POLICY ON DIGITAL PRODUCTS & SERVICES FOR FY 2021-22

VERSION 1.1

DIGITAL BANKING DIVISION

This Policy supersedes and replaces the “Policy on Digital Products & Services for FY 2020-21 version 1.0”

Version Control

Policy Certification

Title	**POLICY ON DIGITAL BANKING PRODUCTS AND SERVICES**
Version	**1.1**

Owned By:	**Digital Banking Division**
Prepared By:	**Digital Banking Division**
Reviewed By:	**Audit Committee of Board**
Approved By:	**Board**
Effective From:	**01 April 2021**

Version Control:

Version No.	Prepared By	Approved By	Effective Date
1.0	Digital Banking Division	Board	01.04.2020

Changes during the year:

Date of Issuance	Circular No.	Circular Name

CONTENTS

1. Purpose of the Policy 7
2. Scope of Policy 7
3. Objectives of the Policy 8
4. Digital Products & Services 8
4.1 Credit Cards 9
4.1.1. Card Issuance and Basic Features 10
4.1.2. Credit Card limits & Sanctioning Authorities 13
4.1.3. Credit Period, Billing & Interest rates 17
4.1.4. NPAs & Recovery Measures 19
4.1.5. Internal control & monitoring systems 27
4.1.6. Compliance to RBI Guidelines and Other Standards 27
4.1.7. Disclosure in Balance Sheet 31
4.1.8. Disclosure to rating Agencies and others 31
4.1.9. Customer Service 32
4.1.10. Eligibility Criteria, Features & Card Limits 33
4.2 Merchant Acquisition and Digital Services 43
4.2.1. Merchant Acquisition 43
4.2.2. Digital Services 47
4.2.3. Roles & Responsibilities 49
4.2.4. Payment gateway service to merchants 49
4.2.5. Charges for Services & Waivers 51
4.2.6. Security & Risk Mitigation 55
4.2.7. Customer Service 55
4.2.8. Outsourcing: 56
4.2.9. Procurement/ Payment 57
4.3 Internet / Mobile Banking 57
4.3.1. Benefits 61
4.3.2. Fund Transfer Limits 62
4.3.3. Roles & Responsibilities 64
4.3.4. Standards & Guidelines 65

4.3.5. Privacy Policy 71
4.3.6. Audit & Compliance 73
4.3.7. Disclaimer Clause 74
4.3.8. Third Party & Outsourcing Services 76
4.3.9. Termination / Suspension / Withdrawal of service 79
4.4 Debit Cards 80
4.4.1. Eligibility Criteria for issuing Debit Cards 81
4.4.2. Guidelines for issuing & delivery of cards through DCMS 84
4.4.3. Security & Risk Mitigation 86
4.4.4. Co-branded Debit Cards 89
4.4.5. Processing of e-mandates for recurring transactions 90
4.5 Prepaid Cards 92
4.5.1. Definition & Classification 92
4.5.2. Issuance, Loading & Reloading 94
4.5.3. Validity, Redemption, Limits and Refund 95
4.5.4. Categories of PPIs permitted by RBI: 96
4.5.5. Security and Risk Mitigation 99
4.5.6. Compliance to RBI Guidelines and Other Standards 102
4.5.7. Customer Service 108
4.5.8. Co-branded PPI Cards 110
4.5.9. Information System Audit and Interoperability 111
4.6 Daily Limits for Debit Card Transactions 115
4.6.1. Debit Card Products and Defined Limits 115
4.6.2. Applicability of Limits 117
4.6.3. Review of Limits 123
5. Role of Internal Auditor 124
6. Review of the Policy 124
7. Annexures 125
7.1 Approval for PPI issuance by Bank (PPI issuance by Indian Bank) 125
7.2 Reconciliation of Digital Transactions 126
7.3 Ombudsman Scheme for Digital Transactions, 2019 126

7.4 RBI Circular on Card Tokenization 129
7.5 RBI Circular on storage of all payment data in India 130
7.6 Harmonisation of Turnaround Time (TAT) and customer compensation for failed transactions using authorised Payment Systems 131
7.7 RBI Master Circular on "Mobile Banking Transactions in India" 135
7.8 RBI Circulars on Merchant Acquisition 135

1. Purpose of the Policy

Our Bank is fast growing in the digital banking business through the following products and services:

- Internet Banking, Mobile Banking & UPI
- Merchant Acquisition on POS, Aadhar Pay, Payment Gateway Services, QR etc.
- Digital Service – FASTag
- Debit Cards, Credit Cards & Pre-paid cards

Digital Banking Division (DBD) is the owner of the policy and its endeavour is to cater to the business requirements of the bank, thereby contributing to the growth and profit of the Bank through Digital and Government Business, through tailor-made products and services which not only enhance customer experience but also earn low cost deposits and Non Interest Income to the bank

2. Scope of Policy

The policy covers various aspects of the following products and services:

1. Credit Cards
2. Merchant Acquisition and Digital Service
3. Internet Banking/Mobile Banking
4. Debit Cards
5. Pre-paid Cards
6. Daily limits for Debit Card Transactions

3. Objectives of the Policy

To cope up with the changes in digital banking trends and financial technology landscape, and to provide best in class digital products and services, continuous efforts are being made to align the digital products and services on par with the latest innovations in digital banking as detailed in the "*Report of the Working Group on FinTech and Digital Banking*" released by Reserve Bank of India.

To have control over the development, delivery and usage of our Bank's digital banking products, the policy on Digital Banking Products & Services is prepared and approved by the Board for FY 2021-22

4. Digital Products & Services

The policy mainly covers following section and is aligned with various RBI guidelines and reports on the Digital Banking:

- Credit Cards
- Merchant Acquisition and Digital Service
- Internet Banking/ Mobile Banking
- Debit Cards
- Prepaid Cards
- Daily Limits for Debit Card Transactions

4.1 Credit Cards

Reserve Bank of India has observed in the Master Circular on Credit Card Operations dated 01.07.2015 that it is important for banks to maintain prudent policies and practices for managing the risks of their credit card business in view of the following reasons.

- The quality of banks' credit card portfolios mirrors the economic environment in which they operate.
- Often, there is a strong correlation between an economic down turn and deterioration in the quality of such portfolios.
- The deterioration may become even more serious if banks have relaxed their credit underwriting criteria and risk management standards as a result of intense competition in the market.

The Banking Codes and Standards Board of India (BCSBI) have released the latest "Code of Bank's Commitment to Customers" (Code) in January 2014, which has been adopted by our Bank.

As our Bank is subscribing to the BCSBI Code, the principles contained in BCSBI Code are adopted in the policy on credit card operations besides incorporating the guidelines contained in the Master Circular No RBI/2015-16/31 DBR.No.FSD.BC.18/24.01.009/ 2015-16 dated July 1, 2015.

The Policy Document on Credit Card Operations has been prepared with a view to consolidate and provide a framework for guidelines and practices adopted by the Bank in its Credit Card Operations. This will facilitate a better understanding of 1) Credit Card Operations in the Bank and 2) the need to ensure that prudent policies and practices are adopted while issuing Credit Cards.

4.1.1. Card Issuance and Basic Features

- Banks with net worth of Rs. 100 Crores and above can undertake credit card business for which no prior approval of RBI is required. Credit Card Business in the Bank is managed at Corporate Office, Credit Card Centre (CO: CCC).As per the RBI Master Circular on Credit Cards, Banks are permitted to issue Co-branded Credit Cards and while issuing Co-branded Credit Cards, banks must undertake due diligence on the non-banking entity to protect themselves against the reputation risk to which bank is exposed to in such an arrangement. Our Bank can also issue Co-branded Credit Cards to our customers under tie up arrangement with other reputed Cards & Payments Service/ NBFC. The NBFC through which Co-branding arrangement is in place, to adhere to the RBI guidelines contained in circular RBI/2006-07/196 dated 04.12.2006.

- Bank will assess independently the credit risk and ensure prudence while issuing credit cards to persons, especially to students and others with no independent financial means.
- Details of the Credit Card functionalities handled is as detailed below

Department	**Functionalities**
CO:RAD	Will be the owner of Credit Card Policy. All Business Related Decision including Fixing of Credit Card Limits, Interest rates and charges, Portfolio Management, Maintenance of Asset Quality and NPA Management, Handling business related Customer Complaints
CO:DBD	All Technology related functionality including

	Issuance of Cards & Pin mailers, providing necessary Hardware & Software support, Card Billing, Handling Transactions & Reconciliation and Redressal of Customer Complaints relating to Issuance of Card and Billing and Transactions

- Bank issues General Purpose Credit Cards in association with M/s Visa International as its Primary Member. Following variants of Visa cards & Rupay Cards are offered in the Personal Card segment:

VISA	RUPAY
Global Gold Card Global Platinum Card Domestic Bharat Card Secure Card	Classic Card Platinum Card Select Card Secure Card

- Issuance of Fresh VISA Global Classic card is withdrawn. During renewal of existing Global classic cards, Global Gold cards will be issued.
- Bank is also issuing IB Visa& Rupay Business Credit Cards to the Business entities for their Employees/Executives of SMEs, Trusts and Corporate Customers to take care of the corporate requirements.
- Bank can also issue, Credit Cards of other Card Associations through same or different vendor, covering all products suite offered by the card association. The eligibility selection/fixation of Credit Card Limit will be common to cards issued by Indian Bank through all Card Association. The revised policy will be applicable for all Credit Cards launched and to be launched by Credit Card Centre.

- No Credit cards should be issued to the customers whose credit cards were before closed under One Time Settlement.

Card Schemes

1. Introduction of New Credit Cards to customers for use in India as well as foreign countries as a business continuity plan and as an alternative to the existing VISA credit card.
2. Issuance of New Credit Cards for all new customers and while renewing the cards of existing customers after getting their consent.
3. Continue with the present practice of issuing VISA Credit Cards to HNIs who widely travel abroad as a practical approach.

- Supplementary cards (also referred as 'add-on cards') are issued to another individual who is an immediate family member (spouse /children/ brothers /sisters /parents) of all card holders.

- While issuing cards, the most important terms and conditions for issue and usage of a credit card should be mentioned in clear, unambiguous and simple language (preferably in English, Hindi and the local language) comprehensible to a card user and should be made available in the Welcome Kit and will also be published in Bank's Web.

Revolving Credit

Credit Card holders are given the option of revolving credit by paying at least the Minimum Amount Due as indicated in the Billing Statement mailed to them.

Bank shall provide EMI facility for specified purchases based on the requests received in writing by mail or email from primary card holders up to the

credit card limit. The modalities of the scheme shall be framed by COLCC (GM) in consultation with existing/new service provider. On extending the facility to card holder(s), the applicable ROI shall be as per 4.1.10.

4.1.2. Credit Card limits & Sanctioning Authorities

Assessment of Card Limits

Application of two different Scoring Models, one for customers and the other for Non-customers, approved by CO: Risk Management Dept factoring in various aspects of customer profile and risk perceptions and giving due weight age to the Business connections of the applicant shall be adopted for assessing the credit rating.

GM (RAD) is authorized to approve/add/modify the models for arriving eligible limits as per the business requirements.

Credit Information Companies (CICs) {that has obtained certificate of Registration from RBI} verification based on details furnished in the application shall be carried out for all card accounts.

Based on the CICs' information & score level, Cards will be approved pro-actively (for CIBIL it is minimum score of 630 for customers and 700 for non-customers & Corresponding Scoring for other CICs).

Zonal Managers & DGM (RAD) are vested with powers to consider deviations on a case to case basis

Credit Card Limits & Sanctioning Powers of various Authorities

The credit limits for various variants of Credit Card are given in 4.1.10 of the Policy

Delegation of powers for sanctioning Credit Card limits for the credit cards and add-on cards (within the overall limit of the primary card holder) based on the application of prescribed Scoring Models (one for customers and the

other for Non-customers) and as per the RAD authorized eligible Credit limits and recommended by Branches are as follows.

Sanctioning Authority	**Limit up to and inclusive of**
CM In-charge of Credit at Zonal Offices	Rs.5,00,000
AGM In-charge of Credit at Zonal Offices/ Deputy Zonal Manager(AGM)/ Zonal Manager(AGM)/ LCB (AGM)	Rs.10,00,000
Deputy Zonal Manager(DGM)/ Zonal Manager(DGM) LCB (DGM)	Rs.15,00,000
Zonal Manager(GM)	Rs 25,00,000/

FGM can sanction up to and inclusive of Rs.25,00,000 where Zones are headed by Zonal Manager (AGM) and Zonal Manager (DGM).

All sanctions made under the powers of Zonal Office/FGM office/LCB office to be reported to CO: Credit Card Centre on a monthly basis.

