The acquirer must ensure merchant compliance with the regulations and confirm the existence of risk control procedures by conducting physical inspection / audit of the outlet or the merchant website. If the investigation reveals merchant involvement in illegal activity or any other activity that has potential damaging effect to the RuPay brand, the acquirer must:

1) Inform NPCI immediately regarding the same
2) Take appropriate legal action to minimize losses.
3) Cooperate with NPCI, issuers and law enforcement agencies, and release all information relative to the merchant upon request.
4) Attempt to make the merchant responsible for the transaction.
5) Hold funds, if possible.
6) Initiate criminal and civil proceedings against the merchant, if applicable.

An acquirer must, to the best of its ability, assist other acquirers with a fraudulent activity investigation with the following:

1) Investigating merchants, cardholders, suspects, physical evidence
2) Cooperate with RuPay, issuers and law enforcement agencies, and release all information relative to the merchant upon request
3) Recovering lost, stolen, or counterfeit cards.
4) Providing information to proper authorities for the possible arrest of person

6.3.6 Merchant Record Maintenance

The acquire must ensure that all applicable rights to provide any requested/required information to NPCI, are available on enrolment of each merchant.

The acquirer should gather and retain the following daily transaction data for each associated merchant for a period of 365 calendar days:

1) Gross sales volume
2) Number of transaction
3) Average transaction amount
4) Number of disputes received

5) Number of reversals/refunds

6.3.7 Merchant Training

The acquirers should take all the measures to ensure that their merchants & third party agents of the merchants are provided with sufficient information & training programs to understand their roles in the payment system and effectively to fulfill their obligations to the members and NPCI. The acquirers must provide their merchants with sufficient information to ensure they comply with all the rules. For more details on Merchant Training; members may refer the Merchant Training Manual.

6.3.8 Card Not Present Merchant Setup

When setting up a new card-not-present merchant, the acquirer must ensure the following:

1) Establish a clear merchant description for cardholder statements to help facilitate easier merchant name recognition
2) Review cardholder data security issues and requirements with the merchant
3) Educate the merchant about the risk exposure and liability associated with accepting RuPay cards in the card-not-present environment
4) Offer Card Verification Data (CVD) and second factor authentication support
5) Offer solutions to enable merchant to detect high-risk transactions for review
6) Ensure merchants are aware of fraud detection, screening, and monitoring tools
7) Ensure data quality standards are adhered to by the merchant

6.3.9 Risk Management and Mitigation Policies

An acquirer should have an underwriting and control policy for its merchants. These policies must be approved by the senior management of the acquirer. The details of this section provide a framework for developing risk management policies. This includes but not limited to underwriting, portfolio risk management, and agent risk management.

An acquirer must have a specific policy for merchants who operate in high-risk environment and may not sign merchants who have

1) Products & services that may lead to high disputes
2) Delayed delivery of products
3) Product/services that are prohibited or illegal

Members may refer the RuPay Acquirer Manual for detailed information on the following aspects of Risk Management and Mitigation Policies:

Underwriting

The acquirer must have a strong background check and approval processes for each of its merchant while on-boarding them. Whenever the acquirer signs-up with a merchant, the acquirer is agreeing to underwrite the merchant's transaction. The acquirer can have a checklist to identify suspicious activities of the merchant.

Risk Mitigation for high risk merchants

1) Daily debiting of discount and fees for higher risk merchants
2) Requiring letters of credit or reserves for higher risk merchants
3) Establishing more restrictive activity monitoring parameters for higher risk merchants

Merchant Portfolio Risk management

The acquirer should have a clear policy of the portfolio mix of its merchants and the risks the acquirer is, or is not, ready to undertake while on-boarding new merchants. The acquirer should balance his portfolio by having a healthy mix of high, medium and low risk merchants.

Fraud Prevention

The following measures, not limited to, needs to be taken to prevent fraud:

a) Verification of merchant application information including promoter's background and financial check
b) Merchant location/Site verification
c) All the merchants should sign the merchant agreement with the acquirer, and retain the same until the relationship exists and up to 12 months from termination date
d) Website inspection including content, products, privacy policy, refund policy, cancellation policy, terms & conditions, website data security, data storage, SSL payment options over the internet and links to other sites
e) Regular periodic audits need to be undertaken at physical site or on the merchant website

The exceptions must be monitored daily and addressed immediately

Suspicious Activity Investigation

Whenever a suspicious activity is detected, the acquirer must be ready to check and investigate the same in a timely manner. The acquirer should have established policies for investigating the frauds approved by the senior management

The acquirer should implement appropriate risk management controls as decided and governed by NPCI or RBI from time to time.

6.3.10Acquirer Performance Standards

6.3.10.1 Retrieval Request Rate for Acquirer

Total number of retrieval requests received under Fraud reason code by the acquirer must not exceed 1 % of the total settled transactions in a quarter.

6.3.10.2 Chargeback Rate for Acquirer

Total number of chargeback's received by the acquirer must not exceed 1 % of the total settled transactions in a quarter.

6.4 Payment Acceptance Requirements

6.4.1 Honouring Cards

The merchant should accept all types of RuPay cards that are made available from time to time, these includes credit, debit, prepaid and any other form of emerging payment instruments. This would also be applicable to the evolving payment technologies like EMV, near field communication or contactless which should be accepted by the merchant. The merchant should not be preferential to any card scheme and should be scheme neutral. The cards should be treated at par with cash.

The merchant should accept all transactions of any card schemes and every transaction should be treated at par. The merchant should not be preferential to any card scheme and should be scheme neutral.

Discount at POS

A merchant may offer a discount on the maximum retail price of the product to incentivize a cardholder to use a preferred means of payment, provided the following rules are followed:

1. Clearly states the incentive as a discount on the standard price
2. Does not discriminate between RuPay cards and any other comparable cards (comparable cards are any general purpose payment cards that use signature/PIN authentication)

6.4.2 Cardholder Verification Requirements

6.4.2.1 Cardholder Signature Requirements

The merchant should check the signature of the customer behind the card with the signature on the receipt. The merchant should closely check if there is any inconsistency in the signatures. While checking the signature, the merchant should also compare the name and Card Number on the card to that on the transaction receipt. Also in case of high value transaction or in suspicious cardholder behavior the merchant must request for additional identity proof such as PAN, driving license or Passport.

6.4.2.2 Unsigned Cards

While checking the identification details, the merchant should also ensure to check that the card has been signed by the customer. An unsigned card should be considered as invalid. If the merchant receives an unsigned card, then the following steps need to be followed:

The merchant should ask the customer to sign the card immediately in front of the merchant. The signature should then be verified with the customer's signature on a valid government issued ID card. In case the customer refuses to sign the card, then the merchant should request for another card for the transaction.

6.4.3 Magnetic Stripe Terminal Requirements

An acquirer must ensure that all magnetic-stripe terminals:

1) Are capable of and obtain authorizations through the RuPay central switch by reading all magnetic stripes that conform to RuPay card and marks specifications.

2) Transmit the entire unaltered data encoded on the magnetic stripe for transaction processing
3) Does NOT erase or alter any magnetic encoding on a card

Magnetic Stripe terminal service codes
The following procedures related to service codes must be followed

All POS terminals must
1) Read and adhere to all requirements specified in the PCI PDE Standards, or
2) Ask for issuer authorization for all transactions

Acceptance of PAN
A RuPay acquirers must ensure that the POS terminal accepts all 16-19 digit PAN's with RuPay issued IIN's

Acceptance of PIN
Acquirers must ensure that while handling the PIN used to identify a cardholder in a transaction, the process and technology used by the acquirer, merchant as well as its agents are compliant with the standards mentioned in the RuPay Fraud Risk Management Manual. Non-compliance to the same, will lead to penalties and assessments.

The PIN acceptance should comply with the PCI-DSS requirements.

6.4.4 Display of Marks at Point of Transaction

All RuPay members or their merchants (including E-Commerce merchants) must display appropriate marks to identify which cards it accepts at easily visible places on their POS location or website.

A merchant website must display RuPay brand mark unless visual representation of RuPay brand mark is not possible, in which case the RuPay Brand name must be used.

The details on the RuPay brand design are specified in RuPay Brand Manual

6.4.5 Card Acceptance Prohibitions

A merchant accepting a RuPay card is prohibited from the following actions:

6.4.5.1 Surcharge

The merchant should not impose any surcharge for transaction on NPCI card, accept for certain Merchant Category Codes (MCCs), the merchant can impose a surcharge for the transaction. The merchant should contact the acquirer for further details and clarifications on these select MCCs.

6.4.5.2 Tip

The merchant should not add any tip amount to the transaction amount unless explicitly mentioned and

authorized by the customer on the charge slip and permitted by the acquirer.

6.4.5.3 Restricted use

The acquirer must ensure that all its merchant outlets, agents or e-commerce merchants do not process any illegal transactions including, but not limited to:

1) Purchase of photographs, videos, cartoons, simulation or any other media or activities including but not limited to
   - Pornography
   - Rape
   - Terrorism
   - Bestiality
2) Gambling in goods or services
3) Goods or services which are illegal (e.g. drug trafficking)
4) Sales where the amounts charged do not correspond with the value of the goods or services purchased or rendered
5) Cash disbursement for transactions classified other that Cash at POS/Cash back or ATM withdrawals
6) Amounts which do not represent a bonafide sale of goods or services at the merchant location
7) Any unlawful activity as defined by the local regulator

6.4.5.4 Convenience charges

The merchant can charge its customers for convenience while providing an additional service like cash on delivery, internet or mobile transaction. Such charge should be clearly mentioned on the invoice being raised as service charge and should be a part of the final invoice against which the payment is being accepted.

6.4.5.5 Split transactions

The merchant should not process multiple split transactions of varied or same values for a single transaction.

6.4.5.6 Taxes

Any tax amount should not be collected separately. Taxes should be included in the total transaction amount and should be a part of final invoice being raised.

6.4.5.7 Cash refunds

Merchant should not provide cash refunds for any RuPay card transactions. The credit should be processed only to the same card used for the purchase and via the RuPay systems.

6.4.5.8 Display of Card number and expiry date on transaction receipt

The expiry date of the card should not be displayed on the cardholder slip of the transaction receipt. The card number should be suppressed and only the last 4 digits of the card may be displayed on the slip.

6.5 Transaction Processing Requirements

6.5.1 Details on Transaction Receipt

The below mentioned details should be specified on a transaction receipt copy

Data	Details
Card Number	Last 4 digits of card account number should be clearly visible on transaction receipt copy. The remaining digits of card account number should be masked.
Cardholder name or Cardholder reference number for instant card	Cardholder name or cardholder reference number should be clearly visible on transaction receipt copy
Cardholder signature	Clearly defined area for capturing the cardholder's signature
Merchant establishment name and location	Merchant establishment name and location should be clearly visible on transaction receipt copy
Authorization /Approval Code	Authorization /Approval code should be clearly visible on transaction receipt copy
Date and Time of Transaction	Date and time for transactions should be clearly visible on transaction receipt copy
Transaction Amount	Total transaction amount should be clearly visible on transaction receipt copy. If applicable, separate Tip and Cash amount should be clearly visible on transaction receipt copy.
Chip card identifier	If the card being used is a chip card, then the word "CHIP" should be printed on the transaction receipt
Terminal ID (TID)	Terminal ID (TID) should be clearly visible on transaction receipt copy

Other requirements

1) A completed copy of the transaction receipt must be presented to the cardholder at the time of delivery of goods or after services are performed by the merchant.
2) A merchant should not ask the cardholder to sign a transaction receipt until the final transaction amount is entered on the transaction receipt.

6.5.2 General Rules

6.5.2.1 Delivery of goods and services

The goods and services must be delivered to the customers on time and confirmation of delivery of goods is to be obtained. For card not-present transactions the cardholder should be informed about the delivery lead time and method of delivery.

6.5.2.2 Cardholder information

The merchant should ensure that the information of the cardholder including the card number and other personal details is kept confidential at all times.

6.5.2.3 Data Storage

The information regarding cardholder account that is stored or processed must comply with the PCI DSS guidelines. The merchant needs to contact the associated acquirer for the details regarding the same. The data needs to be stored by the merchant for a period of 12 months for any audit or inspection that may be conducted by RuPay.

6.5.2.4 Returns and exchanges

The merchant should have a clear return policy. These policies can help the merchant avoid disputes. The merchant can contact their acquiring banks for the best practices to be included in the policy

6.5.2.5 Minimum and maximum purchase limits

There is no floor limit (minimum amount) for the purchase and the maximum amount that can be purchased are as per the limit of the cards or as decided by the issuer, acquirer or merchant agreement.

6.5.3 Presentment Requirements

A merchant must only present valid, genuine and authorized transactions. For DMS transactions, the transactions must be presented within 7 (T+6) calendar days from the authorization date. In case the transactions are deposited after the 7th day, the same will be tagged as late presentment and the chargeback liability will be shifted to the acquirer.

Tips and surcharges are applicable for only certain, specified MCCs such as Railways, Petrol Pumps and Hotels. For DMS transactions, the merchant can present the tip and surcharge with the actual transaction. For SMS transactions, the acquirer must use the Tip and Surcharge adjustment message on previously settled SMS authorizations for the transactions done on applicable MCCs.

