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)