Delegation of powers for sanctioning Pre-approved Credit Card limits are as follows:

Sanctioning Authority	**Limit up to and inclusive of**
Chief Manager of Credit Card Centre	Rs.5,00,000/-
Assistant General Manager of Credit Card Centre	Rs.10,00,000/-
Deputy General Manager of Credit Card Centre	Rs.15,00,000/-
General Manager of Credit Card Centre	Rs 25,00,000/-

On a case to case basis, based on the recommendation of Branch Manager, Zonal Manager, FGM and LCB Branch Heads, higher limits for all categories of pre-approved cards can be sanctioned by the respective sanctioning authority as per the policy.

Branch Managers are authorized to sanction limit for "Secure Card" to Term deposit customers, as per the sanctioning powers for Loan against Deposit defined in the Power Booklet.

Delegation of powers for sanctioning Credit Card proposals beyond the sanctioning powers of Zonal Office/LCB BMs/ FGMs/Credit Card Centre officials are as detailed below:

Sanctioning Authority	**Limit above**
Corporate Office Level Credit Committee (GM)	Rs. 25,00,001/- to Rs.50,00,000
Corporate Office Level Credit Committee (ED)	Rs. 50,00,001/- & above.

- Physical Copy of Credit Card Applications sanctioned at Zonal Offices will be maintained at Zonal offices for future requirements. After sanction, the details are to be entered in the online portal to enable CO: Credit Card Centre to issue cards to the customers.

Limit Enhancement

No unilateral enhancement of existing Credit Card Limit is permitted. Card Holder can apply to enhance the credit card limit with minimum of 6 months in use in the existing credit limit. Branch has to send the request of the Card Holder with the latest income to Zonal Office Non-customers to send directly to Zonal Office. The minimum increase in the eligible amount should be at least Rs 10,000/- in any individual case.

Exceptions to be considered if recommended by Branch Manager/ Zonal Manager depending on the limit to be sanctioned.FGM is empowered for authorizing any deviations/enhancements beyond the sanctioning powers of ZMs/DZMs/BMs on a case to case basis.

Rejection of credit card applications

In compliance with RBI guidelines applicants shall be informed in writing by Zonal Office through the Branches concerned, the reason(s) which has/ have led to the rejection of their credit card application and for Non-customers directly by mail / e-mail.

Staff Card Limits

Credit Card Limits to the staff members have been fixed as follows based on their scale:

S. No	Designation / Employee Scale	Limits (in Rs)	Limits (in Rs)
		During the service	On retirement #
1	Chairman, Managing Director & CEO	10,00,000	10,00,000
2	Executive Directors / Chief General Manager / Board of Directors	10,00,000	10,00,000
3	General Managers	8,00,000	8,00,000
4	Deputy General Managers	6,00,000	6,00,000
5	Asst. General Managers	5,00,000	5,00,000
6	Chief Managers	3,50,000	3,00,000
7	Senior Managers	3,00,000	2,50,000
8	Managers	2,50,000	2,00,000
9	Asst. Managers	2,00,000	1,50,000
10	Clerks / Special Assistant	1,50,000	1,00,000
11	Substaff	50,000	25,000

S. No	Designation / Employee Scale	Limits (in Rs) During the service	Limits (in Rs) On retirement #
12	Full Time Sweeper	40,000	20,000
13	PTS ¾ Wages	35,000	15,000
14	PTS ½ Wages	25,000	10,000
15	PTS 1/3 Wages	25,000	10,000

- *Limit on Credit Card for staff on Probation (i) Officers – Rs.50,000 (ii) Clerks – Rs.25000*
- *No credit card will be issued for Substaff , FTS & PTS on probation*

 # Limits will be modified on retirement by CO: Credit Card Centre.

Staff members can also apply for credit card limits under customer category based on Scoring Model or 100% lien on deposits, both while in service and after retirement / resignation.

Cash Advance Facility & Limits

Cash withdrawal shall be as a sub-limit within the approved card limit as detailed in 4.1.10

4.1.3. Credit Period, Billing & Interest rates

As per RBI guidelines**,** the card holders shall be given sufficient number of days (at least one fortnight) for making payment before the interest starts getting charged.

The pre-determined statement date for the different categories of cards is given below:

Card type	Statement date
Global Classic, Global Gold Card, Global Platinum Card, Secure Card , Business Card & Bharat Card	20th of every month
Rupay Cards – All products	

GM/Department Head of Credit Card Centre is authorized to make any changes in the Billing dates based on the business needs.

The card holders are given 15 days' time for making the payment from the statement date.

- Cash withdrawals through credit cards will attract interest from the date of transaction
- Purchase transactions are interest free credit period of a minimum of 15 days and a maximum of 45 days depending on the date of usage of the card.

The e –statement of the credit card is password protected.

Interest rates and other charges

- RBI instructions (in the circular no. DBOD No.Dir.BC.93/13.03.00/2006-07 dated May 7, 2007) that "Banks should prescribe a ceiling rate of interest, including processing and other charges in respect of small value personal loans and loans similar in nature" have been made applicable to credit card dues also, as per RBI Master Circular on Credit Card Operations. Besides banks have been advised vide RBI circular BOD.No.Dir.BC.88 / 13.03.00 / 2009-10 dated April 09, 2010 that barring exempted categories, all other loans should be priced only with reference to the Base Rate. Bank's policy complies with the above guidelines.

- Presently in our Bank for Personal Loans the ceiling rate of interest is 9.20% (fixed). However considering the high costs involved in credit card operations by way of Fees Payable to Visa & other Service Providers, Periodical Billing / Transaction updates given to card members, Reward

Points etc., finance charges (interest charges), as detailed in Annexure II, are levied on cash and purchase transactions in our Bank.

- The Bank will not levy any charge that was not explicitly indicated to the credit card holder at the time of issue of card and without getting his / her consent. Changes in Charges (other than interest) may be made only with the prospective effect giving notice of at least one month. There is transparency (without any hidden charges) in issuing credit cards free of charge during first year.
- Bank shall charge Joining Fees / Annual Fees for credit card accounts as detailed in 4.1.10 with the prospective effect giving notice of at least one month.
- Details of other financial charges / fees prescribed are given in 4.1.10
- Bank maintains transparency in respect of prescribing ceiling rate of interest and the same has been published in Bank Website. The interest rate charges to various categories of customers and methodology of calculation of finance charges with illustration has also been published in Bank Website.
- Request for closure of credit card has to be honoured immediately by the credit card issuer, subject to full settlement of dues by the card holder and without any extra charge for such closure.

4.1.4. NPAs & Recovery Measures

Appropriation of credit card payments received

As per Bank's policy, appropriations of credits (payments received) to the card account are done as per knock off order communicated to credit card

customers in the Card Member Agreement usage Guide sent along with the credit card. The knock-off order is Government Fee (GST Charges, Cash Advance Interest, Purchase Interest, Other Fee Interest, Cash Advance Fee, Other Fees, Purchase and Cash Advance. Hence any partial payments received against credit card dues will be knocking off / appropriated in the order mentioned above. In the case of credit card accounts in NPA status, the payments received are taken towards the principal amount due in the card accounts. If the repayments / recovery is more than the principal amount, the remaining balance will be appropriated towards Charges/ MOX / Interest.

Over dues / NPA in Credit Card Operations

Credit Card is basically a revolving credit facility, the card holders have the option of repaying either the -

Full amount due: aggregate value of the transactions up to the billing date plus other financial and statutory charges (*or)*

Minimum amount due: reckoned at a certain percentage of the total transactions: value up to the billing date, plus other financial and statutory charges.

In case of default in repayment of the Minimum Amount Due before the first payment Due Date and / or consecutive defaults, the Credit Card holders are categorized into different levels of delinquency as indicated below:

- The movement of delinquency (Del) depends upon the payment received on or before the due date.
- If at least minimum due is received by the due date the del count will decrease by 1 count.

- However, if the total bill amount is received the del count is reduced to zero.
- If payment received is less than minimum due or no payment is received then del count is increased by 1.

Period of Default	Delinquency Level	Default in number of days
Default in payment of Minimum Amount of the 1st Bill	Del 1 i.e. on expiry of the Payment Due Date plus Grace Period of the 1st Bill	Less than 30 days
Continued Default in payment of Minimum Amount of the 2nd Bill	Del 2 on expiry of the Payment Due Date plus Grace Period of the 2nd Bill	30 days
Continued Default in payment of Minimum Amount of the 3rd Bill	Del 3 on expiry of the Payment Due Date plus Grace Period of the 3rd Bill	60 days
Continued Default in payment of Minimum Amount of the 4th Bill	Del 4 on expiry of the Payment Due Date plus Grace Period of the 4th Bill	90 days

- Delinquency levels are progressively increased beyond the above, depending upon the continuance of default.
- Grace period is 3 days from the payment due date

Definition of "over dues":

a) Delinquency Level 1 : not construed as overdue

b) Delinquency Level 2 & 3: only the Minimum Amount due is treated as overdue.

c) If Number of days of default exceeds 90 days or Delinquency Level 4 & above: Entire Balance amount is treated as overdue and classified as NPA.

- Asset Classification and Provision for NPAs for card accounts in Delinquency levels 04 and above (or) if the number of days of default exceeds 90 days are in line with RBI Guidelines in force and as approved in Board Note on Accounting Policy and Practices & Classification of Over dues & NPAs in Credit Card operations.
- The present level of Provisioning for various level of NPA Card accounts are briefly summarized below:

Asset Classification	**Definition**	**Provision**
Substandard	Past dues above 90 days corresponding to Del 04 and upto Del 15 (i.e. for 1 year in substandard category)	25%
Doubtful	Card accounts in Substandard category for 1 year & above (corresponding to Delinquency level 16 and above)	100%
Loss Assets	As per Bank's general guidelines and definition of loss assets	100%

Recovery Measures:

The *salient features of recovery procedure* are summarized below:

- As a part of recovery strategy of NPA in credit cards it is proposed to utilize the services of empanelled Recovery Agents on incentive basis to

augment the recovery under NPA and to contain fresh slippage in credit cards.

- The thrust of the policy in general is to recover the entire outstanding Book Balance appearing in the books as on the date of **Del 4** along with the maximum possible amount of financial charges due to the Bank and also to maximize the Recovery Amount and keep the sacrifice (waiver of financial charges) to the barest minimum.
- Negotiated Settlement / Compromise shall be considered in any account where recovery in normal course is found to be difficult and / or time consuming and the account is in Del 4 (indicating continuous default of 4 monthly Billing Statements and corresponding to 90 days past due) and above. The proposal shall be adequately substantiated for consideration under settlement.
- Write-off of even a part of Book Balance shall be avoided except for exceptional cases.
- Hence with a view to make the OTS Scheme in Credit Card operations more comprehensive, the following will be adopted for the current year 2021-22.
- **Minimum Compromise Amount** (MCA) for NPA Credit Card Accounts / Quantum of Compromise Amount / Sacrifice to be accepted.

a) Computation of Minimum Compromise Amount in all Credit Card accounts including Suit Filed accounts(other than those given in point (b) mentioned below):

Particulars	Sanctioning authority
The Minimum Compromise Amount under One Time	▪ OTS for the real balance of credit card accounts less than Rs. 10.00

Particulars	Sanctioning authority
Settlement is as follows: ▪ Del 4: Outstanding Amount ▪ Del 5 to 16 : Book Balance as on Del 4 + 45% of financial charges ▪ Del 17 to 51 : 80% of the (Book Balance as on Del 4 + 45% of financial charges) ▪ Del 52 and above: 60% of the (Book Balance as on Del 4 + 45% of financial charges) The proposed sacrifice on OTS is well within the proposed quantum of Sacrifice as mentioned in Bank's Recovery Policy.	lakhs and where the credit card holder has no other facilities with the Bank will be considered by the Branch Manager as per the powers delegated in the Recovery Policy of our bank for the "Real Balance upto Rs.10.00 lakhs category" where Real balance is Book Balance+MLE+MOX. ▪ OTS proposals for credit card NPA accounts (irrespective of balance) for which the credit card holder has any other facilities (with/without securities charged to the Bank), Zonal Office Level Credit Committee (ZLCC) is empowered to consider under their powers on the recommendation of the Branch Manager. ▪ OTS proposals for credit card NPA accounts not having any other facility, but having deposit accounts will be considered by as per recovery policy and other applicable policies in force.

- OTS can also be considered in respect of Lok Adalat settled accounts/OTS already sanctioned accounts, where settlement failed.
- In case the Credit Card holder has other facilities with securities charged to the Bank with the realizable value is adequate to cover primary loan and

card dues also, the compromise amount can be considered on a case to case basis on the account of the following:

- The realizable value of the securities net of realization cost
- The asset classification of the primary loan account
- The proposal should be otherwise adequately substantiated.

- The norms given for computation of Minimum Compromise Amount are only indicative and the emphasis shall continue to be on maximizing recovery amount and keep the sacrifice to the barest minimum.