Refer to the RuPay Dispute Management Rules and Regulations and RuPay Global Clearing and Settlement Manual for transaction deposit time frames and other details.

6.5.4 For Voiding Transactions

A merchant must void an authorization before settlement of the transaction

1) If the cardholder elects not to complete the transaction
   OR
2) If the authorization request was submitted in error

The merchant must provide a "VOID" transaction receipt to cardholder for every voided transaction

Further the acquirer should ensure that all voided transactions submitted by the merchants are transmitted onto the RGCS system within 7 calendar days of them been voided.

6.5.5 For Cash at POS Merchants

Disbursal of funds in the form of cash is prohibited for merchants, unless it is participating in RuPay cash at POS and/or cash back service.

A RuPay member must be certified by NPCI for the RuPay cash at POS and/or cash back service, before offering the same to its cardholders. The members are bound by applicable regulatory requirements.

In order to offer cash back and/or cash at POS services, RuPay merchants must ensure that:

1) The transaction is conducted in a face-to-face environment
2) The transaction is authorized by both a PIN and signature
3) Entire unaltered full track data (track 1 & 2) are transmitted
4) The cash back and/or cash at POS service must only be provided to product types permitted by the Reserve Bank of India
5) The cash back and/or cash at POS service must be available regardless of whether the cardholder does or does not make a purchase
6) Cash back and/or cash at POS disbursement limits must not exceed the daily RBI-legislated cash back limits per card
7) For a Cash at POS or purchase with cash back transactions, the merchant must not process a refund transaction for the cash portion of the transaction
8) The transaction receipt should explicitly indicate the cash portion of the transaction
9) Comply with clearing and settlement record requirements

6.5.6 Refund Processing

6.5.6.1 Refund Transaction Receipt

A merchant must process a refund when a valid authorization and presentment was previously processed and

1) The cardholder subsequently either cancelled the transaction or returns the goods.
   Or
2) The merchant wishes to refund the amount in cases of services not rendered
   Or

3) The merchant wishes to rectify any transaction processing error

For processing a refund, the merchant must:

1) Present a refund request to its acquirer along with all the required detail to identify the previously authorized and settled transaction AND Provide a refund transaction receipt to the cardholder
   Or
2) Provide a refund authorization letter to cardholder to raise a dispute on the transaction

Acquirer must process the refund within 5 calendar days from the date the refund request was received. The refund request must describe the merchandise were returned, services cancelled or adjustment made.

6.5.6.2 Refund Restrictions

The merchant must provide a refund in connection with a transaction done on a RuPay card by presenting a refund via the RGCS system only, and not by cash or any other mode.

6.5.6.3 Refund Timelines

An acquirer must process an online refund within 365 calendar days from the authorization date. If this 365 calendar days has lapsed, the acquirer should process the refund via the offline refund process.

6.6 Card Not Present Merchant Requirements

6.6.1 Rules for E-Commerce Merchants

For E-commerce merchants the acquirer must ensure the merchant website provides all of the below mentioned minimum guidelines for their websites.

Description of goods and services

The merchant should provide the complete description of the goods and services offered on their websites. Since the customer cannot see or touch the products, detailed information about the product or service will help the customer

Customer care details

The merchant may provide a customer care number for all its customers even if they have an online or mail grievance system

Return, refund and cancellation policy

The merchant should clearly display its return, refund and cancellation policies. This will help the merchant in reducing its chargeback

Delivery policy

The merchants can have its own delivery policy, however they should be clearly mentioned on the website and any exceptions needs to be detailed

Privacy policy
As a best practice, the merchant should include its privacy policies on the websites for the customers to access

Security policy
Another best practice is to mention details about the security of the site like use of SSL certificates, encrypted web pages and two-factor authentication mechanism for all transactions
The merchant must be educated regarding the risks and liabilities associated with the card not present transactions. The acquirer should advise the merchant to follow strong fraud containment, data security and data storage process. The details can be taken from the RuPay fraud risk management document.

6.6.1.1 E-Commerce indicators

All E-Commerce transactions must be identified with an e-commerce indicator in the authorization request and the clearing record. The e-commerce indicator values should be as mentioned in
1) RuPay Global Clearing and Settlement message specifications manual

Acquirers will be penalized for inappropriate usage of e-commerce indicator value

6.6.2 Two-Factor authentication

As mandated by the Reserve Bank of India (RBI), all the card not-present transaction must have a second level factor authentication. The merchants are expected to follow the guidelines of the regulator and adopt the second-factor authentication mechanism of NPCI for all card not-present transactions. NPCI will provide the acquirer members with the two-factor authentication solution who will then work with the merchant to implement the same.

6.7 Merchant Categories Specific Rules

Below mentioned merchant categories must adhere to the respective rules in addition to the general rules laid down for merchants in NPCI publications.

6.7.1 Airline

Airline Ticket Booking Information
An airline or its third-party booking agent must provide to the cardholder reservation information which must include the following details:
1) Cardholder name, PAN, and card expiration date
2) Reservation confirmation code or a unique reference number
3) Physical address of the establishment
4) Airline ticket booking service provisions relating to the cardholder's obligations
5) All other details related to the reservation

6) Details of cancellation , refund and no show policy
7) On a cardholder's request, the merchant must provide a written confirmation with the above information. The merchant must advise the cardholder to retain the above reservation information for future reference.

Airline multiple tickets authorization

In a scenario when a cardholder purchases multiple airline tickets on the same card, the airline merchant may obtain authorization for each ticket individually.

Airline ticket cancellation code

In case of a cancellation; an airline or its third-party booking agent must:

1) Provide a reservation cancellation code (if the reservation is properly cancelled)
2) And advise the cardholder to retain it in case of dispute.

6.7.2 Hotels

Hotel reservation receipt information

A hotel or its third-party booking agent must provide to the cardholder reservation receipt with the following information:

1) Cardholder name, PAN, and card expiration date
2) Reservation confirmation code
3) Physical address of the establishment
4) Hotel reservation service provisions relating to the cardholder's obligations
5) All other details related to the reservation such as length of stay, room rate, etc.
6) Details of cancellation , refund and no show policy
7) On a cardholder's request, the merchant must provide a written confirmation with the above information. The merchant must advise the cardholder to retain the above reservation information for future reference.

Hotel reservation cancellations

For reservation cancellations:

1) A hotel or its third-party booking agent must accept all reservation cancellations before the specified notification time as specified in the cancellations policy
2) The hotel or its third-party booking agent must not require cancellation notification
3) Merchant outlet or its third-party booking agent must convey in writing the cancellation policy, including the date and time that cancellation privileges expire, to the cardholder

Hotel reservation cancellation code

A hotel or its third-party booking agent must:

1) Provide a reservation cancellation code (if the reservation is properly cancelled)
2) And advise the cardholder to retain it in case of dispute.

Hotel reservation no show requirements

A hotel or its third-party booking agent should not charge more than one night's lodging amount for a no show. A no show would occur if the cardholder has not either:

1) Registered by check-out time the day following the scheduled arrival date

2) Canceled the reservation properly

Hotel refund processing requirements

A refund needs to be processed by a hotel merchant for a cancellation, no show, return of any excess charges, or deposit taken. The same should be processed via its corresponding merchant following the rules of refund processing mentioned above.

6.7.3 Car Rentals

Car rental reservation receipt information

A car rental or its third-party booking agent must provide to the cardholder reservation receipt with the following information:

1) Cardholder name, PAN, and expiration date as displayed on the RuPay card
2) Name and exact street address of the car rental service provider
3) Car rental service provisions relating to the cardholder's obligations
4) A confirmation code
5) Rate for car rental
6) Number of days the vehicle will be held
7) Total amount payable and amount paid if other than amount payable
8) Details of applicable taxes and charges
9) Refund ,cancellation and no show policy

On a cardholder's request, the merchant must provide a written confirmation with the above information. The merchant must advise the cardholder to retain the above reservation information for future reference.

Unavailable vehicle

If a vehicle reserved is unavailable, car rental merchant must provide the following services to the cardholder without charge:

1) Refund the entire advance deposit amount (if taken)
2) At least a comparable vehicle for the number of days specified in the reservation

Car rental cancellation requests

Car rental company must:

1) Accept a reservation cancellation request if made within the larger of
   - 72 hours of the reservation time OR
   - The specified timeframe as mentioned in the cancellation policy
2) On cancellation, the car rental merchant must provide in writing a cancellation confirmation code and advise the cardholder to retain it in case of dispute. Further any

Car rental no-show requirements

A car rental company must hold the vehicle according to the reservation if the cardholder has not claimed or properly canceled the reservation by the specified time. The car rental company may then present a refund with the following information:

1) No-show fee plus tax, as applicable. The amount of the no-show transaction must not exceed the value of:
   - 2 days' rental, including tax, for a specialized vehicle reservation
   - One day's rental, including tax, for a peak time reservation
2) Cardholder name, PAN, and expiration date as displayed on the card
3) The words "No-show refund" should be stated in the refund transaction

6.7.4 Cruise Line

Cruise liner reservation receipt information

A cruise liner merchant must provide to the cardholder reservation receipt with the following information:

1) Cardholder name, PAN, and expiration date as displayed on the RuPay card
2) Name and exact street address of the establishment
3) cruise liner service provisions relating to the cardholder's obligations
4) A confirmation code
5) Room rate
6) Total amount payable and amount paid if other than amount payable
7) Details of applicable taxes, service charges or any other charges
8) Refund ,cancellation and no show policy
9) Other details regarding the reservation

The merchant must provide a written confirmation with the above information. The merchant must advise the cardholder to retain the above reservation information for future reference.

Cruise line authorization - multiple tickets

In a scenario where the cardholder purchases multiple cruise line tickets on the same card, the cruise line merchant should obtain an authorization for each ticket individually

Cruise Line On-Board Casinos

On-board gambling charges, such as the purchase of gaming chips, must be distinct from other cruise charges. They must be:

1) Authorized
   - Processed with MCC 7995, "Betting, including lottery tickets, casino gaming chips, off-track betting, and wagers at race tracks"

Cruise Reservation Cancellations

For reservation cancellations; the cruise line merchant or its third-party booking agent must:

1) Accept all reservation cancellations before the specified notification time
2) The cancellation notification time should not be more than 48hours before the scheduled arrival date
3) Convey in writing the cancellation policy, including the date and time that cancellation privileges expire, to the cardholder
4) On cancellation the cruise liner merchant should provide a reservation cancellation code (if the reservation is properly cancelled). And advise the cardholder to retain it in case of dispute

Cruise reservation no-show requirements

A cruise or its third-party booking agent should not charge more than one night's lodging amount for a no-show. A no show would occur if the cardholder has not either:

1) Registered by check-out time the day following the scheduled arrival date
2) Canceled the reservation properly

Cruise reservation no-show requirements

A cruise or its third-party booking agent must inform the cardholder that one night's lodging will be billed if the cardholder has not either:

1) Registered by check-out time the day following the scheduled arrival date
2) Cancelled the reservation properly

6.7.5 Timeshare

Timeshare Merchant Category Code

Acquirers are required to ensure that the Merchant Category Code 7012, "Timeshares," is assigned to a timeshare merchant that operates sales, rentals, or other uses not including full-service lodging (i.e., maid and room service). Each authorization request must be submitted with the assigned MCC for a timeshare merchant

Timeshare reservation information

A time share merchant or its third-party booking agent must provide to the cardholder reservation information and, on the request of the cardholder, a written confirmation which includes the following information:

1) Cardholder name, PAN, and card expiration date
2) Confirmation code
3) Complete physical address of the establishment
4) Refund/cancellation and No show policy
5) Room rate, service tax and other allowed charges
6) Other details regarding the reservation

Time share reservation cancellations

For reservation cancellations:

1) A time share merchant or its third-party booking agent must accept all reservation cancellations before the specified notification time.
2) The time share merchant or its third-party booking agent must not require cancellation notification more than 72 hours before the scheduled arrival date.
3) Merchant outlet or its third-party booking agent must convey in writing the cancellation policy, including the date and time that cancellation privileges expire, to the cardholder.

Time share reservation cancellation confirmation

If requested by the cardholder, a time share merchant or its third-party booking agent must mail a confirmation of cancellation. The confirmation must include the following:

1) Cardholder name,
2) Account Number,

3) Card expiration date
4) Reservation details
5) Cancellation code
6) Other details regarding cancellation

Time share reservation amount of no-show

A time share or its third-party booking agent must inform the cardholder that one night's lodging will be billed if the cardholder has not either:

1) Registered by check-out time the day following the scheduled arrival date
2) Cancelled the reservation properly

7 RuPay Transaction Processing

7.1 Introduction

This section specifies general and member requirements for payment processing, including authorization, clearing, and settlement.

7.2 Key Principles

1) RuPay card scheme members agree to provide transaction authorization and settlement to their customers.
2) RuPay card scheme members must provide a response to authorization requests, clear and settle all messages passing through NPCInet, and report to RuPay all transactions processed on RuPay cards outside of NPCInet.
3) The issuers need to pay the acquirers for transactions properly accepted and processed by the merchants.
4) The issuers may dispute a transaction if the same is not processed in accordance with the RuPay Operating Regulations or if the cardholder disputes the transaction. Kindly refer the RuPay Dispute Management section for further details.
5) RuPay clearly defines the financial liability of each member for the various types of transaction allowed on RuPay cards, as listed in the RuPay Global Clearing and Settlement Manual.
6) RuPay defines the Interchange fee applicable to each member basis various parameters and updates the same from time to time. All members are liable to pay the applicable Interchange fee.