- The recovery should be the Balance Outstanding in the Credit Card account as on the date of categorization of the card in Delinquency Level 04 (corresponding to 90 days past due) Plus interest as applicable and expenses up to the maximum extent possible.

- Even though, the Credit Card liabilities are maintained centrally at CO: CCC, Branch Managers and ZLCC are empowered to consider / sanction the OTS in the Credit Card accounts.

Terms of Payment of OTS

- Under the OTS Policy, Bank may stipulate that 50% of the OTS Amount is to be immediately deposited as an Upfront Amount in **"No Lien Account"** and the Balance to be paid in a month's time.
- In exceptional and deserving cases, OTS payment period may be allowed up to 90 days. Atleast 25% of the OTS amount (including upfront amount) is to be paid within 10 days from date of acceptance. No interest to be charged during the period.
- Payment in instalments up to 6 months on a case to case basis may be considered. During the period, interest at 12.25% simple from the date of

acceptance of OTS sanction upto the final payment on diminishing balance of OTS amount is to be recovered.

- In rare cases, the payment in instalments not exceeding twelve months may be considered. During the period, interest at 12.25% (quarterly compounding) from the date of acceptance of OTS sanction upto the final payment on diminishing balance of OTS amount is to be recovered.
- Treatment of sacrifice of MLE (Memorandum of Legal Expenses): The element of sacrifice of MLE should be treated as Waiver and not as Write-Off.

Write–off

- As per the Recovery Policy of the Bank, Write-Off of the Principal (i.e. Value of the transactions through Credit Card) is considered. With a view to facilitate better management of NPA Portfolio in our Bank's Credit Card Operations, we may continue to consider write off un-remunerative NPA Card Accounts in the following instances, after exhausting all avenues of recovery through normal course / OTS / Legal measures.
  - The card accounts with default of more than 16 months and corresponding to Delinquency Levels 16 and above.
  - Where borrower has no other means and / or not traceable / deceased.
  - Where recovery prospects are not considered feasible even if suit filing is done.
- Write-Off proposal in the Credit Card operations shall be considered by the ZLCC based on the recommendations of the Branch Managers based on delinquency level.
- COLCC(GM) of Corporate Office is authorized to sanction write off proposals in case of retired staff and existing staff whose whereabouts

could not be located and where the recovery amount is bleak/could not be recovered.

4.1.5. Internal control & monitoring systems

- To ensure compliance with RBI Guidelines and facilitate review by the Standing Committee on Customer Service of the Bank, detailed analysis of credit card related complaints are submitted on a monthly basis and reviewed by the Sub Committee of the Standing Committee on Customer Service. Assistant Branch Manager, Credit Card Centre is the Compliance Officer.
- To ensure compliance with RBI Guidelines CO:CCC shall prepare and place to Board a comprehensive Review Report on half yearly basis at the end of September and March of each accounting year.
- A parallel reconciliation process shall be put in place in co-ordination with CO: O&M Department and CO:Risk Management Department to validate the details given by the vendors.
- Frauds related to Credit Cards shall be reported to Anti-Fraud Cell of CO: Inspection Department on a monthly basis. Such frauds shall be analyzed in co-ordination with Anti-Fraud Cell and arrive at possible solutions for prevention.

4.1.6. Compliance to RBI Guidelines and Other Standards

Fair Practices Code

As per RBI Guidelines each bank must have a Fair Practices Code for credit card operations. The "Code of Bank's Commitment to Customers" issued by the Banking Codes and Standards of India (BCSBI) and the Fair Practices Code of IBA has been adopted by our Bank to cover the entire gamut of its

Banking operations including advances. The same are being adopted in credit card operations also.

It is also ensured that while appointing third party agents for debt collection, the agents should refrain from action that could damage the integrity and reputation of the Bank and that they observe strict customer confidentiality. The Banks should also ensure to comply with the guidelines of RBI, as amended from time to time in respect of engagement of recovery agents.

Compliance with Know Your Customer (KYC) Norms / Anti-Money Laundering (AML) Standards / Combating of Financing of Terrorism (CFT) / Obligation of Banks under PMLA,2002.

The instructions/ guidelines on KYC/AML/CFT will be adhered in respect of all cards issued including business and add on cards as per the Banks policy on Compliance with Know Your Customer (KYC) Norms / Anti-Money Laundering (AML) Standards / Combating of Financing of Terrorism (CFT) / Obligation of Banks under PMLA,2002. As per the annual information return u/s 285 BA of IT ACT details of payments to credit cards aggregating to Rs.1.00 lac or more in cash or Rs.10.00 lacs or more by any other mode in a FY should be submitted to RBI on annual basis. Credit Card Centre will submit the returns to RBI through Corporate Office, Banking Operations Department.

Complying to the RBI circular DBR.No.FSD.BC.18/24.01.009/2015-16 dated 01.07.2015, Bank will engage telemarketers who have complied with directions/regulations on the subject issued by the Telecom Regulatory Authority of India (TRAI) from time to time while adhering to guidelines issued on "Unsolicited Commercial Communications – National Customer Preference Register (NCPR)".

RBI guidelines on Enhancing Security of Card Transactions

- The functionalities as directed by Reserve Bank of India vide circular DPSS.CO.PD No.1343/02.14.003/2019-20 dated 15.01.2020 will be made operational by 16.03.2020.

- All new cards will be enabled for use only at ATMs and Point of Sale (PoS) devices within India.

- Bank will provide customers the following facilities for enabling card not present (domestic and international) transactions, card present (international) transactions and contactless transactions:

  a) facility to switch on / off and set / modify the daily transaction limits (within the overall card limit provided by the bank) for all types of transactions – domestic and international, at PoS / ATMs / online transactions / contactless transactions, etc.;

  b) the above facilities will be provided on a 24x7 basis through multiple channels – Mobile Banking, Internet banking and ATMs

  c) alerts or information or status, etc., through SMS or e-mail will be provided, as and when there is any change in status of the card.

- Existing International Credit Cards which have been never used for international transactions will be disabled for international transactions with effect from 16.03.2020.

- Existing credit cards which have never been used for online (card not present) transactions will be disabled for online transactions with effect from 16.03.2020.
- Accordingly below are the maximum daily usage permitted on various credit card products of our Bank

Various Credit Card products and daily usage limits:

S. No.	Card Product	ATM Cash Limit	POS / E-Com Purchase Limit	Aggregate Limit
1	Bharat/ Classic Card	8000	12000	20000
2	Gold Card	25000	75000	100000
3	Platinum/ Select Card	50000	150000	200000
4	Business Card	50000	300000	350000

- Limits indicated above are as prevalent currently and are subject to revision

- As per the guidelines issued by Reserve Bank of India vide RBI/2019-20/130 DoS.CO/CSITE/BC.4084/31.01.015/2019-20 dated 31.12.2019 certain Cyber Security Controls are required to put in place by the Third party ATM Switch Application Service Providers. In view of this, the RREs (RBI Regulated Entity) shall ensure that the contract agreement signed between them and the third party ATM Switch ASP shall necessarily mandate the third party ATM Switch ASP to comply with cyber security controls on an ongoing basis and to provide access to the RBI for on-site/off-site super vision. Necessary contract agreements to be signed between RREs and service providers to this effect.

Customer Confidentiality

As per the guidelines issued by RBI vide circular DBR.No.FSD.BC.18/ 24.01.009/2015-16 dated 01.07.2015, Bank will not reveal any information relating to customers obtained at the time of issuance of credit card to any other person or organization without obtaining their specific consent, as regards the purpose/s for which the information will be used and the organizations with whom the information will be shared. The information being sought from customers will not be of such nature as will violate the provisions of the laws relating to secrecy in the transactions.

The disclosure to the DSAs/recovery agents will also be limited to the extent that will enable them to discharge their duties. Personal information provided by the card holder but not required for recovery purposes will not be released. Bank will ensure that the DSAs/DMAs do not transfer or misuse any customer information.

4.1.7. Disclosure in Balance Sheet

Credit Card receivables are classified as Unsecured / Clean Advances and the Accounting Standards and Disclosure Norms pertaining to such advances are relevant and applicable to Credit Card Receivables also. Reporting on Movement of NPA in credit card receivables is done as per the format adopted for all advances and provisioning for NPAs as per RBI Guidelines and Board approved Policy.

The following are some of the important features in Credit Card Operations that may be required to be disclosed in the Schedules – Summary of Significant Accounting Policies-

- **Revenue Recognition** – on receipt basis only
- **Loyalty Points** – Reward Points are earned by credit card customers when they use Indian Bank Credit Card.

4.1.8. Disclosure to rating Agencies and others

The Bank shall provide information relating to credit history/repayment record of the card holder to Credit Information Companies (CICs) (that has obtained Certificate of Registration from RBI) explicitly bringing to the notice of the customer that such information is being provided in terms of the CIC

(Regulation) Act, 2005. The credit card customer is informed that in case of default of Payment he/she will be informed as defaulter to the CIC which is stated in our Card Usage guide and also in the monthly billing statement. In the event of customer settling his dues after having been reported as defaulter, the Bank will notify the CICs in the next report withdrawing the customer as defaulter. Presently details regarding the card holders (as given in their applications) along with the payment records for the card liabilities are furnished to CIBIL from card issuance date.

Besides, in case of suspected / fraudulent transactions details are sent through VISA online for information of all Member Banks. The credit card application and card Member Agreements are having the necessary provision for disclosure as above.

4.1.9. Customer Service

Department Head of CO: CCC is the Authority for giving permission to initiate arbitration proceedings.

COLCC (GM)-Recovery authorized to permit such write-off of the disputed amount. Bank would prefer insurance claim under Bank's Indemnity Policy in force. Irrespective of the fact the claim is admitted /settled or rejected by the Insurance Company, COLCC (GM)-Recovery is empowered to write-off of such claims. If the insurance claim is settled for full / partial amount, the same will be appropriated to income of Bank. Hence 100% provision to be made upfront for the disputed amount though it is not an NPA Account as per categorization.

Redressal of Grievances

With a view to facilitate speedy redressal of cardholders grievances, besides Bank's Customer Care Toll Free Call Centre; CO:CCC Officials shall attend the queries and resolve the issues. As per RBI Guidelines, name of the Grievance Redressal Officer (ABM of CO:CCC) shall be furnished in the

monthly Billing Statements. The complaints / grievances received would be resolved within 21 days from the date of receipt of the complaint, as per the Bank's Customer Grievances and Redressal Mechanism Policy.

The online "Centralized Grievance Redressal System" (CGRS) facility will be extended to cover credit card customers also.

4.1.10. Eligibility Criteria, Features & Card Limits

Eligibility Criteria

The features and eligibility criteria for various card types are as follows:

Visa- Global Gold, Platinum Cards, Rupay-Select, Platinum & Classic

- Customers of Indian Bank and Indian Bank sponsored RRBs (Regional Rural Banks) having satisfactorily conducted accounts and with KYC Compliance.
- Indian Nationals of Age between 18 to 80 years with Minimum Gross Income of Rs.12,500/- per month (applicable prospectively).
- PAN Card is mandatory
- Mobile Number and email id are desirable. But, one of these is mandatory.
- For NRIs & PIOs on a case-to-case basis on their agreeing for our marking lien on their deposits (waiver to this condition can be considered by the Zonal Manager OR by FGM, Corporate Office Level Credit Committee (GM) for limits beyond the sanctioning powers of Zonal Manager, FGM, LCB Branch Heads, Branch Managers, Credit Card Centre officials based on specific recommendation of the respective Zonal Manager).

- Add-on cards up to a maximum of 4 to spouse / children / brothers / sisters / parents. KYC Documents (address proof and identity proof) are mandatory.

The eligibility criteria for credit cards limits are given below:

Customer	Condition	Limit
Existing Deposit Customer	Average monthly balance of Rs.50000 & above	Min Rs.50000 Max – Equals to monthly average balance of 1 year
Existing salaried customer	Employed with Central Govt/State Govt/PSU/ MNC/Govt aided institutions and maintaining salary account with us	Min-Rs.50000 Max-Three times of monthly salary
Existing standard home loan customer	Loan limit of Rs.20.00 Lakh and above and servicing instalment regularly	Min Rs.100000 Max – 5% of home loan limit, maximum Rs.300000
New Home Loan customer	Loan limit of Rs.25.00 Lakh and above	Min Rs.100000 Max – 5% of home loan limit, maximum Rs.300000
Existing deposit customer	Annual transaction through Debit card is more than Rs.50000 for non-cash transaction	Min Rs.50000 Max – Equals to monthly average transaction of 1 year
Existing business loan customer	Loan limit of Rs.25.00 Lakh and above and account is	Min Rs.100000 Max – 10% of avg.