7.3 General Requirements

7.3.1 On Boarding With NPCI for the RuPay Card Scheme

NPCI provides both Single messaging system (SMS) and Dual messaging system (DMS) to RuPay card scheme members. All acquiring members on boarding with NPCI should have capabilities to accept and process RuPay card transactions on both, SMS and DMS. Whereas the issuing member must offer SMS or DMS capabilities basis the attributes defined in the IIN Request/Assignment form. Refer RuPay – IIN Maintenance Manual for details.

NPCI offers 99.9% uptime of their systems. All Members must ensure they have access to and maintain connectivity to NPCInet and the RGCS system to provide authorization, clearing and settlement services to RuPay cardholders and merchants.

While on boarding with NPCI and at all times during the membership tenure each participant must provide, without cost to NPCI, support requested by NPCI for establishing connectivity to the NPCInet or installing the RGCS System or any other system required by NPCI from time to time, including:

1) Providing an appropriate location for installing the NPCI system/s at the member's premises
2) Providing trained and qualified personnel to operate the NPCI systems

3) Maintaining records, documents and logs for authorization, clearing & settlement transactions as required by NPCI and providing them to NPCI at their request
4) Providing access to its premises and cooperating with NPCI and its agents for the installation, service, repair, or inspection of NPCI systems
5) Notifying NPCI promptly of any failure in accessing NPCInet or in operating any of NPCI systems
6) Develop, maintain and certify (if required) any software/hardware that may be required for the Member's systems to communicate with NPCInet and any of NPCI's systems

7.3.2 Requirement for Complete and Valid Data

All acquirers, issuers and third-party processors must ensure that all authorization requests and responses sent and the clearing messages transmitted/staged on NPCInet contain complete and valid data. The required data specifications, standards and formats are clearly defined in the RuPay – POS Switching Interface Manual and RuPay - RGCS Technical and Message specifications Manual. If data is missing or incorrect, this may lead to rejections or the non-compliant member may be subject to penalties as decided by the RuPay compliance committee on a case to case basis.

7.3.3 Fees and Charges

All members of the RuPay card scheme must pay the applicable fees and charges as specified in the RuPay Product Manual.

7.3.4 Authorization Requirements

All members should be well informed of the failure conditions listed in the RuPay – POS Switching Interface Manual. They should be aware of their responsibilities and participation in handling each of the failure conditions.

All the transaction authorized on the NPCI central switch should be authenticated by a second factor such as a PIN or any other second factor as prescribed by NPCI from time to time.

7.3.4.1 Authorization Reversal Messages

NPCI generates reversals only for time-out/late response issuer response cases. NPCI will also generate reversal in case the response from issuer fails in format validation.

An acquirer can generate reversal up to next 3 days which is validated by NPCI before forwarding the same to the issuer. If a reversal is generated after 3 days then NPCI will not send it to issuer and those reversals will be handled in RGCS.

Reversal messages follow the Store and Forward (SAF) concept and every reversal needs to be acknowledged. This principal may cause generation of multiple reversals for a transaction and it is the Issuer's responsibility to verify the reversal before posting the same to customer account.

7.3.5 Clearing Requirements

Post authorization, all members should use only the RGCS system for clearing and settlement related activities. The RuPay - RGCS Technical and Message Specifications manual and the RuPay Global Clearing and Settlement (RGCS) Manual clearly defines the formats and the process for clearing and settlement activities.

Each member is bound by the timelines to raise each clearing message defined in the RuPay Global Clearing and Settlement (RGCS) Manual.

All members need to adhere to the cutovers and timelines related to the daily clearing and settlement cycle as defined in the RuPay Global Clearing and Settlement (RGCS) Manual. NPCI will not entertain any requests to process files submitted post the defined submission cutovers.

All members are liable to honour all NPCI generated fee collection and fee disbursement messages.

All members participating in processing RuPay transactions should be capable of handling both 16 digit and 19 digit Primary Account Numbers.

Clearing Record data must be consistent with comparable data in the authorization request and authorization response.

7.3.5.1 RGCS System Usage

The RGCS system supports various clearing message types. The respective members (issuers and acquirers) should raise only the applicable and permitted clearing messages depending on and for the purpose as defined in the RuPay Global Clearing and Settlement (RGCS) Manual.

The RGCS system has two channels through which each clearing messages type can be raised, wiz Web User Interface (Web UI) or File Staging. The respective members (issuers and acquirers) should raise the clearing messages only via the permitted channel/s as defined in the RuPay Global Clearing and Settlement (RGCS) Manual.

Files staged on the RGCS will remain in the staging area for 7 calendar days after which the same will be purged by the system.

All members should ensure that all files staged via the file staging channel is named as per the file naming convention defined in the RuPay Global Clearing and Settlement (RGCS) Manual.

7.3.5.2 Interchange fees

All members are liable to pay the interchange fee as defined in the RuPay Product Manual. Further the direction, applicability and reversal of interchange fee of every transaction type will be processed as defined in the RuPay Global Clearing and Settlement (RGCS) Manual.

7.3.6 Reporting Requirements

Each member is liable to provide relevant report/s to NPCI on a timely manner, as and when requested by NPCI.

7.3.7 Purged Data

Besides unsettled authorization all transactions that have been settled and have not witnessed any further activity on them by the acquirer or the issuer post the final settlement date, for a period of 365 calendar days will be purged by the system and the same would not be available for view on the RGCS system. A member has to provide a separate written request to NPCI for any requirements pertaining to purged data.

7.3.8 Settlement Requirements

On enrolment with NPCI, all members authorize NPCI to debit/credit their settlement account/s maintained with the settlement bank (RBI) to settle the net settlement amount arrived upon by the RGCS system.

The Net settlement amount arrived upon at the end of each settlement cycle will be net off transaction amount, applicable service tax/VAT, applicable fees/charges and interchange fee.

All RuPay transactions should be settled via the RGCS system only. Members cannot settle RuPay transactions by any means outside the RGCS system.

Every member is liable to pay the applicable fees as defined in the RuPay Product Manual.

7.3.8.1 Settlement Account & Currency Requirements

All principal members must maintain a settlement account with the RBI, Mumbai for each designated settlement currency. NPCI will calculate and settle the net settlement amount only in these currencies.

A principal member must maintain sufficient funds in each settlement account to ensure smooth daily settlement activities.

A principal must have sole ownership of any of it settlement accounts it uses for RuPay settlements.

In cases of a third party processor, the ownership and funding liability of the settlement account will lie with the sponsoring member bank/s only. No third party member will have a settlement account of its own.

Settlement for each processing date of RuPay transactions will be made separately based on instructions received from NPCI. For settlements on Sundays and holidays observed by Reserve Bank of India Mumbai the settlement will be effected on the next business day as separate entries.

If NPCI cannot complete the settlement processing cycle in sufficient time to affect funds transfers, it will:
1) Postpone Settlement
2) Notify Members of the situation
3) Make Settlement on the next business day that the NPCI Settlement Bank (RBI) is open

7.3.8.2 Late Settlement Fees

A member is liable to pay a late settlement fee for each calendar day that it has been unable to meet its settlement liability as provided in the daily settlement advice. The fee would be calculated on the daily unsettled amount. The late settlement fee will be determined as per the below formula

Late settlement fee = (Number of calendar days) X (Interbank rate + 3%) X (Settlement amount) / 360

Calendar days include the day that the settlement amount was due and exclude the day that the settlement amount was made available. After NPCI receives the delayed settlement amount, the late settlement fee is collected through a NPCI fee collection message.

7.3.8.3 Settlement Financial Obligations

A member is responsible for all financial obligations owed to NPCI by any entity or subsidiary owned or controlled by the member, even if the entity is separately incorporated or in any other way legally independent of the member. NPCI may offset any amount owed to NPCI by the entity or subsidiary against the member accounts, or other owned or controlled entity globally. Member must ensure that they do not default on daily settlement to NPCI.

NPCI may, at its discretion, offset or otherwise net all or some financial obligations of or due or settlement totals of certain or all members.

NPCI may offset certain settlement and other obligations in calculating settlement amounts owed to a member. This right may be implemented by a fee collection message initiated by NPCI.

NPCI reserves the right to withhold or redirect settlement funds if it is necessary to protect NPCI or its members from risk of financial loss or damage to the goodwill of NPCI.

NPCI, under the RuPay Bylaws and the RuPay Settlement Guarantee Document, may impose financial or other obligations on a member, including financial collateral obligations to cover the member's daily settlement obligations. If a member does not satisfy financial obligations adopted under the RuPay Bylaws or the RuPay Settlement Guarantee Document, NPCI will collect those obligations through a fee collection message as part of the settlement.

7.4 Issuer Requirements

7.4.1 Authorization Requirements

7.4.1.1 Authorization Request Response

Issuer should respond to all acquirer authorization requests within a maximum of 15 seconds as defined in the RuPay - PoS Switching Interface Specifications Manual. Failing which, RuPay will respond with a decline response to the acquirer and will send a reversal to the issuer.

7.4.1.2 Cash at POS Authorizations

Issuers should not authorize Cash at POS and cash back transactions where the daily cash at POS limit exceed the applicable limits mandated by the regulator.

7.4.1.3 Monitoring Authorizations

An issuer must analyze and review their authorization records periodically and should retain the data for at least 30 calendar days.

It is recommended that the Issuers should generate exception report for following scenarios

1) Individual authorized transaction exceeding issuer pre-set limits of amount.
2) Total amount of authorized transactions exceeds issuer pre-set limit for amount.
3) Total number of authorized transactions exceeds issuer pre-set limit for count of transactions.

7.4.1.4 E-Commerce Authorization

An issuer must authenticate users by way of PIN and other parameter i.e. image code and passphrase. The Issuer must retain a log of all authentication requests & authentication records and provide the log to NPCI as and when required.

7.4.1.5 Maximum Authorization Decline Rate

RuPay would be charging member banks on business declines. The maximum level of decline responses applicable to the total number of authorization requests registered per issuer, per quarter must not be more than 5%. Issuers that register a decline response level higher than 5% may need to pay NPCI a penalty for each additional decline response, as determined by NPCI from time to time.

For computation of the authorization decline rate, decline for the below “Response codes” will be excluded:

- 05 – Do not honor
- 04 – Pick Up
- 17 – Customer Cancellation
- 33 – Expired card, capture

- 34 – Suspected Fraud, capture
- 41 – Lost Card, capture
- 43 – Stolen Card, capture
- 51- Not sufficient funds
- 54 – Expired Card, Decline
- 55- Incorrect personal identification number
- 59- Suspected fraud, decline
- 61- Exceeds withdrawal amount limit
- 65- Exceeds withdrawal frequency limit
- 75- Allowable number of PIN tries exceeded, decline

7.4.1.6 Authorization Reversal

Any issuer that receives an authorization reversal request must attempt to match the same with a previous authorization request. When matched, the Issuer should check if the matched authorization has not already been reversed. If the same has not been reversed and the account is in good standing, the issuer should credit the cardholders account immediately.

7.4.2 Clearing Requirements

On receipt of the incoming file/s from NPCI, the issuer should attempt to post the entry to its account/s upon successful matching with the authorization data.

On receipt of reversal information from acquirer, issuer must reverse the transaction from their cardholders account post necessary account checks.

7.4.2.1 Financial Obligation

Each issuer must pay the acquirer the net amount due for valid RuPay card transactions processed in accordance with the RuPay guidelines.

7.5 Acquirer Requirements

7.5.1 Authorization Requirements

7.5.1.1 IIN Range Table for Routing

An acquirer may use the IIN range table provided by NPCI to determine the routing of an authorization request. An acquirer that uses the account range table to validate RuPay cards must update the table every day or as prescribed by NPCI from time to time.

An Acquirer must not distribute the IIN range table without the prior written consent of NPCI

7.5.1.2 Incorrect Transaction Identifier

An acquirer is subject to the penalties decided by the RuPay compliance committee, if an authorization request contains data that incorrectly classifies a transaction.

For e.g.:
Wrong Merchant Category Code (MCC) assigned to merchant. e.g.: For gambling merchant category non gambling MCC assigned.
An online gambling transaction will be termed to be incorrect if it fails to include:

1) MCC 7995, Betting
2) POS condition code = 59, E-commerce request

Besides levying a penalty, NPCI may further prohibit an acquirer from contracting with any new high brand risk merchant for a period of one year or more if the acquirer has one or more non-compliant merchants identified for 4 or more months during a 12-month period.

7.5.1.3 Merchant Category Code Assignment

An acquirer must assign the appropriate merchant category code to each merchant and ensure that the assigned merchant category code is included in the authorization request and clearing message.

7.5.1.4 Merchant Descriptor

An acquirer should ensure that the merchant description in the authorizations request is accurate, valid and recognizable. NPCI will apply a fine using Fee Collection message/s for each merchant descriptor that is inaccurate, invalid, or unrecognizable in the authorization request or clearing messages. The applicable fine will be decided by the RuPay compliance committee.

7.5.1.5 Data Quality Requirements

To enable the valid identification of data, an acquirer must:

1) Ensure that all high-brand risk merchants have been correctly identified, as per the RuPay Acquirer Manual
2) Ensure that all authorization requests and clearing messages contain complete and valid data, as specified in the RuPay - PoS Switching Interface Specifications Manual, RuPay-RGCS Technical and Message Specifications Manual and the RuPay Operating Regulations

If NPCI determines that an acquirer or its merchant changed, modified, or altered any merchant information/data in any way, NPCI may:

1) Apply a fine as decided by the RuPay compliance committee per merchant, per month, to the acquirer
2) Instruct the acquirer to implement risk reduction measures
3) Prohibit the acquirer from acquiring high-brand risk merchants for a period of one year or more

7.5.1.6 Merchant Authorization Requirements

A merchant should request for a transaction authorization n regardless of the transaction amount.

Merchant is liable to accept all the RuPay cards presented except in the below scenario where merchant discretion may apply

1) Transaction is suspicious
2) Card signature panel is blank
3) Counterfeit card (RuPay card and mark specification not adhered too)

7.5.1.7 E-commerce Authorization

All e-commerce transactions should undergo 2-factor authentication using the RuPay Secure Payment Systems (RSPS). Acquirers should not process E-commerce transactions which have failed the two-factor authentication.

7.5.1.8 Monitoring Authorization

Acquirer must monitor and retain all the authorization requests processed through NPCINet for each merchant outlet on a daily basis and should retain the data for at least 30 calendar days.

It is recommended that the Acquirer should generate report for following scenarios:

1) More than 5 authorizations on an individual card holder account within a 24 hour period
2) Acquirer authorized transactions exceeds pre-set limit for transaction amount for each of their merchants within a 24 hour period

7.5.1.9 Authorization Reversal Requirements

An Acquirer must process a reversal for an online authorization if either the:

1) Acquirer, merchant, or terminal did not receive an authorization response
2) Transaction is subsequently voided or cancelled

An acquirer must send the authorization reversal request received from any of the merchant to NPCINet system.

7.5.1.10 Others

Acquirer must provide authorization, clearing and settlement service to all its merchants

Acquirer must ensure network connectivity between its or its associated Third Party's switch and NPCI central switch

Acquirer should not reject or decline any authorization request based on internal parameter set at acquirer end for specific RuPay IIN or IIN ranges or any RuPay account number

For card present authorization requests, the acquirer should ensure that track 2 of the magnetic-stripe is read and transmitted successfully along with all the data elements mentioned in RuPay - PoS Switching Interface Specifications Manual.

7.5.2 Clearing Requirements

The acquirer must submit the presentment within 7 calendar days from the date of transaction.

For cash at POS transactions the acquirer should ensure that the presented amount is same as the authorized amount.

An acquirer must initiate reversal in RGCS System for following reasons

1) To correct processing error
2) Multiple processing of transaction

7.5.2.1 Amount Requirements

For SMS transactions, depending on the MCC the Tip amount and surcharge amount in restricted to 30% and 2.5% of the authorization amount respectively. In case the Tip and Surcharge message is exceeding the above mentioned values, NPCI will reject the same.

For DMS transactions, a presentment is allowed for an amount greater than the authorization of up to INR 50,000/-.

7.5.3 Settlement Requirements

7.5.3.1 Payment to Merchants

An acquirer must pay or credit its merchant's account promptly after NPCI has completed its daily settlement fund transfer. These payments must be the same as the transaction totals, less any applicable dispute amount, discounts or debit adjustment.

8 RuPay Risk Management

8.1 Introduction

As a card scheme, RuPay is exposed to a wide variety of risks, some inherent to the system and some due to external sources. The RuPay Operating Regulations on risk management have been defined to reduce RuPay's exposure to risk. RuPay risk management is based on following key principals:

8.2 Key principals

1) To protect NPCI against any illegal, inappropriate, undesirable or unauthorized activity that may damage the RuPay brand or operations or systems, all participants in the NPCI system should adhere to the risk and fraud controls as outlined by NPCI.
2) In order to enable NPCI to effectively counter ever-evolving frauds and the associated risks and security threats, participants in the NPCI system are required to report all fraudulent activity to NPCI immediately.
3) In order to ensure the security of elements of the NPCI system, all participants having access to RuPay transaction or account information are responsible for thoroughly following payment card industry data security standards.
4) The RuPay brand protection guidelines apply to all participants of the scheme. The guidelines guide the merchants in situations where RuPay brand may be associated with illegal activities or any other activity that may have an adverse impact on RuPay brand. These include, but are not limited to, child pornography, money laundering, financing terrorist activities, financing anti-national or anti-religious societies etc.

8.3 General risk management requirements

Every NPCI member bank must have a risk management and fraud detection and control capability and function, including transaction monitoring and fraud investigation. Participants in the RuPay card scheme are required to comply with the "RuPay Fraud Security Contact" and "RuPay Member Fraud Control staff information" regulations as described below. Non-compliance would lead to a fine as determined by NPCI, for the first year and for each subsequent 12 month cycles of non-compliance.

NPCI fraud security contact

Every NPCI member must have a fraud security contact available 24 hours a day, 7 days a week.

NPCI member fraud control staff information

All NPCI member bank fraud control staff must have the authority to provide the following information to NPCI upon request:

1) Basic cardholder information
2) Details on suspicious or fraud-reported account activity
3) Lost/stolen cards information

8.4 Issuer Requirements

8.4.1 Fraud reporting

The issuer should keep in mind the following guidelines related to reporting frauds:

1) If a third-party processor is used, it is the Issuer's responsibility to ensure that fraud is being reported to NPCI completely and accurately.
2) Fraud should be reported as soon as it is detected
3) A member must report all fraudulent activity upon detection, but no later than 90 calendar days from the transaction date.
4) If the cardholder does not dispute the transaction as fraud with the issuer within the 90-days, the fraud must be reported to NPCI no later than 30 calendar days from the receipt of the dispute notification by the issuer.
5) If a member does not report its fraud, it can be subjected to fines, sanctions or an on-site NPCI audit at its expense.

Refer to the Fraud Risk Management manual for the Fraud Reporting fields

Fraud Reporting Compliance

A NPCI member is compliant with fraud reporting requirements if it:

1) Reports at least 90% of confirmed fraud activities
2) Reports at least 90% of fraud within 90 calendar days of the transaction date
3) Uses correct fraud types for at least 90% of reported fraud
4) In case of non-compliance, penalties will be levied on the member.

8.4.2 Issuer fraud programs

8.4.2.1 Issuer - Fraudulent Activity Comparison and Tracking (I-FACT)

The issuer must make efforts to reduce fraud risk in its RuPay card portfolio. The fraud activity comparison and tracking program uses a metric to quantitatively identify sensitive areas related to fraud control for issuing banks. As a part of this program, NPCI will calculate the Fraud to Sales (FTS) ratio for each RuPay issuer and publish it every month.

Threshold Limits:

3 tiers of issuing banks would be defined based on the volume of transactions. FTS for issuers would be compared with other peers within their tiers as well as at a pan-India level. The threshold limits for FTS would be kept at 150% of the Average FTS value for all issuers in their respective tier or 300% of the average Pan-India FTS value.

The calculation for FTS will be done as follows:

Let's assume that for issuer ABC, value of total transactions done in the month of February is INR 650,000,000. Also lets assume that tier average value of FTS = 3.5%, Pan-India average value of FTS = 3%
The table below details the fraudulent transactions reported in each of the months of February, March, April, May and June for the transactions with the transaction date in February 2011.

Month	Value of frauds reported for the transactions with transaction date in February 2011	Total value of frauds reported for the transactions with transaction date in February 2011	Cumulative FTS for the Month of February 2011
February	3,000,000	3,000,000	0.46
March	6,000,000	9,000,000	1.38
April	12,000,000	21,000,000	3.23
May	15,000,000	36,000,000	5.53
June	3,000,000	39,000,000	6

Since according to the number of frauds in February 2011 reported as on June 2011, the FTS exceeds 150% of the tier average, the issuer will be assumed to have failed i-Fact program.

NPCI action:
If the FTS for a RuPay issuer exceeds threshold limits, NPCI will provide warnings on a monthly basis to the issuer. NPCI will contact flagged issuers through electronic or system generated notifications.

Timelines:
In case the FTS value exceeds the threshold limit for a quarter, RuPay will provide the issuer with a work-out period of a quarter to reduce the FTS and bring it within acceptable limits. The issuer must outline a clear action plan to reduce their fraud exposure with timelines and expected outcomes. They must also consider guidelines provided by NPCI for the same. The issuer is expected to provide NPCI with monthly reports tracking the progress of their fraud control effort during this period.

Fines and penalties:
Penalties will be imposed on the issuer if its FTS exceeds threshold limits for any quarter. The value and nature of these penalties will be communicated by NPCI depending on the severity of the situation.

I-FACT for card-Not-present transactions
A separate FTS calculation will also be conducted for CNP transactions and issuers exceeding 150% of their tier and 300% of the pan-India average of CNP frauds will be penalized separately.

8.5 Acquirer requirements

8.5.1 Merchant fraud control guidelines

All acquirers must engage in at least the following risk and fraud detection activities on their merchants. The acquirers must ensure that fraud control staff and other security resources are employed accordingly:

1) Identifying the merchant employee responsible for a particular transaction using audit trails
2) Implementation of security controls to govern access to point-of-sale (POS) devices in order to track and prevent:
   - Employee collusion
   - Inappropriate use of POS devices as defined by NPCI or the Member's Merchant contract

- Acceptance of counterfeit cards where the magnetic stripe data differs from that embossed on the card

3) Ensuring full cooperation with NPCI in the course of an investigation and honor requests for all information relative to the merchant. Ensuring full cooperation with issuers as well as law enforcement agencies also.
4) Ensure termination of the merchant agreement, in case, it is determined that the merchant:
   - Poses a threat to the RuPay brand
   - Introduces a disproportionate level of fraud into the NPCI system
5) Ensure that legal action is taken to minimize losses wherever appropriate
6) If possible, hold merchant funds while the merchant is being investigated
7) Initiate criminal and legal proceedings against the merchant, if applicable

Acquirer initiatives for merchant fraud reduction and control

All acquirers must implement fraud reduction initiatives at relevant merchant outlets, including a minimum:

1) Merchant staff fraud awareness
2) Decrease in floor limits for authorization
3) Implementation of secondary cardholder identification checks
4) Implementation of CVD2 processing

Disclosures by merchants during promotions

All acquirers must ensure that the following points have been thoroughly disclosed by all their merchants:

1) All terms and conditions in case of a promotion
2) Date of commencement of charges to the customer
3) Duration of a trial period, if any, and a clear disclosure that the customer will be charged by the merchant unless (s)he refuses the charge
4) A transparent cancellation policy clearly outlining the steps a customer has to take to cancel the transaction before the end of the trial period

8.5.2 Merchant Monitoring

The acquirer should monitor its merchant's deposit and authorization activities daily. This will help in detecting any unusual patterns and help prevent frauds. This section recommends monitoring and practices to help acquirers identify merchant fraud and keep losses to a minimum.

8.5.2.1 New merchant monitoring

While the acquirer may take all the precautions and follow all the RuPay guidelines during signing-up a merchant, the acquirer still needs to be careful in the initial few days of the new merchant set-up. Acquirers need to be on the lookout for any evidence of suspicious activity associated with burst-out or other merchant fraud scams or any activity that is out of line with the merchant application and may indicate higher risks.

The acquirer should carefully monitor the merchant deposits and flag-off any unusual pattern for investigation. The suspicious activities may include:

1) **Deposit variations**: The acquirer should check for significant variations in the deposit amount or frequency.
2) **Large deposits**: When a merchant suddenly makes large deposits for settlement
3) **Suspicious authorization activity**: The acquirer should check for authorization activity of the new merchants. The merchant should check if the merchant is sending authorization requests at unusual hour or there are high declines to the authorizations submitted by the merchant

Acquirers should look for sudden changes in ownership, location, phone number, product line, or selling methods. Other signs of suspicious activity may include requests for new accounts or for additional sales equipment-such as terminals, imprinting machines, or sales transaction receipts-at new or additional locations.

8.5.2.2 Existing merchant monitoring

The acquirer should also continue monitoring the existing merchant portfolio. The acquirer should keep a track of the deposits, chargeback, refunds, transaction receipts, and authorization reports. The acquirers should conduct periodic reviews of a merchant's financial status and business operations. The acquirer should also look out for signs of suspicion like:

1) An unusual or unexpected increase in the number or amount of transactions. Likewise, a sudden re-activation of a previously inactive account.
2) A huge shift, up or down, in the average transaction size.
3) A sudden drop or stop in sales deposits.
4) Account numbers in a numerical sequence or within the same IIN. Acquirers should also track deposits over periods of a few days or weeks to check for transactions or authorizations with account numbers in a single IIN. A string of account numbers may be the first sign of fraud
5) An unusual proportion of declined transactions. This could be an indication of account testing.
6) Authorization or transaction activity that takes place after hours, when the business should be closed. After-hours sales are associated with several types of fraud, including bust-out merchants and account testing
7) Excessive credits or discrepancies between sales and credits. Acquirers should check transaction records for any discrepancies between the number and amount of sales and credits. These are often the first sign of a merchant credit scam.
8) Transactions charged against a merchant's personal account.