Customer	Condition	Limit
enjoying working credit facility	regular	monthly turnover (past 1year)
Existing Current Account customer	Monthly turnover of Rs.10.00 Lakh and above	Min Rs.100000 Max – 10% of avg. monthly turnover (past 1year)
Existing Business Correspondent	Having monthly remuneration of Rs.10000 and above (based on last six months average)	Min Rs.25000 Maximum- Three times of average monthly remuneration

Bharat Cards

- Only to Indian Bank customers having satisfactorily conducted accounts and with KYC Compliance
- Indian Nationals of Age between 25 to 60 years with Minimum Gross Income of Rs.5000/- per month (applicable prospectively).
- No add-on cards.
- Voter ID/AADHAR No is mandatory.
- Landline, Mobile Number and email id are desirable. But, One of these is mandatory.
- In case, the card usage amount exceeds Rs.1.00 lakh in a financial year, PAN Card details are to be furnished by Card holder.
- Form 60 of Income Tax Rules 1962 to be obtained, in case Pan Card is not available.

Business Cards

- Corporate & SMEs Loan Accounts – (Limited Companies, Partnerships, Sole Proprietary Concerns, Trusts & Association) having aggregate secured limits of Rs. 25.00 lakhs & above
- Reputed Corporate current accounts with satisfactory track record of operations and financials in the past two years on a case to case basis only by the Zonal Manager or with Zonal Manager's recommendation for limits beyond the sanctioning powers of Zonal Manager.
- Up to a maximum of 5 cards to the individual executives / employees nominated by the company and within the overall limit to the Company: the card, apart from the name of the individual, will also carry the name of the Business Entity.

Secure Cards

- Customers of Indian Bank having Term Deposit Accounts of Rs.25,000/- & above.
- Consent letter for marking lien on the deposit amount up to the limit sought is mandatory.
- PAN Card is mandatory.
- Mobile Number and email id are desirable. But, One of these is mandatory
- Add-on cards up to a maximum of 4 to spouse / children / brothers / sisters / parents. KYC Documents (address proof and identity proof) are mandatory.

Non-Customers

- Satisfactorily conducted SB/Current account with any scheduled Bank in India.
- Mobile number, email ID, PAN number and AADHAR card mandatory
- CIBIL score of 700 and above
- Age from 20 years to 70 years
- Income Rs.3 lakhs and above p.a. as per latest 2 years IT returns with income proof.

The features and credit limits of credit card range are given below:

S. No	Product Name	Card Type	limit range	Other Terms / Features
1.	Bharat Card (VISA Classic)	Domestic	Rs.10000 to Rs.19,999	EMI Facility – NO Cash Limit – 25% Minimum amount payablemonthly–10 % Reward points – NA Insurance Cover – *
	Rupay Classic	Domestic	Rs.10000 to Rs.25000	EMI Facility - Yes Cash Limit – 25% Minimum amount payable monthly– 5% Reward Points – NA Insurance Cover - *
2.	Business Card VISA (Gold/ Platinum) & Rupay	Global	As requested by the customer	EMI Facility – NO Cash Limit – 40 % Minimum amount payable monthly– 5 % Reward points –1 point valued at Re.1 for every Rs.200 spent – to be

S. No	Product Name	Card Type	limit range	Other Terms / Features
	(Platinum/ Select)			credited on 500 points accruing. Insurance Cover – * Insurance cover for Rupay cards as offered by NPCI
3.	Visa-Gold Card / Classic Card	Global	Rs.20000 to Rs.99999	EMI Facility – YES Cash Limit – 40 % Minimum amount payable monthly– 5 % Reward points –1 point valued at Re.1 for every Rs.200 spent – to be credited on 500 points accruing. Insurance Cover – *
4.	Visa Platinum Card	Global	Rs. 100000 and above	EMI Facility – YES Cash Limit – 40 % Minimum amount payable monthly– 5 % Reward points – 1 point valued at Re.1 for every Rs.200 spent – to be credited on 500 points accruing. Insurance Cover – * Insurance cover for Rupay cards as offered by NPCI
	Rupay Platinum Card	Global	Rs.250001 to Rs.1,99,000	
	Rupay Select Card	Global	Rs.2.00 lakhs & above	
5.	Secure Card (Card to be issued against lien on the total	Global	Minimum of Rs. 25000 or 100% of the Deposit amount or lesser limit requested by	Term Deposit Period – Minimum One Year EMI Facility – YES Cash Limit – 40% Minimum amount payable monthly- 5% Reward points – 1 point

S. No	Product Name	Card Type	limit range	Other Terms / Features
	amount in Term Deposit offered as security)		the customer. Accrual of Interest on term deposit will not be considered for enhancement of Credit Card Limit.	valued at Re.1 for every Rs.200 spent – to be credited on 500 points accruing. Insurance Cover – * For Rupay credit cards as offered by NPCI

Accident Insurance Cover and other Insurance Benefits to Card Members

- Under tie up with The Oriental Insurance Co Ltd, our credit card members are extended certain insurance benefits including cover for Accident Death under a tailor made Policy for IB Card Members. The Policy is based on MOU and agreement entered into with The Oriental Insurance Co Ltd and the same is reviewed every year by the functional General Manager of CO: CCC.

- The Insurance cover is offered as value addition to our card members free of cost.
- The Insurance Cover includes Accident Death / Hospitalization, Baggage Cover, Purchase Protection Cover and Credit Shield.
- Details of the insurance company (Name, Address & Telephone nos.) will be informed to the card holders.
- Nomination details will be obtained from the card holder and same will be communicated to the Insurance Company for registration.

	* Insurance cover		Visa Gold, Platinum, Business, Secure cards	Visa Classic	Bharat & Rupay Classic
A	Death (100%) due to Air Accident		Rs.5.00 lakhs	Rs.2.00 lakhs	Rs.1.00 lakh
B	Death (100%) due to any other accident		Rs.2.00 lakhs	Rs.1.00 lakh	Rs.0.50 lakh
C	Hospitalization Cover due to accident	Age upto 65 years	Rs.1.00 lakh	Rs.0.50 lakh	Rs.0.50 lakh
		Age 66 to 80 years	Rs.0.50 lakh	Rs.0.25 lakh	Not Applicable
D	Baggage Cover		Rs.10,000	Rs.5,000	Not Applicable
E	Credit shield on death		Rs.25,000	Rs.10,000	Rs.10,000
F	Purchase protection cover		Rs.25,000	Rs.10,000	Rs.10,000
G	Death (100%) due to any other accident to First Add On Card member		Rs.1.00 lakh	Rs.0.50 lakh	Not Applicable

(** Inclusive of GST)

Schedule of Service Charges

S. No	Nature of services	Classic, Gold, Platinum, Select, Business, Secure cards	Bharat & Rupay Classic
1	Joining Fee	Free for Primary Card	Free for Primary Card
2	Annual Membership (AMC Charges) **(From 2nd year onwards) +**	**Classic,Gold, Platinum,Select** : Rs.250	NIL

S. No	Nature of services	Classic, Gold, Platinum, Select, Business, Secure cards	Bharat & Rupay Classic
		Business : Rs.500 **Secure cards** : NIL Waiver of AMC is permitted in the following case: 1. If the transaction usage in the previous year exceeds Rs.50,000 p.a in Select/ Platinum/Gold/Classic 2. If the transaction usage in the previous year exceeds Rs.2,00,000 p.a in Business card	
3	Cash Advance charges	2.25% p.m.	1.99% p.m.
4	Cash Advance Fee	Rs.50	Rs.25
5	Late Fee	Rs.250	Rs.50
6	Over Limit Fee	Rs.50	Rs.25
7	Limit Enhancement Fee	Rs.100	Rs.25
8	Cheque return Charges/Invalid Cheque Fee	Rs.250	Rs.50
9	Card Re-issue Fee	Rs.250 (Rs.100 for classic card)	Rs.100
10	Pin Mailer Re- issue Fee	Rs.50	Rs.25
11	Foreign Currency Transaction Fee	Conversion Mark up 3%	N A
12	Surcharge	Petrol: 2.5% , Railway Ticket 1.8% of transaction amount	

S. No	Nature of services	Classic, Gold, Platinum, Select, Business, Secure cards	Bharat & Rupay Classic
13	Statement Retrieval Fee	Rs.100 per statement	Rs. 50 per statement.
14	Charge Slip Retrieval Fee	Rs.125 per Slip	Rs. 75 per Slip
15	Balance Enquiry through ATM	Rs. 35 (in India) and Rs.50 (in abroad)	Rs.35 in India
16	Cash withdrawal at Bank's ATM's Cash withdrawal at Other than Bank's ATM's in India Cash withdrawal at any ATM at Abroad	Nil Rs.100 Rs.250	Nil Rs.75 NA

All charges are exclusive of GST.

Standard Operating Procedures for Credit Card Operations will be formulated and upon approval of the same by General Manager the same will be submitted to Executive Director for information.

4.2 Merchant Acquisition and Digital Services

4.2.1. Merchant Acquisition

Merchant acquisition is primarily referred to as the mechanism of providing necessary infrastructure for facilitating payment of goods and services purchased. Merchant payments constitute a majority in the daily transactions carried out by customers. Payments to Utility Companies, Educational Institutions, and Public Distribution System outlets, Government Departments / Institutions etc. are also included in Merchant payments apart from regular purchase of goods from traders, which were traditionally covered under Merchant payments.

The thrust on cash-less payments in the post- demonetisation scenario has expanded the scope for merchant acquisition manifold with huge demand from all entities, irrespective of their size of operations, for cash-less modes of receiving payments from their customers.

Traditionally, Point-Of-Sale (POS) machine was the only electronic mode of receiving payments from customers through cards. Reserve Bank of India, while encouraging Banks to expand card acceptance infrastructure to a wider segment of merchants across all geographical locations, advised Banks vide Circular No.RBI/2015-2016/410.DPSS.CO.PD.No.2894/02.14.003/2015-2016 dated May 26, 2016 to put in place their own Board approved Policy on merchant acquisition.

With the advent of Digital Technology and the need for cash-less payment emanated by demonetization in our country, many digital modes have evolved for receiving payments from customers.

In view of the current digital revolution happening in payments in our country, Merchant Acquisition policy needs to cover all digital modes. Merchant Acquisition Policy for our Bank is formulated to suit the current payment environment in the country.

Modes of Acquisition

Merchant Acquisition in our Bank can be carried through the modes as mentioned below:

[i] Point of Sale (POS) machines

POS machine is one of the digital payment acceptance channels that are widely used across globe.POS machines are used to receive payments from customers using their Debit/Credit cards/Prepaid/NFC cards. Various features are enabled in POS namely UPI QR on POS, NCMC acceptance, Cash@POS and other value added services based on market requirement from time to time.

[ii] QR (Quick Response) Code

QR Code generated for every merchant will be unique which contains the details of merchant's bank account or pointers to merchant's bank account. Customers use their Mobile Payment App to scan the QR Code and make payment from their account to the merchant's account. Both merchant and customer get an SMS informing the details of the payment transaction for the sale made.

- *Merchant UPI QR* : As an extension of QR facility to merchant to perform P2M(Person to Merchant) and P2PM(Person to Small Merchant) transactions, Merchant UPI QR facility is launched. Merchant will be provided with Virtual Payment Address (VPA)/Static UPI QR by

Branches/Zonal offices for acceptance of payment. Small merchants(monthly inward credit less than Rs.1 lakh through UPI) can self onboard themselves and create UPI Merchant QR using IB Small Merchant app. Corporate merchants (monthly inward credit more than Rs.1 lakh through UPI) will be provided with Static QR for receiving payments in their account through Corporate QR UPI solution. Customer will transfer the funds from their account to merchants account by scanning the QR code. Both merchants and customer will get notification in mobile through SMS/UPI app

[iii] Aadhaar Pay

In Aadhaar Pay which is developed in association with UIDAI and NPCI, merchant needs a smart mobile device with Aadhaar Pay App installed along with biometric fingerprint scanning facility. While making a purchase, merchant will enter the sale details, enter the Aadhaar number of the customer and fingerprint of the customer will get captured. The fingerprint is authenticated by UIDAI and the amount will be debited account mapped to Aadhaar number in the Aadhaar Payment Bridge with NPCI. Merchant will get a notification in the mobile App and customer and SMS.

[iv] Digital Collection Services

Merchants can Collect funds through various online and offline collection products viz. Multi Utility Payments (MUP), IB V Collect / IB V Collect Plus, Generic Fee Collection, IB Collect / IB Collect Services (Payment Gateway Services)

- Multi Utility Payments (MUP): MUP deals with the process of enabling the Corporate/ Institution Collect utility payments/fees from their clients/end

users. MUP – Multi Utility Payments is a product for offline challan collection of various payments like (i) Insurance Premiums (ii) School / College / University Fee, Telephone bills, Electricity bills, Subscription to Newspapers, Dealer payments for supply of goods and other B2B (Business to Business) and C2B (Customer to Business) payments can be collected in the accounts using MUP facility.