8.5.3 Acquirer and merchant fraud programs

8.5.3.1 Acquirer - Fraudulent Activity Comparison and Tracking (A-FACT)

A-FACT is a program for RuPay acquirers to monitor and reduce their exposure to fraudulent transactions through their merchants. As a part of the program, RuPay will track the frauds for every acquirer and benchmark it against the performance of its peers to identify if they are within acceptable limits.

Threshold Limits:

3 tiers of acquiring banks would be defined based on the volume of transactions. FTS for acquirers would be compared with other peers within their tiers as well as at a pan-India level. The threshold limits for FTS would be kept at 150% of the Average FTS value for all acquirers in their respective tier or 300% of the average Pan-India FTS value.

The calculation for FTS will be done as follows:
Let's assume that for acquirer ABC, value of total transactions done in the month of February is INR 650,000,000. Also lets assume that tier average value of FTS = 3.5%, Pan-India average value of FTS = 3%

The table below details the fraudulent transactions reported in each of the months of February, March, April, May and June for the transactions with the transaction date in February 2011.

Month	Value of frauds reported for the transactions with transaction date in February 2011	Total value of frauds reported for the transactions with transaction date in February 2011	Cumulative FTS for the Month of February 2011
February	3,000,000	3,000,000	0.46
March	6,000,000	9,000,000	1.38
April	12,000,000	21,000,000	3.23
May	15,000,000	36,000,000	5.53
June	3,000,000	39,000,000	6

Since according to the number of frauds in February 2011 reported as on June 2011, the FTS exceeds 150% of the tier average, the acquirer will be assumed to have failed i-Fact program.

NPCI action:
If the FTS for a RuPay acquirer exceeds threshold limits, NPCI will provide warnings on a monthly basis to the acquirer. NPCI will contact flagged acquirers through electronic or system generated notifications.

Timelines:
In case the FTS value exceeds the threshold limit for a quarter, RuPay will provide the acquirers with a work-out period of a quarter to reduce the FTS and bring it within acceptable limits. The acquirers must outline a clear action plan to reduce their fraud exposure with timelines and expected outcomes. They must also consider guidelines provided by NPCI for the same. The acquirer is expected to provide NPCI with monthly reports tracking the progress of their fraud control effort during this period.

Fines and penalties:
Penalties will be imposed on the acquirers if its FTS exceeds threshold limits for any quarter. The value and nature of these penalties will be communicated by NPCI depending on the severity of the situation.

A-FACT for card-Not-present transactions
A separate FTS calculation will also be conducted for CNP transactions and acquirers exceeding 150% of their tier and 300% of the pan-India average of CNP frauds will be penalized separately.

8.5.3.2 Merchant Fraud monitoring programs

8.5.3.2.1 RuPay merchant level fraud control program

Depending on the expected risk exposure and fraud history, merchants are divided among 3 different levels.

Merchant Level	Number of fraudulent transactions in a calendar month	Value of fraudulent transactions in that calendar month (INR)	Fraud to Sales ratio (FTS) in that calendar month	Other comments
Level 1: Early warning merchant	Greater than or equal to 3	Greater than 100,000	Greater than or equal to 2% and less than 4%	
Level 2: Warning and review merchant	Greater than or equal to 4	Greater than 200,000	Greater than or equal to 4% and less than 6%	These merchants need specific trainings or inspections to enable better control
Level 3: warning, review and action	Greater than or equal to 6	Greater than 300,000	Greater than or equal to 6%	An ongoing fraudulent activity at the merchant location itself in addition to poor fraud control systems. These merchants pose a huge risk to the acquirer

If within a six month period, a merchant is tagged at more than one level, the highest level within that period will be considered.

Applicability:
Merchants of all RuPay acquirers will be subject to this program. In case a merchant has multiple outlets across different locations, outlets in one location will be identified as one merchant for the purpose of this program. The outlets from other location will be termed as to be part of a different merchant.

Monitoring and Identification:
Each merchant would be monitored based on the parameters mentioned in the table above to check if they lie within acceptable limits set by NPCI. In case a merchant is unable to contain its frauds within thresholds for any month, NPCI will flag the merchant according to the table above and send a notification to the acquirer.

NPCI will notify the acquirer in case of the following:

3. NPCI may have reason to believe that the merchant is engaging in collusive or otherwise fraudulent or inappropriate activity, or
4. NPCI determines that the merchant's ratio of charge-backs, credits to sales exceeds the limits established by NPCI.

An acquirer must accept charge-backs for all fraudulent transactions that took place during the entire period in which the merchant did not comply to the NPCI valid transaction rules.

Timelines:

In case a merchant is identified as Level 3: Warning, Review and Action merchant, RuPay will provide a work-out period of one quarter after notification to reduce fraud levels for that merchant and bring them within threshold limits. The acquirer must outline a clear action plan to reduce this fraud level with timelines and expected outcomes. They must also consider guidelines provided by NPCI for the same.

The acquirer may choose to deactivate such a merchant or provide details of the action taken by them. The acquirer is also expected to provide NPCI with monthly reports tracking the progress of their merchant fraud control effort during this period.

Sample Calculation:

Let's assume that for a merchant XYZ, total sales are INR 6,500,000 in the month of February, 2011

Month	Number of frauds reported for the transactions with transaction date in the month of February 2011	Cumulative number of frauds reported for the transactions with transaction date in the month of February 2011	Value of frauds reported for the transactions with transaction date in the month of February 2011	Total value of frauds reported for the transactions with transaction date in the month of February 2011	Cumulative FTS for frauds reported for the transactions with transaction date in the month of February 2011
February	1	1	30,000	30,000	0.46
March	1	2	60,000	90,000	1.38
April	2	4	120,000	210,000	3.23
May	1	5	150,000	360,000	5.53
June	1	6	30,000	390,000	6

Since according to the frauds reported for February 2011 till June 2011, the merchant falls under Level 3: Warning, Review and Action merchant, it will be subject to the RuPay merchant level fraud control program.

Fines and Penalties:

Penalties will be imposed on an acquirer for a merchant tagged as level 3 for every quarter after the work-out period. The value and nature of these penalties will be communicated by NPCI depending on the

severity of the situation.

Exit Criteria:
The RuPay merchant level fraud control program case will be closed if the acquirer is able to bring the merchant fraud levels within thresholds for at least one quarter after the work-out period. Any subsequent identification will be treated as new cases.

8.5.3.2.2 RuPay CNP Merchant level Program

NPCI understands the significant exposure to risk that CNP transactions entails as compared to other card present transactions. The CNP Merchant Level program has been designed keeping this in mind.
Depending on the expected risk exposure and fraud history, merchants are divided among 3 different levels.

Merchant Level	Number of fraudulent transactions in a calendar month	Value of fraudulent transactions in that calendar month (INR)	Fraud to Sales ratio (FTS) in that calendar month	Other comments
Level 1: Early Warning merchant	Greater than or equal to 4	Greater than 150,000	Greater than or equal to 2% and less than 4%	
Level 2: Warning and Review merchant	Greater than or equal to 8	Greater than 300,000	Greater than or equal to 4% and less than 6%	These merchants need specific trainings or inspections to enable better control
Level 3: Warning, Review and Action	Greater than or equal to 10	Greater than 450,000	Greater than or equal to 6%	On ongoing fraudulent activity at the merchant location itself in addition to poor fraud control systems. They pose a huge risk to the acquirer

If within a six month period, a merchant is tagged at more than one level, the highest level within that period will be considered.
Merchant levels are computed from data calculated on a monthly basis for the last 4 months period and any threshold breached during the last 4 months period would qualify the merchant for this program

Applicability:
CNP merchants of all RuPay acquirers will be subject to this program. In case a merchant has both physical as well as CNP sites (E-Commerce/IVR etc.), only CNP transactions will be considered for the purpose of this program.

Monitoring and Identification:
Each CNP merchant would be monitored based on the parameters mentioned in the table above to check if they lie within acceptable limits set by NPCI. In case a merchant is unable to contain its frauds within thresholds for any month, NPCI will flag the merchant according to the table above and send a notification to the acquirer.

NPCI will notify the acquirer in case of the following:
1) NPCI may have reason to believe that the Merchant is engaging in collusive or otherwise fraudulent or inappropriate activity, or
2) NPCI determines that the Merchant's ratio of charge-backs, credits to sales exceeds the limits established by NPCI.

An acquirer must accept charge-backs for all fraudulent transactions that took place during the entire period in which the merchant did not comply with the NPCI valid transaction rules.

Timelines:
In case a merchant is identified as Level 3: Warning, Review and Action merchant, RuPay will provide a work-out period of one quarter after notification to reduce fraud levels for that merchant and bring them within threshold limits. However if a merchant has been accepting transactions which are not 2-factor authenticated (2FA), no work-out period will not be given for such merchants. The acquirer must outline a clear action plan to reduce this fraud level with timelines and expected outcomes.

The acquirer may choose to deactivate such a merchant or provide details of the action taken by them. The acquirer is also expected to provide NPCI with monthly reports tracking the progress of their merchant fraud control effort during this period.

Fines and Penalties:
Penalties will be imposed on an acquirer for a merchant tagged as level 3 for every quarter after the work-out period. The value and nature of these penalties will be communicated by NPCI depending on the severity of the situation.

Exit Criteria:
The RuPay CNP Merchant Level Program case will be closed if the acquirer is able to bring the merchant fraud levels within thresholds for at least one quarter after the work-out period. Any subsequent identification will be treated as new cases.

8.5.3.2.3 High Charge-back Rate Program

The High Charge-back Rate Program (HCRP) seeks to reduce the incidence of charge-backs for its acquirer. The program includes identifying merchants with chargeback rates higher than thresholds set by NCPI and

warning the corresponding acquirer, aiding the acquirer in reducing their exposure to charge-backs and imposing penalties in case the acquirer is unable to control charge-backs for its merchant.

Identification:
NPCI will monitor the Chargeback to Sales (CTS) ratio (the number of RuPay charge-backs received by the Acquirer for a merchant in a calendar month divided by the number of the Merchant's RuPay sales in the preceding month acquired by that Acquirer) of all their merchants and identify High Chargeback Rate Merchants (HCRMs).

Sample CTS calculation:
Consider the following figures for the illustration:

Month	January	February
Sales Transaction	95,000	95,100
Chargebacks	1200	1300
CTS (basis points)	-	(1,300/95,00) = 137

HCRM categorization:
HCRMs will be categorised into two levels:

A merchant is **Level1 HCRM** if
1) it has a CTS in excess of 50 basis points and at least 50 chargebacks in a calendar month

A merchant is a **Level 2 HCRM** if:
2) For two consecutive calendar months (the "trigger months"), the merchant has a minimum CTS of 100 basis points
3) In each of the two consecutive calendar months, the merchant has at least 50 chargebacks in each month.

The designation of Level 2 HCRM is maintained until the HCRM's CTS is below 100 basis points for two consecutive months.

Acquirer warning and penalties:
NPCI will notify acquirers of all Level 1 HCRMs and the same will be issued a warning through electronic mail or NPCI system generated notifications. The acquirers must acknowledge the warning and revert back to NPCI with an action plan to reduce the incidence of chargebacks.

In addition to a notification, acquirers of all Level 2 HCRMs will be charged with a monetary penalty on a monthly basis till the time merchants are designated as Level 2 HCRMs. The penalty will be decided by NPCI depending on the severity of the situation.

Exit Criteria:

The HCRP case will be closed if the acquirer is able to bring merchant CTS levels within thresholds. Any subsequent HCRP identifications will be treated as new cases. The acquirer can terminate an agreement with a Level 2 HCRM or reduce chargeback levels to within acceptable limits.

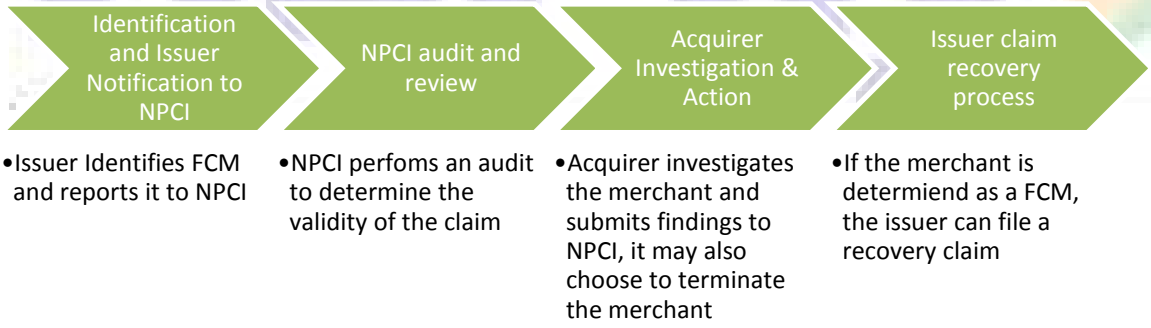
8.5.3.2.4 Cardholder-Merchant Collusion Prevention (CMCP) Program

The Cardholder-Merchant Collusion Prevention (CMCP) Program permits an issuer to file a claim against the acquirer associated with an identified fully collusive Merchant (as defined below), and to seek partial recovery for fraud losses attributable to transactions on Cardholder accounts performed in collusion with the merchant. The recovery amount value in such a situation can be a maximum one-half of the actual monetary value of fraud losses.