Charges for the same has to be recommended by Branch and Zonal Office. The charges should be in flat rate basis and are applicable per transaction.

Configuration of parameters for new applications and reconfiguration of parameters for existing accounts can be sanctioned under the powers of Assistant General Manager (DBD).

- IB V Collect / IB V Collect Plus: A Collection Product with MIS regarding remitter / remittance details etc. IB V Collect suits any institution intends to receive funds from different sources through any Bank branch counter or net banking of any bank. The collection is enabled through Cash/ Cheque at any branch counter, NEFT / RTGS through any Bank Branch counter or net banking of any bank.

  Charges for the same has to be recommended by Branch and Zonal Office. The charges should be in flat rate basis and are applicable per transaction.

  Configuration of parameters for new applications and reconfiguration of parameters for existing accounts can be sanctioned under the powers of Assistant General Manager (DBD).

- Generic Fee Collection: To meet the requirements of the various Educational Institutions / other Organizations, a generic Fee Collection Module has been developed in CBS. The Institution having existing account with our Bank can opt to use this fee collection module through the Nodal Branch.

  Charges for the same has to be recommended by Branch and Zonal Office. The charges should be in flat rate basis and are applicable per transaction.

  Configuration of parameters for new applications and reconfiguration of parameters for existing accounts can be sanctioned under the powers of Assistant General Manager (DBD).

- IB Collect / IB Collect Services (Payment Gateway Services):A collection product that enables institution/corporate/merchants to collect funds online using payment gateway services from the remitters using the payment modes such as Credit/ Debit cards, Net banking of various banks, UPI and wallets.

  In addition to the above, any new mode of Merchant Acquisition, either innovated by our bank or becomes available in the market, may be adopted on approval from Executive Director.

  All the above modes shall be offered to the merchants and their preferred mode is provided to them.

4.2.2. Digital Services

As digitization rapidly redefines and magnifies customer expectations, it is imperative to enhance its customer interaction channels. Our Bank always brings the best possible ways to onboard new customers and unifies the user flow throughout all touch points with a bank. For the customer convenience

and comfort, our Bank has launched initiatives and government schemes. One such initiative is Indian Bank FASTag.

FASTag

To reduce traffic at the toll plazas, the Government of India (GOI) has mandated all toll plazas, to make toll payments electronic. With this mandate, all vehicles travelling through toll plazas will have to mandatorily pay toll charges using FASTag. This program is part of the National Electronic Toll Collection (NETC) initiative, rolled out by National Payments Corporation of India (NPCI) under the guidelines of National Highways Authority of India(NHAI) & and Indian Highways Management Company Limited (IHMCL). FASTag is a reloadable tag that employs Radio Frequency Identification (RFID) technology for making toll payments directly while the vehicle is in motion.

Retail customers of amalgamated entity can purchase FASTag through following modes:

1. Online Purchase through our Bank's website. FASTag will be delivered at doorstep.
2. Visiting Bank's Branch. Branches are facilitated to generate the challan and to issue FASTags at Branch counter through in-house portal (http://10.100.12.213:8080/fastag) in Bank Helpdesk.

Wallet account will be created for each customer at the time of issuing FASTag. Customer can recharge/reload the wallet either through online or Branch counter.

4.2.3. Roles & Responsibilities

Digital Banking Division is the custodian of the Merchant Acquisition Policy.

- For each mode of Merchant Acquisition, Digital Banking Division shall be the owner and formulate the functional requirements.
- Organization & Methods Department shall formulate the systems & standard operating procedures for on-boarding, operations, accounting, settlement, reconciliation, intra-bank dispute management and termination of the service.
- Risk Management Department shall study the risks involved and recommend suitable mitigation measures.
- Information Technology Department shall provide necessary IT infrastructure, developing product that meets the requirement of the customer.
- Information Systems Security Department shall study the Information system security risks and suggest suitable mitigation measures.
- Department Head of Digital Banking Division is authorized to take decisions on the operational aspects of the services.

Bank may also explore the possibility of using the college students in Management studies for conduct of survey for identification of potential market for POS machines and other modes of Merchant Acquisition.

4.2.4. Payment gateway service to merchants

IB Collect/ IB Collect Plus (Payment gateway services)

IB Collect/ IB Collect plus (Payment Gateway Services) is a service provided to merchants/institutions which enables the end user or consumer to make their payments through online mode. It is similar to the POS terminal where

the transaction is considered as card not present transaction in case the payment made through cards.

How the payment gateway service is provided to merchant

Payment Gateway Services requirement differs from merchant to merchant. Rates for providing the service to merchants also varies based on the merchant category and various guidelines issued by Government of India and partner Banks. Bank engages the services of the established payment gateway aggregators who provide the service through their gateway and facilitates service to our customers. Aggregators work with Banks and provide us with the ability to accept Debit cards, Credit cards, Net Banking and other payment modes. The cost for engaging the services of the aggregator will be passed on to the merchant, which results in no cost to the Bank. If Bank chooses to have a mark-up over the rates proposed by the service provider then the margin will be Non interest Income for our Bank.

Process for engaging a payment aggregator

Bank will avail the services of Payment Gateway Aggregators already providing gateway services to the Bank. Bank will identify the service provider for each merchant based on the lowest quote/cost (L1) arrived through receipt of competitive quotations from the service providers. However, Bank may engage such service providers other than L1 on a case to case basis considering Institutional/Govt. Dept preference along branch and Zonal office recommendation and the same will be under the sanctioning powers of General Manager (DBD).

Bank may empanel a minimum of three service providers for providing gateway services to our merchants.

New service providers may be empanelled considering expression of interest (EOI) by such service providers based on market requirements. General Manager (DBD) is empowered to approve such empanelment.

4.2.5. Charges for Services & Waivers

Charges on Services

POS: POS Services can be enabled to Merchants / Establishments directly through Branch, Lead Generation or Referral Channel.

POS Machines can be supplied to the Merchants / Establishments under Out Right Purchase Model / Rental Model / any other Model based on market requirement.

- Fixed charges: If any equipment/solution/connectivity is provided by Bank to Merchant under Rental Model/ any other model requiring collection of fixed charges, such charges shall be collected from the merchant on monthly/quarterly/half- yearly/yearly basis towards usage cost of the equipment/solution/connectivity and its maintenance.
- Recurring charges: Recurring charges shall be charged either fixed amount per transaction or as a percentage on the value of transaction, based on the costs associated with the transaction mode of Merchant Acquisition.
- The fixed charges can be recovered from the customer's account or Settlement Amount and recurring charges will be recovered from the settlement amount.

Rate fixation for providing payment gateway services (Commercial Proposal): Rate fixation for providing commercial proposal to merchant with margin (as Bank's Non Interest Income), will be as follows:

Rates to be proposed	**Minimum Margin**
In case of flat rates	Rs. 2
In case of relative rates	0.20%

RBI guidelines are to be strictly adhered.

The option for closing business at a higher rate than the minimum margin is not restricted/not capped.

The commercial proposal with above mentioned markup margins or higher margins and selection of service provider for the same can be sanctioned under the powers of Assistant General Manager (DBD). AGM (DBD) can sanction the selection of service provider with lesser margin, if such rates are governed (capped) by the regulations of RBI/GOI.

DGM (DBD) can sanction the selection of service provider up to a discount of 50% on the minimum mark up value (i.e Margin of Re.1/- in case of flat rates and 0.10% in case of relative rates)

General Manager in charge of DBD is authorized to approve enabling of services at Nil Margin (up to the level of rates quoted by the service provider i.e. no cost and no income basis.) and approve enabling services to customers with Concession / Nil charges involving expenditure to the bank. General Manager (DBD) in also authorized to make necessary changes in the powers of approval considering the market requirement.

Aadhaar Pay/ QR/ UPI: Charges applicable as per NPCI/RBI/GOI guidelines issued from time will be levied.

FASTag: FASTag has a onetime Fee of ₹100/- inclusive of all taxes. The Security Deposit, Wallet Minimum Balance and Tag Cost for different vehicle class are proposed as follows:

(in Rs.)

Vehicle	Description	Tag Cost	Security	Wallet

Class		(including GST)	Deposit	Threshold Amount
4	Car/ Jeep/ Van	100	200	200
4	Tata Ace and Similar mini Light Commercial Vehicle	100	200	200
5	Light Commercial vehicle 2-axle	100	300	300
6	Bus 3-axle	100	400	300
6	Truck 3-axle	100	400	300
7	Bus 2-axle/ Mini-Bus	100	400	300
7	Truck 2-axle	100	400	300
12	Tractor/ Tractor with trailer	100	400	300
12	Truck 4-axle	100	400	300
12	Truck 5-axle	100	400	300
12	Truck 6-axle	100	400	300
15	Truck 7-axle and above	100	400	300
16	Earth Moving/ Heavy Construction Machinery	100	400	300

- Convenience fee will be applicable for online recharge.
- FASTag Replacement cost is Rs.100 (inclusive of all taxes).
- Threshold amount is the minimum recharge amount to be done at the time of tag activation.
- The above mentioned deposit rates would be applicable as per the vehicle class. Balance amount will be refunded at the time of closure of FASTag account.
- Toll amount will be deducted as per the applicable amount, depending on the vehicle class and the plaza used.

Waivers and Concessions

- Waiver/Concession of POS services (MDR, Rent and Connectivity charges/One time cost/transaction charges) can be considered, if there is a Net Benefit accruing out of Float funds available in SB/Current account. In other words, Benefit accruing out of Float Funds maintained by the Customer should be more than the Cost to be incurred on deploying the POS terminal.
- Providing Waiver/Concession on Payment Gateway Service to merchant / Institution/ Government Department i.e with rates lesser than the rates quoted by the service provider shall not be entertained. However, if there is net benefit, considering the overall business portfolio with the merchant and cost benefit analysis, the expenditure shall be borne by the Branch

- The discretionary powers for the sanction of Concession/ Waiver for POS and Payment Gateway Services up to the expenditure limit is detailed below:

Net Out Go * (per year)	**Sanctioning authority**
Upto Rs. 3 Lakh	ZLEAC (AGM)
Upto Rs. 5 Lakh	ZLEAC (DGM)
Upto Rs. 10 Lakh	ZLEAC (GM) / FGMEAC(GM)

*Net Out Go is the total expenditure incurred/to be incurred on providing the services at nil/reduced charges

- Concessions beyond the powers as enumerated above can be considered on a case to case basis, upon recommendation of the zonal manager

based on the overall business of the customer with the bank as detailed below:

Net out go (per year)	Sanctioning authority
Up to Rs. 25 lakh	COLCC (GM)
Above Rs. 25 lakh to Rs. 1 crore	COLCC (ED)
Above Rs. 1 crore	CAC

- Waivers / Concessions should be Reviewed Once in six months to ensure compliance to sanction terms. However, the charges can be reviewed before completion of six months, considering changes in the market, regulatory guidelines, government guidelines, any special campaigns launched by the Bank etc.

4.2.6. Security & Risk Mitigation

Security

Security measures as specified in Bank's Information Security Policy will be followed by all products/services.

Risk Management

Service providers, merchants and customers shall be liable for the frauds and or losses attributable to them. Other risks in merchant acquisition business shall be managed by the Bank

4.2.7. Customer Service

HelpDesk support will be provided to the customers for queries, information or grievance redressal. Department Head of Digital Banking division can

designate Grievance Redressal Officer for each mode of merchant acquisition services. Necessary Training and Technical Integration related support will be provided by the service provider.

All disputes in the service provided shall be resolved as per the Dispute Management guidelines of the agency handling the interbank settlements. Any intra-bank dispute shall be resolved as per the dispute management procedures formulated by Organization & Methods department. Any dispute raised regarding transactions/settlement should be resolved by the service provider in co-ordination with DBD.

Fastag: To block the FASTag account in case of lost/ damage of RFID Tag, to raise the complaint of any incorrect debit, to get the refund in case of sold/transferred of vehicle, to get the replacement of tag, and for any other queries & information, customer can contact Customer care on **1800 258 6680** which is managed by the Vendor.

All disputes in the service provided shall be resolved as per the Dispute Management guidelines of the agency handling the interbank settlements. Any intra bank dispute shall be resolved as per the dispute management procedures formulated by Organization & Methods department. Any dispute raised regarding transactions/settlement should be resolved by the service provider in co-ordination with DBD.

Customer will get an SMS update every time the toll amount gets deducted. Customer can even get the balance through SMS by giving missed call to **8886658808** from their registered mobile number.

4.2.8. Outsourcing:

If any part of the service is required to be outsourced, it shall be as per the Bank's policy on outsourcing.

4.2.9. Procurement/ Payment

All payment towards procurement/availing of digital services shall be governed by Bank's "Procurement Policy for IT Related Goods and Services"

4.3 Internet / Mobile Banking

With the advent and advancement of technology, new horizons of Banking are being explored and various delivery channels for customers are being introduced.