A merchant is termed as a **fully collusive merchant (FCM)** if it is identified to be in collusion with a cardholder beyond reasonable doubt. It is defined as someone who:

1) Presents transactions authorized by a cardholder that is in collusion with the merchant for a fraudulent intent. The transactions authorized by the cardholder should also be invalid transactions according to RuPay rules
2) Meets all of the following criteria:
   - The merchant submits at least INR XXX in transaction volume in any one month, and
   - At least 50 percent of the Merchant's Transaction volume results from collusive transactions, and
   - The merchant has been active and processing transactions for at least 30 calendar days.

The process is outlined below:



Identification and Issuer Notification to NPCI

In case an issuer believes that a Merchant is a fully collusive merchant, it must notify NPCI via electronic mail or NPCI approved system within three calendar days of such identification. The Issuer must provide the basis for its reason to believe that the said merchant is a fully collusive Merchant, supported by all of the following information:

1) Issuer and acquirer Details (Name and Member ID)
2) Merchant Details (Merchant name and complete address)
3) Collusive Transaction details:
   - Total transactions processed at the merchant site

- Total volume of losses (in INR) accrued by Issuer at the Merchant
- Percentage of collusive transactions that can be attributed to Cardholder bust-out accounts
- Details of each collusive Transaction which have been confirmed by the issuer, including Cardholder account number, Transaction date and time, and Transaction amount in INR

4) Merchant investigation report by issuer
5) Report on the Issuer's tracking system
6) Detailed report on issuer's communication regarding the merchant with the acquirer
7) Complete details of the issuer's knowledge of law enforcement involvement

The issuer will be able to file for recovery only those transactions that occurred up to 180 calendar days before the date of this notification.

NPCI Audit and review

NPCI may initiate an audit to determine whether the merchant is a FCM using the acquirer's records, at its sole discretion and upon notification by the issuer. At the initiation of an audit, NPCI will inform the security contact of each known Acquirer of the Merchant using electronic mail or through system generated notifications. NPCI may list the suspected collusive Merchant in FIND.

NPCI will notify Issuers whose accounts are believed to have been used in transactions at the Merchant being audited within seven calendar days from the date of receiving the initial Issuer notification using electronic mail or NPCI system generated notifications. All affected issuers must assist NPCI in the audit by providing all necessary documentation regarding the FCM within 30 days of receipt of request or notification. Collusive transactions on the same account are treated as separate events if they occur at different Merchant locations and must not be included in the documentation for the Merchant that is the subject of the audit.

NPCI will determine whether to declare the audited Merchant a FCM, and do the following:

1) Notify the Merchant's Acquirer in writing, and
2) Indicate that in the Merchant's FIND record

Acquirer Investigation and Action

Within a period of 15 calendar days from the date of the NPCI notification, the Acquirer must:

1) Investigate the identified Merchant, and submit required documentation to NPCI
2) Provide a record of all transaction activity at the identified merchant, including the transaction amounts, dates and times, and affected account numbers, for the 180-calendar-day period preceding the date of initial Issuer notification to NPCI.
3) Provide any other additional information that NPCI may request.

In case the acquirer determines that the merchant is a FCM, it may terminate the Merchant Agreement. The acquirer must then add the Merchant to FIND within five calendar days of the decision to terminate the merchant. The acquirer may choose to continue to acquire from the Merchant after NPCI declares it a FCM. The Acquirer must then accept liability for charge-backs with questionable merchant activity reason code at the FCM location, for a period of at least one calendar year following the identification.

Issuer Recovery Claim Process

An affected issuer will be eligible to claim a recovery as per the CMCP program if it:

1) Cooperates fully with NPCI regarding a CMCP audit by providing all information regarding the merchant either by itself or when required by NPCI
2) Reports all fraud transactions related to CMCP at the FCM once it is identified by NPCI and notified to the issuer
3) File a claim within 120 days of receipt of the NPCI notification regarding the FCM
4) Issuers must acknowledge and certify that all claims on cardholder bust-out accounts submitted are according to NPCI definitions and that:
5) All transactions occurred before the date of receipt of notification of RuPay identifying a merchant as a FCM
6) The issuer received no other recovery for any of the transactions - via any existing remedy in the RuPay system, recovery process, or the Issuer's own collection process
7) First party fraud (fraudulent application or account takeover) transactions are not included in the claim
8) Requisite cardholder screening processes as suggested by NPCI and mandated by regulatory bodies had been conducted on the cardholder account including but not limited to KYC processes and continued monitoring of the Cardholder's account.
9) The Issuer's Principal Contact must sign and date this acknowledgement and certification.

NPCI will not permit Issuers to file a recovery claim for any transaction:

1) That took place after the NPCI notification regarding that FCM
2) For which the Issuer received recovery via any existing remedy in the NPCI system, including charge-back, recovery process, or the Issuer's own collection process.

NPCI has the sole discretion regarding acceptance, reduction or rejection of any claim. NPCI will not pay claims in excess of the amount collected from the Acquirer(s) for that purpose.

8.5.4 Card Authentication requirements

NPCI has provided a string of card security features to enable multiple levels of verification before a transaction is processed. The following guidelines regarding usage of these features should be implemented.

PIN Verification

1) PIN Verification is mandatory for all ATM transactions.
2) If the Issuer performs PIN Verification, it must comply with requirements for PIN processing specified in the RuPay manuals
3) Acquirers must ensure that while handling the PIN used to identify a cardholder in a transaction, the process and technology used by the acquirer, merchant as well as its agents are compliant with the standards mentioned in the RuPay Fraud Risk Management Manual. Non-compliance to the same, will lead to penalties and assessments.

Triple Data Encryption Standards

1) All issuers must be certified to receive and process Triple Data Encryption Standard (DES) Transactions.

2) All ATMs must support Triple DES
3) All PIN-based POS acceptance devices must be Triple DES compliant
4) All transactions initiated at Triple DES-capable devices must be Triple DES-encrypted from point of acceptance to NPCI

Card Verification Data (CVD)

1) Ensure that CVD is verified in all authorization requests
2) All CVD mismatches must be reported and the reason for mismatch (acquirer error, bad magnetic stripe, counterfeit card etc.) must be determined.
3) An acquirer must ensure that the entire unaltered contents of the magnetic stripe/chip are transmitted by the merchant terminal or the acquirer can be subject to a chargeback.

CVD2

1) Ensure that the 3-digit CVD2 is printed on the signature panel of all cards.

Expiration Date

1) The expiration date may be used by merchants as an additional level of authentication and must be clearly mentioned on the card. Refer to the "RuPay Card Marks and Specifications" document for design standards for the same.
2) Verify expiration dates from authorization requests and decline most requests with mismatched expiration dates.

Hologram

1) The card must bear the RuPay hologram as an additional security feature. Refer to the "RuPay Card Marks and Specifications" document for design standards for the same.

Signature Panel

1) The signature panel provided on the card should be tamper-evident.
2) The panel must be duly signed by the cardholder failing which the card should not be accepted. Refer to the "RuPay Card Marks and Specifications" document for the signature panel design standards.

9 RuPay Dispute Management

9.1 Introduction

Dispute management is a process through which member institutions determine the validity and liability of a financial transaction

After completion of settlement process between acquiring institution and issuing institution, the issuing institution may determine that the transaction may be unacceptable or invalid for any of the reasons listed in this manual and further clearly defined in the RuPay Dispute Management Rules and Regulations manual. The issuing institution may return the original transaction to the acquiring institution as a chargeback for resolution.

9.2 Key Principles

1) RuPay issuing members should accept and honour all transactions on RuPay cards. However, they have the rights to return transactions to the acquirers for reasons specified by RuPay.
2) Members should attempt to mutually resolve disputed transactions prior to approaching RuPay to provide resolution. RuPay will act as the arbitrator for resolving any unresolved disputes.
3) Members should take appropriate actions to ensure that there is no unjust enrichment of themselves or their customers.

9.3 Acquirer Responsibility

All acquirers are responsible for the following:

1) Ensuring that presented data is accurate, complete, and in compliance with the RuPay Operating rules and guidelines.
2) Ensuring reconciliation of all rejected and accepted messages.
3) Receiving all chargeback messages that issuers submit and either:
   a) Accepting responsibility for the transactions received.
   b) Pursuing a remedy for the transactions in accordance with the rules and procedures specified within this guide.

9.4 Issuer Responsibilities

All issuers are responsible for the following:

1) Receiving all presentment messages as presented by the acquirer.
2) Ensuring that all necessary data is passed to the cardholder, or is readily accessible for transaction research and monitoring purposes.
3) Ensuring that all rejected and accepted messages are reconciled.
4) Before exercising a chargeback, the Issuer must attempt to honor the transaction. If this fails and the Issuer has already billed the transaction to the cardholder, the Issuer must credit the cardholder for the chargeback amount
5) The Cardholder/ Issuer must not be reimbursed twice for the same transaction

6) A cardholder must not be credited twice as a result of both
   a) Chargeback
   b) Refund processed by a merchant

9.5 Mutual Assistance

A member bank must attempt to offer mutual assistance to other member banks to resolve disputes between both:

1) Its cardholder and another member bank's merchant
2) Its merchant and another member bank's cardholder

If a cardholder or merchant accepts financial liability for a transaction, the related member bank must reimburse the other member bank directly through refunds, fund collection or disbursement options as applicable.

RuPay dispute resolution process entails the following stages of dispute cycle.

1) Retrieval Request
2) Retrieval Request fulfilment or Retrieval Request non fulfilment
3) Chargeback
4) Chargeback acceptance
5) Re-presentment
6) Re-Presentment acceptance
7) Pre-arbitration
8) Pre-arbitration acceptance
9) Pre-arbitration decline
10) Arbitration case
11) Arbitration case acceptance
12) Arbitration case continuation
13) Arbitration case withdrawn
14) Arbitration verdict
15) Pre-compliance
16) Pre-compliance acceptance
17) Pre-compliance decline
18) Compliance case
19) Compliance case acceptance
20) Compliance case continuation
21) Compliance case withdrawn
22) Compliance verdict
23) Bulk compliance staging
24) Good-faith
25) Good-faith acceptance
26) Good-faith decline
27) Bulk good-faith staging

9.6 Dispute Processing

All members must process dispute stages through the RuPay Global Clearing and Settlement (RGCS) system. Dispute request should be raised on RGCS system by following two methods:

1) **Web-UI :**Selecting a transaction on the RGCS system and raising the relevant dispute request
2) **File Staging:** Raising the relevant dispute request through file staging on RGCS System.
   a) Only validated files will be allowed for staging
   b) The member may select all or selective files for staging
   c) The file will remain in the staging area for 7 days, following which the file will be purged from the system

Members may do a bulk file staging for good faith and compliance stages only.

9.7 Retrieval Request

Retrieval request is a non-financial message (no transaction related fund transfer takes place between the member banks) that may be initiated only by the issuing institution to procure successful transaction related documents from the acquiring institution. The responsibility to respond/fulfill retrieval request lies with acquiring institution.

9.7.1 Retrieval Request Reasons

An issuing institution can raise a retrieval request for any of the below reason only:

1) Cardholder does not recognize the transaction
2) Cardholder disputes billed amount
3) Transaction Supporting Document (TSD) needed for cardholder's personal records expense reporting
4) For fraud /dispute investigation or legal/ regulatory issues

Once the retrieval request is processed, the same cannot be reversed.

9.7.2 Time-lines for Raising Retrieval Request

Issuing institution may raise retrieval request within 180 calendar days from the settlement of a transaction.

9.7.3 Time-lines for fulfilling Retrieval Request

Acquiring institution needs to respond to retrieval request within 30 days of initiation of retrieval request by the issuing institution.

9.7.4 Acquiring Institution Responses Options

An acquiring institution that receives a retrieval request must provide a response to the same via any of the below options

1) Fulfill the retrieval request with legible and valid transaction supporting documents (TSD)
2) Responding with Non-Fulfillment message

3) No response to retrieval request-which is deemed, declined if no response received within 30 calendar days from retrieval request initiation.

9.7.5 Retrieval Fulfilment Fees

For every retrieval request fulfillment, the acquiring institution will receive retrieval fulfillment fees from issuing institution. The retrieval fulfillment fee is based on tiered structure depending upon how soon the acquirer responds to retrieval request.
NPCI is responsible for debiting the issuing institution and crediting the acquiring institution for the applicable retrieval fulfillment fees. Net settlement between the issuer and the acquirer during the settlement cycle will include any fee transfers related to retrieval fulfillment.

In case of invalid or illegible retrieval request fulfillment the issuing institution can claim reversal through fund collection or acquiring institution can initiate fund disbursement of retrieval fulfillment fees. Additionally issuing institution may raise chargeback on the disputed transaction.

Please refer RuPay Dispute Management – Rules & Guidelines for further details on Retrieval Request.

9.8 Chargeback

After completion of settlement process between acquiring institution and issuing institution, the issuing institution may determine that the transaction may be unacceptable or invalid for any of the reasons listed in this manual or as defined in the RuPay Dispute Management Rules and Regulations manual. The issuing institution may return the original transaction to acquiring institution as a chargeback for resolution.
The acquiring institution has rights to represent disputed transactions to the issuing institution, based on NPCI defined chargeback reason codes. At every chargeback stage transaction related fund transfer will take place between issuing and acquiring institution.