One such delivery channel is through the Internet. Enabling banking through Internet will facilitate remote access and provide relief to the customers from going to the bank premises for their financial & non-financial transactions. Internet Banking takes our Bank's services to the customers' premises and provides them banking access on a 24 x 7 basis at the place of their convenience. Further it gives avenues for the Bank to project all relevant information about our products with customer-specific approach.

Another medium for extending the banking services particularly owing to the rapid growth of young users in India is through mobile phone. Mobile applications provide versatility and ease of use to the customers. This makes Mobile banking an important channel to extend banking service to every segment of society.

Scope: Internet Banking and Mobile Banking

The scope of this policy includes Internet Banking, Mobile Banking and all other infrastructure, people and processes required to make these channels open to the customers. The various aspects of policy with regard to Internet Banking will be applicable to Mobile Banking services also unless specifically mentioned otherwise. The Policy generally conforms to the guidelines on Mobile Banking by Reserve Bank of India. Wherever a specific mention is not made herein, Reserve Bank of India guidelines for Mobile Banking will hold good as far as it is applicable to the environment.

Our Bank and banking services are being presented to the Customers away from normal banking environment and all relevant information required by the customers must be provided in full without any room for ambiguity.

Bank commits itself for such information and hence carries the risk of being misrepresented. Unlike branch banking, the security aspects lie mainly with the customer.

At the organizational level, there is a paradigm shift in the functional level and the roles and responsibilities must also be defined for internet banking and mobile banking. Since transactions through internet and mobile banking channels are carried out remotely, there needs to be a framework which clearly defines the procedures and guidelines. Such procedures must enable the Bank and the Customers to communicate effectively and carry out the transfer of information and data in a secured environment in the interest of the bank and all its stakeholders.

Reserve Bank of India vide their communications DBOD No. Comp.BC.13/07.03.23/2001-01 dated 14-June-2001 and DBOD No. Comp.BC. 14/07.03.29/2005-06 dated 20-July-2005 have directed that no prior approval from RBI is required for offering internet banking services. However the internet banking policy has to be approved by the Bank's Board and should comply with the guidelines issued in the circulars.

Internet Banking is being provided to our customers in two flavours:

a) Retail Internet Banking

b) Corporate Internet Banking

Various financial and non-financial services are being offered to our retail and corporate customers through our internet banking website: https://www.indianbank.net.in.

Transactions carried out through Payment Aggregators and Payment Gateways in internet Banking shall be guided by RBI Circular Ref: RBI/DPSS/2019-20/174 DPSS.CO.PD.No.1810/02.14.008/2019-20 dated 17.03.2020 updated as on 17.11.2020.

Subsequent to RBI guidelines dt. 28.11.2014 and RBI approval vide their letter DPSS/CO/AD No.2694/02.27.004/ 2015-16 Dt.16.05.2016, RBI had provided in-principle approval to the Bank to operate as Bharat Bill Payment Operating Unit (BBPOU) under Bharat Bill Payment System. Customers can perform bill payments through this facility available in the Bank's internet banking application.

Subsequent to RBI guidelines dt.08.10.2008 and RBI approval vide their letter DPSS/CO/No.1182/02.23.03(PD)/ 2008-09 Dt.12.01.2009, funds transfer facility was extended to our Mobile Banking customers.

"IndOASIS / IndPay" is the Mobile Banking application of the Bank through which financial and non-financial transactions can be carried out by customers through their mobile phone / tablet devices. In future, this application will also be used for disseminating information to the public viz. display of bank's products and services, results, statistics, awards, accolades, achievements etc. Both the above applications are to be governed by this Policy.

Mobile banking operations shall be guided by the RBI Master Circular – Mobile Banking transactions in India – Operative Guidelines for Banks Ref: RBI/2016-17/17 DPSS.CO.PD.Mobile Banking.No./2/02.23.001/2016-2017 dated 01.07.2016 updated as on 10.01.2020.

Bank is providing SMS Banking for low-end phones, IndOASIS / IndPay mobile application for Android and iOS smart phones for customers.

Bank is also providing UPI services through IndOASIS. The USSD service on *99# has been enabled through UPI for basic handset.

Bank is in the process of extending services such as WhatsApp Banking in the future using the existing infrastructure of Internet Banking / Mobile Banking.

Applicability

This policy applies to employees, contractors, consultants, customers using the facility and other workers at the Bank and their associates, including all personnel affiliated with third parties. This policy also applies to all applications and equipment that is owned or leased by the Bank. Internet Banking & Mobile Banking facilities are available to our customers on the basis of the eligibility norms fixed.

Product Name of Internet Banking & Mobile Banking

Product name for the Internet Banking services is named as "IndNetBanking" and services are being enabled through the Bank's website https://www.indianbank.net.in. Product name of the Mobile Banking service is "IndOASIS/IndPay". IndOASIS mobile application has the combined features of IndPay and erstwhile BHIM Indian Bank UPI application. The Mobile applications can be installed in smart phones with operating systems Android and iOS. Compliant versions of Android and iOS Operating Systems shall be decided by security guidelines issued by RBI / NPCI/ other regulatory organisations.

4.3.1. Benefits

Benefits for the Bank:

- Efficient and cost effective delivery mechanism of select banking services
- Widening retail reach: It removes the traditional geographical barriers as it could reach out to customers globally.
- Rapidly increasing retail customer base.
- Customer transition to electronic channels.
- Deepening relationship.

- Improving internal systems

Benefits for the customers:

- No necessity to go to the bank for non-cash transactions.
- Banking in the comfort of home/ office/ anywhere / anytime in the world.
- Funds Transfer, e-TDA, Bill Payment, Statement of account, Lodging Request for cheque book, Status enquiry for issued/deposited cheques, Standing Instruction, etc.
- Online availability of Information about the Bank and the products
- Various services are offered through Internet banking & Mobile Banking. New services are introduced based on emerging technologies, customer requirements, Business needs etc.

4.3.2. Fund Transfer Limits

The default Fund Transfer Limit for Internet Banking is Rs.10 Lakhs. All new Internet Banking users shall be created with the default limit of Rs.10 lakhs. For existing users, provision will be provided to branches to enhance the default limit up to Rs.10 lakhs in due course.

Retail Net Banking (RNB)

Transaction Limits for transactions through Retail Net Banking application shall be as follows:

Type of Internet Banking	**Fund Transfer Mode**	**Per-day Limit (in Rs)**
Retail Internet Banking	Cumulative per-day limit	10,00,000
	NEFT/RTGS	10,00,000

	IMPS	2,00,000
	Tax Payment	No limit
	Other Merchant Payments (Third Party)	10,00,000
	Fund Transfer without Beneficiary addition (EasiPay)*	10,000

**Beneficiary added in Retail Net banking will be activated only after 4 hours. Provision will be made in RM Module for branch to activate beneficiary with due diligence upon receipt of request letter from customer.*

Corporate Net Banking (CNB)

Transaction Limits for transactions through Corporate Net Banking application shall be as follows:

Type of Internet Banking	Fund Transfer Mode	Per-day Limit
Corporate Internet Banking	Cumulative per-day limit	As per customer's requirement, customer will mention the required per-day transaction limit in the Corporate Internet Banking application form. Zonal Manager can sanction up to Rs.100 Crores
	NEFT/RTGS	
	Other Merchant Payments (Third Party)	
	IMPS	Rs.2,00,000*
	Tax Payment	No limit

The above funds transfer limits are applicable to per Customer ID (CIF) per day irrespective of the number of accounts linked to the CIF/ mapped to the User. There is no restriction on the number of transactions per day. In the

case of Government transactions, the per day funds transfer limit is not applicable for all the above categories.

Mobile Banking (with end to end encryption)

Banks are free to set their own limits as per RBI circular RBI/2011-12/312 DPSS.CO.PD.No 1098/02.23.02/2011-12 dated 22.12.2011. Transaction Limits for transactions through Mobile Banking application shall be as follows:

Channel	**Fund Transfer Mode**	**Per-day Limit (in Rs)**
Mobile Banking	Cumulative per-day limit	5,00,000
	NEFT	5,00,000
	IMPS (included in Mobile Banking Cumulative per-day limit)	2,00,000
	Fund Transfer without Beneficiary addition (EasiPay)*	10,000
Unified Payment Interface (UPI)	Unified Payment Interface (UPI)	1,00,000 (2,00,000 for ASBA)

Beneficiary added in Mobile banking will be activated only after **4 hours. Provision will be made in RM Module for branch to activate beneficiary with due diligence upon receipt of request letter from customer.*

4.3.3. Roles & Responsibilities

CO: Information Technology Department will be looking after implementation and technical aspects. Functional aspects relating to

operations and defining Terms and Conditions thereof, will be looked after by CO: Digital Banking Division. CO: Information Systems Security Cell will be devising the security aspects and CO: Inspection Department will be assessing the security periodically.

Custodian for the Policy:

To devise, implement and review various aspects of the policy, as approved by the board, there needs to be functional custodians. Department Head of DBD as functional in-charge of Internet Banking & Mobile Banking will be the custodian of the policy. However any change or modification of the policy will be approved by IT Strategy Committee / Audit Committee of the Board.

4.3.4. Standards & Guidelines

The standards and guidelines provide the various parameters for smooth and secured functioning of Internet Banking & Mobile banking. The Customer Aspects on Eligibility, Access rights, Terms and Conditions for operation and Procedures based on KYC norms and RBI directives forms part of the Net banking / Mobile banking facility provided to customers. Infrastructure and connectivity aspects comprising of various layers as follows:

- Browser
- Firewall
- Web Server
- Application Server
- Database Server
- Internal Network
- Data Center
- Software for internet banking which include eBankWorks – an Internet Banking Solution developed by TCS, Various services being offered on

SMS and WhatsApp, Database linked to the Core Banking Applications (BANCS)

- Other resources which include People, Processes etc.

Infrastructure and Connectivity aspects

The Information security parameters are elaborated in detail in the policy below along with the guidelines and are based on a multi-layered concept, on the premise that each financial transaction uses multiple layers of security and every layer adds a different technology resulting in a trusted system that is monitored at all times. The security guideline for each layer is prescribed separately. Compliance of an individual layer per se does not ensure security to that layer unless all the interlinked layers are complied.

Standards and Security guidelines of Internet Banking

Internet Banking application servers are hosted in our Data Center in three tier architecture of Web, Application and Database. Web servers are kept in DMZ (De-Militarized Zone). A dedicated internet link for connecting the web server from Internet Cloud is provided at our Data Center. Firewall in High availability mode in the Internet Banking Segment is made available. Network Intrusion Prevention Systems for monitoring the Internet Banking system and Host Intrusion Detection Systems placed in critical servers of Internet Banking

Security features available in Internet Banking & Mobile Banking

Our Bank has taken several security measures as per details given below for protecting the customers while using the online channel for transactions through Internet:

[i] Antiphishing measures

- Anti-bot Captcha is introduced in Login Page to avoid brute-force attack.
- Dynamic Virtual Keypad in our Login Page for those customers accessing from cyber-cafes or shared networks.
- Right Click and Menu Bar disabled to avoid copying/ duplication of the HTML source codes.
- To enforce better security to the customers, the login page has been segregated into two screens. In the first screen the user has to enter user-id and anti-bot captcha. User will be prompted to enter the password only in the next screen.
- Display of necessary Security Tips in the Internet Banking Home Page about Phishing Attacks for customer education and guidance on how to avoid such attacks like "Not to part with details of personal credentials on any site other than the login page of Internet Banking site".

[ii] Encrypted Communication

- Our Bank uses digital certificate with RSA 2048 bit encryption facility to ensure security of online transactions and confidentiality of the data of Internet Banking Customers.
- Extended validation Certificate from internationally accepted certifying authority which, in addition to the existing lock symbol, will display the URL bar in green colour for genuine sites. In the case of phishing sites, the URL bar will be displayed in Red colour in higher versions of browsers.
- "URL Hashing is done using SHA1" or higher standards with SALT hashing to encrypt all URL requests from the Customers Browser to the Internet Banking Server.

- Password encryption using SHA1 or higher version with Salt Hash Algorithm before transmission.

Distributed Denial of Service (DDoS) facility is being availed from the Internet Service Provider to avoid disruptions to the net banking services due to Denial of Service attack as enhanced security measure.

[iii] Customer Education

In the age of the self-service model of banking, the customer has to be equipped to do safe banking through self-help. It is often said that the best defence against frauds is customer awareness. Security awareness is the understanding and knowledge of the threats to sensitive personal information of the customer and the protection measures to be adopted. Hence customer awareness activities are taken up on an ongoing basis, using a variety of delivery methods to educate customers, general public and Bank employees. As mentioned in RBI Working Group guidelines on Information Security, awareness education is being provided for more understanding response to customer complaints to other stakeholders such as law enforcement personnel who can act as resource persons for customer queries and to media for dissemination of accurate and timely information.