9.8.1 Chargeback amount

An issuing institution must chargeback for either
1) Transaction amount or actual billed amount
2) Partial transaction amount or equal to disputed amount

9.8.2 Time limit for applicable document submission for Chargeback

Member institution sending chargeback documentation must submit the same within 5 calendar days of chargeback.
1) Member institution must submit applicable documents via RGCS only.
2) In case of non-receipt of applicable documents within the specified time period the other member can counter the dispute.
3) The liability to provide legible copy of the documents lies with the provider member institution.

9.8.3 Stages of chargeback cycle

9.8.3.1 Chargeback Stage-1

Chargeback (for Full or Partial amount)

1) Initiation member /institution: Issuing institution
2) Details: Issuing institution initiates a chargeback for the full or partial transaction amount within the specified time frame applicable to the specific message reason.
3) Time Lines: Kindly refer respective chargeback reason codes for details, as defined in the RuPay Dispute Management Rules and Regulations.
4) Remarks: Once processed, a chargeback is not allowed to be reversed.

9.8.3.2 Chargeback Stage-2

Chargeback acceptance

1) Initiation member /institution: Acquiring institution
2) Acceptance Amount: Full or Partial Amount
3) Details: Acquiring institution may accept the chargeback initiated by the Issuing institution.
4) Time Lines: Within 10 calendar days following the chargeback initiation date.
5) Deemed Acceptance: Any chargeback not re-presented within the specified re-presentment due date is deemed to be accepted by the acquiring institution.

9.8.3.3 Chargeback Stage-3

Re-presentment

1) Initiation member /institution: Acquiring institution
2) Re-presentment Amount: Full or Partial Amount
3) Details: Acquiring institution may present the transaction again to the issuing institution either to correct an earlier defect or to indicate disagreement with the chargeback raised by the Issuing institution.
4) Time Lines: Within 30 calendar days following the chargeback initiation date.
5) Re-presentment Documents: The re-presentment should be backed by all relevant documents wherever applicable and prescribed in the RuPay Dispute Management Rules and Regulations.
6) Kindly refer respective chargeback reason codes in the RuPay Dispute Management Rules and Regulations for details.

9.8.4 Chargeback categories

Issuing institution must raise chargeback only under any of the below identified categories and reasons:

Category	Reason
Goods and service related issues	Credit not processed for cancelled or returned goods and services
	Goods and services not as described/ defective

	Paid by alternate means
	Goods or services not provided/ not received
Processing error related issues	Late presentment
	Credit posted as debit
	Incorrect transaction amount or primary account number
	Single transaction processed more than once
Copy request related issues	Illegible fulfillment
	Retrieval request not fulfilled
	Invalid fulfillment
	Cardholder does not recognize the transaction
Authorization related issues	Transaction received declined authorization response
	Transaction not authorized
	Non-matching account number
Fraud related issues	Fraudulent card present transaction
	Fraudulent card not present transaction
	Fraudulent multiple transactions

Refer the RuPay Dispute Management Rules and Regulations for further details on the categories and reasons.

9.9 Re-presentment

Acquiring institution may present the transaction again to the issuing institution either to correct an earlier transaction processing defect or to indicate disagreement with the chargeback raised by the issuing institution. Re-presentment gives rights to the acquiring institution to shift the transaction liability to issuing institution.

9.9.1 Re-presentment Amount

An acquiring institution must process re-presentment for either

1) Chargeback amount
2) Partial chargeback amount

9.9.2 Time limit for applicable document submission for Re-presentment

Acquiring institution sending re-presentment documentation must submit the same with in 5 calendar days of re-presentment processing date.

1) Member institution must submit applicable documents via RGCS only.
2) In case of non-receipt of applicable documents within the specified time period the other member can counter the dispute.
3) The liability to provide legible copy of the documents lies with the provider member institution.

9.9.3 Re-presentment timelines

30 calendar days from the chargeback processing date

9.10 Pre-arbitration

When applicable, the issuing institution may use this message as a final attempt to mutually resolve the disputed transaction before an arbitration is filed with RuPay to resolve the dispute.
Though it is recommended, it is not necessary for an issuing institution to raise a pre-arbitration prior to arbitration

9.10.1Pre-Arbitration Amount

An issuing institution must process pre-arbitration for either

1) Re-presentment amount
2) Re-presentment partial amount

9.10.2Pre-arbitration raising timelines

Issuing institution must raise pre-arbitration within 15 calendar days following the chargeback re-presentment date.

9.10.3Pre-arbitration Response

An acquiring institution that receives a pre-arbitration attempt must provide their stand on pre-arbitration, using either of the below options.

1) Accept the pre-arbitration
2) Decline the pre-arbitration

No response to pre-arbitration is deemed declined if no response is received within 15 calendar days from pre-arbitration processing date

9.11 Arbitration

When the chargeback and re-presentment process fails to resolve the dispute, arbitration process allows RuPay to assign liability to member institution for the disputed transaction.

RuPay arbitration committee will review all documentation/information submitted by both member institution to determine who has final liability for the transaction.

NPCI will decide which member institution is liable for the disputed transaction. The decision taken by NPCI in case of arbitration will be final and binding on the member institutions.

9.11.1Arbitration case filing conditions

An issuing institution has the right to file arbitration case with NPCI in case of any of the following:

1) The acquiring institution accepts only the partial pre-arbitration amount but the issuing institution is of the opinion that the acquiring institution is liable for the entire pre-arbitration amount.
2) The acquiring institution declines the pre-arbitration attempt and the issuing institution has sufficient documents to prove the dispute in its favour.

3) The acquiring institution does not respond to the pre-arbitration attempt within 15 calendar day's response timeframe.
4) Acquiring institution re-presentment was not valid or the cardholder still disputes the transactions.

Pre-arbitration is not a mandatory step before arbitration. The issuing institution may directly file for arbitration with NPCI after the re-presentment stage itself.

9.11.2Arbitration Amount

An issuing institution may process arbitration for any one of the following
1) Re-presentment amount
2) Pre-arbitration amount
3) Re-presentment partial amount
4) Pre-arbitration partial amount

9.11.3Arbitration timelines

Issuing institution must raise arbitration request with NPCI within 60 calendar days following the re-presentment date.

9.11.4Arbitration case response from Acquiring institution

The acquiring institution must respond to the arbitration case filing within 15 days from arbitration received date in any of the following ways:
1) Acquiring institution can accept the arbitration case
2) Acquiring institution can choose to continue with the case
3) If the acquiring institution does not respond to the arbitration case filing within 15 days from arbitration received date, the case is termed as 'to continue'.

9.11.5Arbitration case withdrawal

Issuing institution can withdraw arbitration case within 15 calendar days from arbitration raising date.

9.11.6Arbitration response timelines

RuPay arbitration committee would respond with a verdict within 60 calendar days following the arbitration initiation date.
No ruling would be taken by the RuPay arbitration committee in the first 15 calendar days following the arbitration initiation date, to allow issuing institution to withdraw arbitration case or acquiring institution to accept or to continue the arbitration case.

9.12 Pre-Compliance

When applicable, a member that has no chargeback, re-presentment, pre-arbitration or arbitration right may use pre-compliance as a final attempt to file a complaint against another member for violation of the RuPay operating regulations, before compliance is filed with RuPay to resolve the dispute.

1) Pre-compliance is not a mandatory step before compliance. However, the requesting member must attempt to resolve the dispute with the opposing member through pre-compliance
2) Pre-compliance can be raised by either the issuing institution or acquiring institution

9.12.1Pre-compliance Filing Conditions

A member may file for pre-compliance if all of the following conditions are true:

1) There was a violation of the RuPay rules or regulations
2) The filing member has no chargeback or re-presentment right. This means that the violation cannot be remedied using any chargeback or re-presentment reason code
3) The filing member can document a financial loss because of the violation and not simply assert a violation as a basis for filing the case. In other words, the loss could have been avoided if the other member or affiliate had followed the rules

9.12.2Pre-compliance amount

Member institution must process pre-compliance for either

1) Transaction or settlement amount
2) Partial transaction or settlement amount

9.12.3Pre-compliance raising timelines

Initiating institution must raise pre-compliance within 365 calendar days of settlement of transaction.

9.13 Pre-compliance response timelines

Receiving institution must respond within 15 calendar days following the Pre-compliance receipt date

9.13.1Pre-compliance Response

Receiving institution has the following 3 options once the pre-compliance is received

1) Accept Pre-compliance (full or partial)
2) Decline Pre-compliance
3) No response within 15 calendar days from the Pre-compliance receipt date, which will be deemed declined

9.14 Compliance

When applicable, a member that has no chargeback, re-presentment, pre-arbitration or arbitration right may use compliance as a final attempt to file a complaint against another member for violation of the RuPay operating regulations.

If the initiator is unsatisfied with the pre-compliance response from the opposing member, the initiating member may file compliance case with NPCI to provide a decision on the disputed matter.

RuPay compliance committee will review all documentation/information submitted by both member

institution to determine who has final liability for the transaction.

NPCI will decide which member institution is liable for the disputed transaction. The decision taken by NPCI in case of compliance will be final and binding on the member institutions.

9.14.1Compliance Filing Conditions

A member may file for compliance if all of the following conditions are true:

1) There was a violation of the RuPay rules or regulations.
2) Member has no chargeback or re-presentment right. This means that the violation cannot be remedied using any chargeback or re-presentment reason code.
3) The filing member can document a financial loss because of the violation and not simply assert a violation as a basis for filing the case. In other words, the loss could have been avoided if the other member or affiliate had followed the rules.

The member will have no compliance rights in case an earlier retrieval request was not responded to.

9.14.2Compliance case filing reasons

The initiating institution has the right to file compliance case with NPCI in case of any of the following:

1) The receiving institution accepts only the partial pre-compliance amount but the initiating institution is of the opinion that the receiving institution is liable for the entire pre-compliance amount.
2) The receiving institution declines the pre-compliance attempt and the initiating institution has sufficient documents to prove the dispute in its favour.
3) The receiving institution does not respond to the pre-compliance attempt within 15 calendar day's response timeframe.

9.14.3Compliance amount

Member institution must process compliance for either

1) Pre-compliance amount
2) Partial pre-compliance amount
3) Transaction settlement amount
4) Partial transaction settlement amount

9.14.4Compliance timelines

Initiating institution may raise compliance request with NPCI within 365 calendar days following the transaction settlement date

9.14.5Compliance case response from receiving institution

The compliance case receiving institution must respond to the compliance case filing within 15 days from compliance received date in any of the following ways:

1) Acceptance
2) Continuation
3) If the receiving institution does not respond to the compliance case filing within 15 days from compliance received date, the case is termed as 'to continue'.

9.14.6Compliance committee response timelines

RuPay compliance committee will provide decision within 60 calendar days following the compliance initiation date.
No decision would be taken by the RuPay compliance committee in first 15 calendar days following the compliance processing date, to allow initiating institution to withdraw compliance case or receiving institution to accept the compliance case.

9.15 Good-faith

A good faith process is an attempt to resolve transaction supported by RuPay Global Clearing and Settlement System (RGCS). Good-faith allows the member that has no presentment, chargeback, re-presentment, arbitration, or compliance right to make a mutual attempt to resolve its card member's dispute or any other transaction related disputes.

RuPay dispute management system enables the members to raise good faith and respond to the good faith attempt initiated by the other member. Good faith can be raised by either the issuing or acquiring institution.

The decision to accept or reject the good faith attempt solely lies with receiving institution. NPCI shall have no role and responsibility in case of good faith raised by a member and cannot be approached to give a ruling.

In case of good faith decline by the receiving institution, no additional rights are left with the initiating institution and NPCI is not bond to resolve the issue.

9.15.1Good faith filing condition

Good-faith allows the member that has no presentment, chargeback, re-presentment, arbitration, or compliance right to make a mutual attempt to resolve its card member's dispute or any other transaction related disputes.

Receiving institution is not bound to respond the good faith attempt, but if the good faith attempt is valid, the receiving institution should accept the good faith.

9.15.2Good faith amount

Initiating institution can process good faith for either

1) Transaction or billed amount
2) Partial transaction or billed amount

9.15.3Good faith timelines

Initiating institution can raise good faith request within 365 calendar days of settlement of transaction.
Member institution can also raise good faith for transactions older than 365 through off line mode. In off line mode processing of good faith will not be done through RuPay RGCS System.

9.15.4Good faith case response from receiving institution

The good faith receiving institution must respond to the good faith attempt within 30 days from good faith received date in any of the following ways

1) Acceptance
2) Decline
3) No Response

9.16 Purchase with Cash-Back at Point of Sale (POS)/Cash at Point of Sale (POS)

Purchase with cash-back transaction is a face to face (Card present) transaction where the cardholder uses the card for cash back in conjunction with a retail purchase. Cash at point of sale is a face to face (Card present) transaction where the cardholder uses the card only for cash disbursement at Point of sale (with retail purchase amount as zero). 'Cash-Back' below refers to either Purchase with cash-back or cash at point of sale.

9.16.1Disputes on Cash-Back portion of the transaction

Issuing institution cannot raise chargeback on cash-back portion of the transaction under the following chargeback reason codes.