[iv] User-ID related

- Facility to change the User ID to "Preferred User ID" as per the customer's choice.
- Locking of User ID in case of 3 unsuccessful login attempts.

- Automatic Unlocking of locked User IDs every day at 5:00 AM and 5:00 PM.
- Session timings of 20 minutes for Active Session and 10 minutes for Idle Time Out for Internet Banking and 2 minutes for IndOASIS / IndPay .
- User status changes to "DORMANT" state on non-usage of the Internet Banking facility within 15 days from the date of activation of User ID.
- Facility to transfer funds only to added Beneficiary Accounts (for all funds transfer to other customers' accounts within Indian Bank and for RTGS / NEFT / IMPS / UPI Transactions).
- Facility to Transfer Funds without adding Beneficiary Accounts (funds transfer to other customer's accounts within Indian Bank and IMPS) up to Rs.10,000/-.
- Separate Services for each type of transaction and individual restrictions to account types in each category.

[v] Password related

- Forced Password Change during the First Login attempt and forced password change every 180 days (both Login & Transaction passwords).
- Separate Login and Transaction Passwords for View and Funds Transfer Facility
- Automatic disabling of "AUTO COMPLETE" option in case of User ID and Passwords
- Preferred User ID and passwords cannot be the same
- The login and transaction password should not match with the previously used 3 passwords.

[vi] Two Factor Authentication in Internet Banking

In the recommendations of Working Group of RBI on Information Security, One Time Password as second factor of authentication has been recommended. On account of increasing incidents of phishing attempts, One Time Password to be delivered through mobile has been extended to all the fund transfer transactions under Retail Net Banking except fund transfer transactions relating to TNEB or other statutory related transactions. As per specific mandate from customers, OTP is being delivered through E-mail also. Maker and Checker concept had been introduced for corporate customers. Apart from Maker and Checker, One Time Password (OTP) is introduced as additional factor of authentication for Corporate Customers.

The working group also discusses introduction of Risk Based Authentication in Internet Banking. Feasibility of implementing Risk Based Authentication shall be looked at and necessary steps will be taken for implementing the same. Bank is implementing Fraud Risk Management solution covering CBS and delivery channels like internet Banking, mobile banking, ATMs, credit cards etc. for transaction monitoring, analysing frauds etc. as suggested in RBI Working Group guidelines on Information security.

Security features built in the Mobile Banking Application following the RBI guidelines on Mobile Banking

IndOASIS / IndPay mobile application is compatible with all latest model mobile phones with operating system of Android and iOS. IndOASIS / IndPay application complies with RBI Guidelines. The IndOASIS / IndPay Application is protected by SSL certificate. The data transfer between client hand set and Bank's Middleware server is over https connection. IndOASIS / IndPay is introduced with device binding where by the customers can register only through the mobile device having the mobile number which is registered with our Bank. The registration to the Mobile Application will be allowed by

validating the ATM Card Credentials or Internet Banking Credentials or existing Mobile Banking credentials. M-PIN is a 4-digit numerical password which is set by the customer at the time of registering for IndOASIS / IndPay. MTPIN is Mobile Banking Transaction PIN which is a 4 digit number set by the customer at the time of registration.

After 3 incorrect attempts of M-PIN, the status of M-PIN will get locked. Locked M-PIN will be released by an automated process at 5.00 AM and at 5.00 PM daily. The MPIN and MTPIN are stored in Bank's Database Server in hashed form. The Authentication of PINs is happening in Bank's Server.

Contingency and Continuity Planning/ Disaster Recovery Drills

The contingency and continuity planning for Internet Banking and Mobile Banking Services will be part of the overall contingency and continuity planning of the Bank. D R Drills for Internet Banking and Mobile Banking are part of disaster recovery drills being conducted for CBS. The drills are conducted two times in a year as per RBI guidelines. During the D R Drill, the services are provided from the infrastructure at the D R site at Mumbai.

4.3.5. Privacy Policy

Customers' privacy is very important to Indian Bank (hereinafter referred as the Bank). Privacy Policy is ported in Indian Bank's corporate website. The Bank is committed to the Privacy Promise for Customers, which is as under:

Indian Bank Privacy Promise for Customers

While information is the cornerstone of our ability to provide superior service, our most important asset is our customers' trust. Keeping customer information secure, and using it only as our customers would want us to, is a

top priority for all of us at the Bank. Here then, is our promise to our customers:

1) The bank or its contractors may hold & process customer's personal information on computer or otherwise in connection with IndNetBanking & Mobile banking services as well as for statistical analysis and credit scoring.
2) The bank will safeguard, securely and confidentially, any information our customers share with us. The bank will continue to maintain its tradition of not sharing the transaction information in customers' account with anyone except when required by law or statutory agencies.
3) The bank will limit the collection and use of customer information to the minimum we require for delivering effective service to our customers, to administer our business and to advise our customers about our products, services and other safeguards.
4) The bank will give access to customer information to only those employees who are authorized to handle the customer information. Employees who violate our Privacy Promise will be subject to our normal disciplinary process.
5) The bank will not reveal customer information to any external organization unless the bank has previously informed the customer in disclosures or agreements have been authorised by the customer or as required by the law and statutory authorities.
6) The bank will always maintain control over the confidentiality of the customer information. The bank may, however, facilitate relevant offers from reputable companies for product promotion jointly/tied up with the bank.

7) Whenever the banks hire other organizations to provide support services, the bank will require them to conform to our privacy policy standards.
8) For purposes of credit reporting, verification and risk management, the bank may exchange information about our customers with reputed and clearinghouse centres.
9) The bank will exercise due diligence about ensuring the accuracy of the information collected.
10) The bank will ensure that customer data stored with the bank will be protected from any malicious activities/hacking attempts.
11) The bank will continuously assess to ensure that customer privacy is respected and will conduct the business in a manner that fulfils the bank's Promise.

4.3.6. Audit & Compliance

Auditing Internet Banking and Mobile Banking Application

Additional delivery channels have been added using the infrastructure of Internet banking and the architecture has been strengthened by introducing Firewalls and NIPS. Anti-phishing monitoring is also being carried out. The application, infrastructure and the architecture are being regularly audited by Cert-In empanelled auditors under periodical Information System Audits taken up by the Inspection Department for compliance to I S Security Policy and the RBI guidelines with reference to the following circulars: DBOD No. Comp.BC.130/07.03.23/2000-01 dated June 14, 2001 DBOD No. Comp.BC.14/07.03.29/2005-06 dated July 20, 2005 DBS.CO.ITC.BC.No. 6 / 31.02.008/2010-11 dated April 29, 2011 In order to establish effective control mechanisms, the following audit/tests must be conducted either internal or external:

- Pre-Launch audit
- Periodic audit
- External Penetration
- Internal Penetration
- Process audit
- Infrastructure Audit

The appointment of Auditors and the functional areas of Audit will be as per the Information Systems Audit Policy of the Bank. The issues if any, pointed out by the auditors are immediately attended and compliance reported. As part of net banking and mobile banking applications, audit log is maintained for transactions conducted by each customer id and administrator Id. All the audits conducted by internal and external auditors would be preserved for RBI / AFI inspection.

Compliance

The Policy conforms to the guidelines on Internet Banking and Mobile Banking by Reserve Bank of India. Wherever a specific mention is not made herein, Reserve Bank of India guidelines for Internet Banking will hold good as far as it is applicable to the environment. The various standards and guidelines enumerated in the policy are to be strictly adhered by all the parties concerned. The custodians of the Policy are empowered to formulate additional guidelines or modify the existing guidelines as and when required and any technological advancement or modification takes place and any new product introduced through Internet Banking / Mobile Banking by following the procedures and after approvals.

4.3.7. Disclaimer Clause

When internet banking and mobile banking are provided to the customer, the Bank must take all the precautions as to the confidentiality and integrity of the information. Adequate precautionary measures must be undertaken to ensure a secured login procedure and confidentiality of information provided to the customer. The information provided to the customer must be only through the Bank's website and Mobile APP and only from the data available at the Bank, thus ensuring integrity. The confidentiality of the information provided through internet is based on the premise that the customer only has logged in using his user-id and password. The bank cannot substantiate any proof as to the physical identity of the customer and thus furnishing information through internet may lead to disputes as to the confidentiality. Besides, there is a chance of external intrusion which is beyond the control of the Bank. To overcome such unwanted, unforeseen situations, the login procedure a disclaimer clause has been included as below:

- "The contents on this site have been provided for general information. The information and materials contained herein, and the terms, conditions and descriptions that appear are subject to change. Those who would like to have additional information or latest development may contact the Bank. The information and materials contained herein including text, graphics, links or other items are provided as is and as available. The Bank does not warrant the totality and absolute accuracy, adequacy or completeness of this information and materials and expressly disclaims any liability for errors or omissions in this information and materials herein.
- While the bank will take every effort to give the correct information, The Bank does not accept any legal liability whatsoever based on materials herein. The Bank does not accept any legal liability whatsoever based on any information contained herein. The Bank is

not liable for non-availability of services due to reasons beyond the controls of the bank."

- The hyperlinks in Internet Banking will lead to resources located on servers maintained and operated by third parties over whom Bank does not have any control and bank accepts no responsibility or liability for any of the material contained on those servers.
- The hyperlink is provided is for the user convenience and will direct user to websites operated by third parties who may or may not be a part of Bank.
- Users will be using such hyperlinks and third party websites at their own risk and Bank will not be liable for any damages or losses, direct or indirect, arising out of or in connection with it.
- Bank is not in any way liable for the contents of any of these linked websites or Web Pages. By providing hyperlinks to an external website or webpage, Bank shall not be deemed to endorse, recommend, approve, guarantee, indemnify or introduce any third parties or the services/products they provide on their websites.
- When user click on the link to the external websites, user will be leaving the Bank's website and Bank Policies, terms & conditions, disclaimers will cease once user leave our website.
- Bank is not a party to any contractual arrangements entered into between user and the provider of the external website unless otherwise expressly specified or agreed to by Bank. Such external websites are governed by their respective policies.

4.3.8. Third Party & Outsourcing Services

Identification of issues

Any application related issues identified by the Internet Banking and Mobile Banking are raised to the respective service providers and/or application provider. Depending on the severity of the issue, necessary priority is assigned and escalated to respective service providers for fixing the issue. Root cause analysis (RCA) of the issue has to be obtained from the service provider forming part of incident report. The modifications required/ envisaged will be authorized by the AGM / Chief Manager before placing the request to the service provider. If the issue is of High Priority, necessary steps are taken for fixing the issue on immediate basis. Medium Priority issues are normally fixed at the end of the day. The issues are raised through online issue tracking system with the Service Providers and the same are recorded in the Patch Release Note (PRN) during application of the patch.

Enhancements / New modules

Based on new requirements envisaged, Software Development Life Cycle (SDLC) approach for development, User Acceptance Test and roll out to Production environment is followed. The enhancements are raised through email and the same are recorded in the Patch Release Note (PRN) during application of the patch.

Assurance from the application vendor that the application is free from embedded malicious/ fraudulent code, will be obtained periodically along with all new developments and enhancements. As per the new requirements raised by the User Departments for introduction of new facility/ module, necessary Administrative approval approved by the competent authorities is provided to CO: DBD by the respective User Departments. Based on the requirements (as per the discussions/ meetings held with the User Department) (or) requirements document / integration document supplied

by the User Departments, request is raised for development of new module. New modules ported in production are recorded in the Patch Release Note (PRN) during application of the patch.

Patch testing / release

The patch is tested and released for UAT based on the issue escalated to the application vendor. The code released is reviewed by another member in their team (or) team leader before releasing the patch to UAT. The patch is deployed in UAT/ test environment and tested for the functionality of the patch by integrating the same with the production Enterprise Archive (.ear) file. The Patch Release Note (PRN) released is signed and necessary approval obtained from AGM / Chief Manager for porting the same in production at Data Centre. The test results of all the patches released are provided to the internal auditor for review at the end of the month.

Functional testing would be performed by Bank officials as part of UAT before releasing any patch to production. The details of patches applied in production would be shared with the internal auditors on a monthly basis. The same shall also form a part of monthly report of e-banking channel activities submitted to the Department Head.

Monitoring of Internet Banking Website

The internet banking services are being monitored at various levels which are detailed below:

1) Internet banking website is being monitored by the Bank's performance monitoring Service Provider to know the performance levels and to maintain uptime.
2) Monitoring of phishing sites is being carried out by our Bank's security operations service provider.

3) DDoS filtering services have been availed from the Bank's internet Service Provider to monitor network traffic of internet banking segment.