1) Credit not processed for cancelled or returned goods and services
2) Goods and Services not as described / defective
3) Paid by alternate means
4) Goods or Services Not Provided / Not Received

For rest of the chargeback reason codes mentioned above and clearly defined in the RuPay Dispute Management Rules and Regulations, the chargeback can be raised for the full transaction amount including cash portion of the cash-back transaction.

10 RuPay Pricing, Fee and Interchange

10.1 Introduction

This section contains guidelines and information for issuing or acquiring member participating in the RuPay card scheme. It outlines the requirements, procedures and other service standards to be followed by a member for pricing, fees and interchange setup for RuPay brand products.

10.2 Key Principles

1) **Fees for access and use of RuPay products and services:** RuPay card scheme members pay fees to NPCI for access to and use of RuPay products and services. NPCI establishes certain fees between issuers and acquirers for specific actions. All members are liable to pay these fees and authorize NPCI to recover the same during the daily settlement.
2) **Paying or receiving interchange:** All RuPay acquirers and issuers pay or receive interchange every time a RuPay product is used. The direction (paying or receiving member) of the interchange and the amount payable is defined by RuPay and is payable by one member to another.
3) **RuPay liability:** RuPay applies interchange fees as part of the clearing and settlement process and does not keep any part of the interchange fee for itself. The interchange fee scheduled is modified by RuPay from time to time. The interchange fee is based on several factors which primarily includes card type, merchant type, transaction type and many others. Further details on the applicable interchange fee amount and parameters can be referred from the RuPay Product Manual.

10.3 Interchange Fee

10.3.1 What is Interchange?

Interchange is a fee charged to the acquiring bank for payment to the issuing bank to facilitate the various services and benefits offered to the cardholders, in order to increase usage at merchant locations.

Interchange is established to incentivize banks to issue payment cards and merchants to accept those cards. It is a small fee paid by an acquiring institution to an issuing institution and serves to compensate the issuing bank for a portion of the risks and costs it incurs to maintain cardholder accounts.

These costs include finance costs for the interest free period between the time a consumer makes a purchase and pays his/her bill, credit losses, fraud protection and processing costs.

By shifting some of the cost of the payment system from issuers and their cardholders to acquirers and their merchants, NPCI can encourage greater utilization of the RuPay cards. Often referred to as “balancing the system” this makes the system more efficient and valuable to cardholders and merchants. When a purchase is made with a RuPay card, the acquiring institution pays the issuing institution an interchange fee to help offset a portion of these costs. The acquiring institution eventually collects this fee from the merchant as a component of the merchant discount rate (MDR).

10.3.2Interchange Fee Parameters

RuPay Interchange rates are established by NPCI, and are generally paid by acquirers to card issuers on purchase transactions and by card issuers to acquirers in case of cash at POS (for the cash portion), chargeback etc. Interchange rates are only one of many cost components included in a MDR, and are a necessary and efficient method by which NPCI maintains a strong and vibrant payments network. Setting interchange rates is a challenging proposition that involves an extremely delicate balance. If interchange rates are set too high, such that they lead to disproportionately high MDRs, merchants' desire and demand for RuPay card acceptance will drop. If interchange rates are set too low, card issuers' willingness to issue and promote RuPay card will drop, as will consumer demand for such cards.

10.3.3Direction of Interchange

The interchange fee is paid by either the acquiring or issuer depending on the type of transaction being processed through the RGCS. There are certain transaction types that do not effect a movement of interchange fee between members. The comprehensive list of all the transaction types and the applicability and direction of interchange fee between members is as defined in the RuPay Global Clearing and Settlement Manual.

10.4 NPCI Charges

10.4.1Broad Pricing Principles

NPCI determines the pricing for member banks issuing, acquiring or processing RuPay card transactions. The broad pricing principles influencing RuPay pricing are as follows:

1) The pricing structure should be simple and clearly defined so that it is easy for the members to comprehend
2) The pricing should contribute positively to the member banks in the growth of their cards business

10.4.2Major Price Heads

The major price heads under which NPCI may levy charges and the applicability and rationale of each head is provided below:

1) **Administrative Fees:** This is a monthly fee that may be charged to all members. This fee is to cover various administrative aspects of the functioning of the scheme
2) **Assessment Fees:** This fee may be charged for using the RuPay brand for merchant transaction. NPCI may recover the marketing initiatives expenses through this charge. The assessment fees may be charged as a percentage to the total transaction volumes over POS and non ATM transactions
3) **Authorization Charges:** These charges are meant to recover the expenses for authorizing a transaction over the network and may be charged as a flat fee per transaction, including business declines
4) **Clearing and Settlement Charges:** NPCI may charge a flat fee for all transactions processed by the NPCI network using the RuPay Global Clearing and Settlement (RGCS) system. Dispute management and adjustments done per transaction may form part of the transaction processing fees

5) **Member Audit Charges:** These fees may be charged to the members for auditing their systems on a cost plus basis
6) **Training Fees:** RuPay scheme may charge its member banks for recovering the costs for imparting training on a cost plus basis
7) **Certification Fees:** NPCI may charge its member banks for recovering the costs for conducting different certifications, on a cost plus basis
8) **Arbitration/Compliance Charges:** In case a dispute does not get resolved between member banks, the final step will be to approach NPCI via the arbitration process. NPCI may charge a filing fee and a review fee to the members to recover the costs involved in managing the entire arbitration process
9) **Retrieval Request Charges:** In a retrieval request charge the acquirer is paid the amount upon fulfilling the issuer's request for information on a particular transaction

For details on the RuPay pricing, please refer the RuPay Product Manual.

10.4.3Other Pricing Considerations

1) NPCI has the right to relax or waive charges
2) The defined charges could be for a fixed amount or an ad-valorem amount or a combination of both
3) The fees structure, frequency and applicability are at the discretion of NPCI and any revision will be communicated to the member.
4) The above mentioned price points are not inclusive of taxes
5) NPCI will decide on fines and Penalties as per the recommendations of the RuPay compliance committee.

11 RuPay Liability

11.1 Introduction

This section clearly identifies the conditions and liability of RuPay, issuers and acquirers under various transaction conditions.

11.2 Key Principles

1) Under different transaction conditions, the member banks (issuer or acquirer) will have to take the liability for the transaction conducted
2) The member banks should accept the transaction liability if the conditions laid down in this section are applicable to the transaction

11.3 Liability Classification

The liability in the RuPay network can be classified as below:

1) Liability for non-EMV Card and non-EMV terminal
2) Specific provisions for Offline and Key entry terminals
3) Specific provisions for Fraudulent transactions

Liability of Card-Present RuPay card transactions if service code is 126 or 520

1) For international transactions: If the merchant accepts a PIN preferring magnetic stripe card (service code 126) and processes the transaction on a magnetic stripe/Chip terminal (POS Entry 90), but processes the transaction based on the cardholders signature and does not take the PIN inspite of the presence of a PIN pad, then the issuer will be liable for the transaction if the issuer authorizes the transaction knowing that the transaction has been processed using a signature and no PIN has been provided
2) For domestic transactions: If the PIN only card (service code 520) transaction is processed on a magnetic strip/Chip terminal (POS Entry 90) using the PIN provided by the cardholder, then the issuer will be liable for the transaction and will no chargeback right under the Card-present fraud reason code

Specific provisions for the Offline and Key Entry Transaction Conditions

1) If the merchant/acquiring bank completes a magnetic-stripe or chip transaction with or without PIN either through magnetic swipe or key entered and the service code indicates 'X2X Positive Authorization' without obtaining authorization from the Issuing Bank and submits the settlement details directly, then the acquiring bank will be liable for the transaction and will have no representment rights for X2X Chargeback dispute

Specific provisions for Fraudulent transactions

1) If the issuing bank validates the PIN provided by the cardholder during a transaction using magnetic stripe swipe at POS and PIN, then the issuing bank will be liable for the fraud types lost, stolen, counterfeit, never received card, account takeover and e-commerce transactions

12 Glossary

Abbreviation	Description
AEPS	Aadhaar Enabled Payment System
APBS	Aadhaar Payment Bridge System
ACS	Access Control System
ATM	Automated Teller Machine
ATL	Above The Line
ARD	Acquirer Reference Data
API	Application Programming Interface
AP	Access Point
ACQ	Acquirer
ACH	Automated clearing house
AML	Anti-Money Laundering
AID	Acquirer ID
BIN	Bank Identification Number
BCP	Business Continuity Planning
B2B	Business-to-business
B2C	Business-to-consumer
BPSS	Board for Regulation and Supervision of Payment and Settlement systems
BTL	Below-The-Line
BIS	Bureau of Indian Standards
CVD	Card Verification Data
CVD 2	Card Verification Data-2
CB	Chargeback
CNP	Card not present
CP	Card present
CPC	Cheque Processing Centre
CPP	Common Purchase Points
CoD	Card/Cash on Delivery
CBCH	Chennai Bankers' Clearing House
CTS	Cheque Truncation System
CTR	Chargeback to Transaction Ratio
CIM	Chargeback Identified Merchant
CMYK	Cyan, Magenta, Yellow & Key (Black)
CCIL	The Clearing Corporation of India Limited
CCN	Clearing Cycle Number
CHI	Clearing House Interface
CAF	Card Acceptance Forum
CCTV	Closed Circuit Television
DSP	Dispute
DES	Data Encryption Standard
DTD	Document Type Definitions
DSE	Data Storage Entity
DOM	Domestic

DMS	Dual message system
DSS	Data Security Standard
DR	Disaster Recovery
E-COMM	Electronic Commerce
EDC	Electronic Data Capture
ECS	Electronic Clearing Service
EMV	Euro pay, MasterCard and VISA
EMS	Environmental Management Systems
ECCS	Express Cheque Clearing System
ERM	Enterprise Risk Management
FTS	Fraud-to-Sales
FEMA	Foreign Exchange & Management Act
HTTP(S)	Hyper Text Transfer Protocol (Secure)
HSM	Host Security Module/ Hardware Security Module
HCRM	High Chargeback Rate Merchant
ICS	International Card Scheme
IC	Integrated Circuit
ISS	Issuer
ISP	Internet Service Providers
IDS	Intruder Detection System
IMPS	Interbank Mobile payments service
IVR	Interactive Voice Response
INTL	International
IIN	Issuer Identification Number
ISMS	Information Security Management Systems
IDRBT	The Institute of Development and Research in Banking Technology
IQA	Image Quality Assurance
ISO	International Organization for Standardization
ITCC	Income Tax Clearance Certificate
IPR	Intellectual Property Rights
IPSP	Internet Payment Service Provider
JPEG	Joint Photographic Experts Group
JD	Julian Date
KYC	Know Your Customer
LRC	Longitudinal Redundancy Check
MTI	Message Type Identifier
ME	Merchant Establishment
MCC	Merchant category code
MO/TO	Mail Order/Telephone Order
MMT	Member Message Text
MRN	Member Reference Number
MIS	Management Information System
MMID	Mobile Money Identifier
MPIN	Mobile PIN
MAS	Mobile Account Selector

MTI	Message Type Identifier
NPCI	National Payments Corporation of India
NECS	National Electronic Clearing Service
NFC	Near-field communications
NFS	National Financial Switch
NEFT	National Electronic Fund Transfer
NBIN	National Bank Identification Number
NDA	Non-Disclosure Agreement
NOC	No Objection Certificate
OHSMS	Occupational Health and Safety Management Systems
POS	Point of Sale
PCI DSS	Payment Card Industry Data Security Standards
PID	Participant ID
PIN	Personal Identification Number
PAN	Primary Account Number
P2P	Person-to-person
P2F	Paper to Follow
PSD	Payment Services Directive
PSP	Payment Service Provider
PA-DSS	Payment Application Data Security Standard
PTS	PIN Transaction Security
PG	Payment Gateways
PPS	Perimeter Protection System
PDF	Portable Document Format
PCE	Personal Consumption Expenditure
PED	PIN Entry Device
QM	Quality Management
QA	Quality Assurance
QMS	Quality Management Systems
RBI	Reserve Bank of India
RRB	Regional Rural Banks
RGCS	RuPay Global Clearing and Settlement
RRN	Retrieval Reference Number
RR	Retrieval Request
RTGS	Real Time Gross Settlement
RoC	Registrar of Companies
SBIN	Settlement BIN
SWIPS	System-Wide Important Payment System
SSID	Service Set Identifier
SCB	Scheduled Commercial Banks
ST	Service TAX
STIP	Stand in Processing
SMS	Single Message System
SNMP	Simple Network Management Protocol
SWIFT	Society for Worldwide Interbank Financial Telecommunication

SSL	Secure Sockets Layer
SGF	Settlement Guarantee Fund
SBIN	Settlement BIN
TIFF	Tagged Image File Format
TID	Terminal ID/Transaction ID
TCC	Transaction Category code
TAT	Turnaround Time
TXN	Transaction
TPP	Third Party Processors
TSD	Transaction Supporting Document
UID	Unique Identification
UCB	Urban Co-Operative Bank
URL	Uniform Resource Locator
XML	eXtensible Markup Language
VPN	Virtual Private Network
VaR	Value at Risk
Wi-Fi	Wireless Fidelity
WPA	Wi-Fi Protected Access
WEP	Wired Equivalent Privacy
Web UI	Web User Interface