4.3.9. Termination / Suspension / Withdrawal of service

The users may de-register from the facility of Internet Banking and Mobile Banking by giving a request/notice to Branch in writing requesting termination and disabling the Internet Banking/ Mobile Banking facility. The Branch will terminate the facility immediately after receipt of the request/notice and provide acknowledgement to customer with date and time. For De-registration of IndOASIS/UPI, user has to deregister through the option provided in the app. The user will remain responsible for any transactions made on his account(s) through Internet Banking / Mobile Banking prior to the time of such cancellation of the Internet Banking services.

The Bank may withdraw the Internet Banking/ Mobile Banking/UPI services facility anytime, provided the user is given reasonable notice under the circumstances. If the Internet Banking service / Mobile Banking is withdrawn by the Bank for a reason other than the breach of the terms and conditions by the user, the Bank's liability shall be restricted to the return of the annual charges, if any, recovered from the user for the period in question. Bank can disable/ suspend the facility to the Internet Banking/ Mobile Banking user, if the facility is withdrawn by the Bank. The reason for withdrawal shall not be questioned by the User. The decision taken by the Bank for withdrawing the facility shall be final. The Bank may suspend or terminate Internet Banking/ Mobile Banking facilities without prior notice if the user breaches the terms and conditions or the Bank learns of the death or lack of legal capacity of the user.

4.4 Debit Cards

ATMs and Debit cards constitute the most used Alternate Delivery Channel in the Banking Industry today. As a result of the increase in the number of avenues for usage of cards and the initiatives like Financial Inclusion and

Promotion of Digital Transactions, the number of users and transactions through the debit card has increased manifold.

Following are the benefits to the Bank from increased usage of debit cards by our customers:

1. Reduction in the transactions across the counter.
2. The extra manpower can be utilized for other development work of the Bank.
3. Reduction in the cost of operations.
4. Non-interest income by way of Annual Maintenance Charges and issuer interchange fee (for POS transactions).

The policy is issued to provide the branches with information on various debit card products of our Bank and the rules and regulations applicable on debit cards. Policy covers the following aspects related to debit cards:

1. Eligibility criteria for issuing debit cards.
2. Various debit card products and daily usage limits.
3. Guidelines on issuing and delivering the cards through DCMS.
4. Transaction security and risk mitigation.
5. Co-branded debit cards.

4.4.1. Eligibility Criteria for issuing Debit Cards

Eligible accounts / customers:

Debit cards can be issued to the following categories of customers:

1. All Individuals having savings bank / current accounts / Proprietorship accounts including visually challenged and illiterate customers.
2. Minors above 12 years, if the account is opened under "IB Smart Kid".
3. Add on cards can be issuer in the second customer's name, for accounts opened under E or S, A or S.
4. Non-resident account holders.
5. Kisan Credit Card customers.
6. Mudra account customers.

The instructions/ guidelines on KYC/AML/ CFT applicable to banks, issued by RBI from time to time, may be adhered to in respect of all cards issued, including co-branded debit cards.

While opening the BSBDA accounts, branches should educate such customers about the ATM Debit Card, ATM PIN and risk associated with it. However, if customer chooses not to have ATM debit card, branches need not force ATM debit cards on such customers. If, however, customer opts to have an ATM debit card, branches should provide the same to BSBDA holders through safe delivery channels by adopting the same procedure being adopted for delivery of ATM debit card and PIN to other customers.

Ineligible accounts / customers:

Debit cards should not be issued to the following categories of customers:

1. Cash credit / loan account holders

2. Joint accounts where accounts are operated by jointly or more than one signatory.
3. Accounts of Company, Partnership Firms, Associations, Trusts, HUF, Clubs, Government Departments, etc.
4. Accounts in the name of minors (Jointly or severally), except "IB Smart Kid" accounts.
5. Accounts operated upon by Mandate or Power of Attorney.
6. Accounts subjected to litigation/dispute.
7. Accounts attached by a Garnishee/Attachment order.
8. Accounts where no debits are permitted.
9. Encumbered accounts.
10. Accounts of suspended employees (disciplinary action initiated/pending).
11. Accounts for which Debit cards facility was withdrawn earlier because of unsatisfactory conduct of the accounts.

RBI, vide their circular dated 23.04.2020, has permitted banks to issue electronic cards to natural persons having Overdraft Accounts that are only in the nature of personal loan without any specific end-use restrictions. The card shall be issued for a period not exceeding the validity of the facility and shall also be subject to the usual rights of *t*he banks as lenders.

The electronic card for Overdraft Accounts in the nature of personal loans will be allowed to be used for domestic transactions only. The usage of such cards is restricted to facilitate online/ non-cash transactions. However, the

restriction on cash transaction will not apply to overdraft facility provided along with Pradhan Mantri Jan Dhan Yojana (PMJDY) accounts.

Bank will issue the above debit cards for OD accounts after framing the terms and conditions and risk management measures and grievance redressal mechanism etc.

International debit cards should be issued only after obtaining specific request from the customers who intent to travel abroad. Issue of international debit cards will also be subject to directions issued under Foreign Exchange Management Act, 1999, as amended from time to time.

4.4.2. Guidelines for issuing & delivery of cards through DCMS

Depending on the card product, request for debit cards should be submitted through CBS or DCMS as mentioned in the below table:

No.	Card Product	First card	Duplicate Card / Re-issue
1	Contactless debit cards (RuPay Platinum domestic/ International cards, Rupay Debit Select Cards and RuPay Kishore Domestic cards)	Through CBS	Through DCMS, if the account is already having a RuPay Contactless debit card.
			Through CBS, if the account does not have a RuPay Contactless debit card.
2	MasterCard World Debit Card, RuPay PMJDY, RuPay Mudra, RuPay Pungrain and IB Surabhi cards.	CBS	DCMS

3	RuPay Insta Debit Card (Contactless)	DCMS & CBS	DCMS
4	RuPay Insta Debit Card (Contact)	DCMS	DCMS
5	RuPay KCC with photo	DCMS	DCMS
6	RuPay KCC without photo	CBS	DCMS
7	RuPay Senior Citizen with Photo	DCMS	DCMS
8	MasterCard e-purse	Net Banking	DCMS
9	RuPay IB-Digi	Bank's website	DCMS
10	MasterCard customized Image Card	Bank's website	Bank's website

- All cards will be issued with Green PIN in normal course. However, branches can request for paper PIN mailer if there is no ATM available near the branch for setting Green PIN.
- On receipt of the cards & PIN, branches shall update the receipt in DCMS and keep the cards and PIN under dual custody of designated officers.
- On delivery of the cards / PIN to customers, the status shall be updated in DCMS for activating the card. No card shall be delivered to customers without activation.
- Cards not delivered to customers within 120 days from date of receipt will be hot-listed automatically for security reasons (except Rupay PMJDY debit cards). Branches shall destroy such cards and PINs physically and record in the register.

4.4.3. Security & Risk Mitigation

With the increase in number of debit card holders and transaction channels, there is also an increase in the number of frauds and unauthorized usage of debit cards. Various types of frauds are being reported in the industry, with the Modus Operandi ranging from customer- targeted activities such as card skimming and vishing, to large scale attacks targeting the Banks such as ATM Cash Out attacks & Man in the middle attacks.

With new security threats emerging regularly, Banks are also making all efforts to secure the payment systems and customer data from attacks and to prevent cyber-attacks on the payment eco system and to avoid financial and reputational risks to the Bank. Reserve Bank of India is issuing various guidelines for strengthening the Information System Security procedures of the Banks.

Hence the following measures are adopted to enhance the security of card transactions:

- While issuing, all new debit cards will be enabled for use only at contact based points of usage [viz. ATMs and Point of Sale (PoS) devices] within India.
- Other transaction facilities such as online transactions, international transactions (on international cards) and contactless purchases will be disabled by default.
- Based on the written request from customers, branches can select the additional facilities and set the daily usage limit for all types of transactions, while activating the cards in DCMS. Any subsequent changes can also be done through DCMS as a card modification request.

Facilities enabled by default	**Facilities to be enabled on Customer's request**
ATM transactions in India	Online transactions in India (E-Com)
POS Purchase in India	Transactions outside India (Only for International Debit Cards)
Cash at POS and Purchase with Cash back in India	Contactless transactions (Only for Contactless Debit Cards)

- Customers can also enable / disable the transactions and set the daily usage limits by logging in to their internet banking or mobile banking facilities.

- Debit cards issued before 01.04.2020 but not used for online transactions or international transactions at least once during the last financial year will be disabled for online transactions or international transactions (as applicable) before 30.04.2021.

- If those customers want to enable the above features for their card, they can send the request to the branch for enabling the same through DCMS portal or enable the facility through their net banking user ID / Password.

- Transactions on all new and existing debit cards will be restricted to 5 transactions in ATMs and 10 transactions in POS (Including E-com) per day.

- Limits are set in the Fraud Risk Management (FRM) Software of ATM EFT Switch for generating alerts based on the transaction velocity. Below are some of the limits set based on transaction velocity.

- Alerts will be generated for transactions done at abnormal time period for amount above Rs.20,000.
- Alerts will be generated for transactions done between 11 PM and 12 AM for amount above Rs.25,000.
- Alerts will be generated for Card to Account fund transfers done between 12 AM and 6 AM and between 10 PM and 12 AM for amount above Rs.50,000.
- Alerts will be generated when transaction volume exceeds 2 transactions and cumulative transaction value exceeds Rs.20,000 between 12 AM and 6 AM.

- Similarly, transactions will be restricted in specific geographical locations (countries & cities) by setting the rules in the FRM Software of ATM EFT Switch. Below are some of the restrictions set based on the geographic locations of origination of transaction:
  - Transactions are not permitted from different countries within 1 hour.
  - By default, transactions are not permitted in high risk countries such as China, Cambodia, Thailand, Panama, Indonesia, Hungary and Kenya. Branches can submit online request through ATM website for enabling transactions in these countries based on specific request received from the card holder
  - Card Not Present (e-com) transactions are not permitted if originated from Brazil.
  - Only 3 transactions will be permitted in a day if the card is used abroad.

- Cards cannot be used for more than 5 times within 72 hours in cities with Maoist presence.
- POS transactions originated within India, but without PIN, will be declined.

- Based on the alerts generated in the FRM application, our 24x7 call center team will try to contact the customer to verify the genuineness of the transactions and to block the cards if the transactions are not initiated by the customer. If the call center agents are unable to contact the customer, they will change the card to RESTRICTED status to prevent further financial transactions on the card.

  Branches can verify the card status from the card enquiry menu available in the DCMS login, by searching using the card number. If the card status is OPEN but switch status is RESTRICTED, branches can send an e-mail request to atm_alerts@indianbank.co.in to get the list of the suspicious transactions, confirm the genuineness of the transactions with the customer and then send another request to remove the card from RESTRICTED status.

4.4.4. Co-branded Debit Cards

Co-branded debit cards can be issued in association with partner entities such as educational institutions and corporates. These cards will have logos our Bank, the non-banking entity and card network (RuPay / MasterCard). Special features like RFID based access control cards can be provided using the co-branded cards.

Issuance of co-branded debit cards will be subject to the following terms and conditions:

- The Co-branding partner shall be selected after evaluating the various risks associated with the arrangement with the partner, including reputation risk.
- Bank will carry out due diligence in respect of the non-banking entity with which the bank intends to enter into tie-up for issue of co-branded debit cards to protect the bank against the reputation risk the bank is exposed to in such an arrangement.
- Suitable risk mitigation measures shall be put in place after obtaining risk clearance from the competent authority.
- In cases where the proposed co-branding partner is a financial entity, it should obtain necessary approvals from its regulator for entering into the co-branding agreement.
- Outsourcing of activities: Bank would be liable for all acts of the co-branding partner.
- Role of non-bank entity: The role of the non-bank entity under the tie-up arrangement should be limited to marketing/ distribution of the cards or providing access to the cardholder for the goods/services that are offered.
- Confidentiality of customer information: Bank should not reveal any information relating to customers obtained at the time of opening the account or issuing the card and the co-branding non-banking entity should not be permitted to access any details of customer's accounts that may violate bank's secrecy obligations.

4.4.5. Processing of e-mandates for recurring transactions

Bank will provide the customers with the facility of processing e-mandate on debit cards without additional factor of authentication (OTP). The process

will involve registration of e-mandate and completion of first payment using OTP authentication. Subsequent recurring payments will be initiated by the merchants and will be completed without OTP authentication. Customers will be able to modify or revoke the e-mandates online. The maximum permissible limit for a transaction under this arrangement will be Rs.5,000/-.

4.5 Prepaid Cards

Prepaid Payment Instruments (PPIs) are payment instruments that facilitate purchase of goods and services, including financial services, remittance facilities, etc., against the value stored on such instruments. PPIs may be issued as cards, wallets, and any such form/ instrument which can be used to access the PPI and to use the amount therein.

In the light of developments in the field, progress made by PPI Issuers and experience gained, and to foster innovation and competition, ensure safety and security, customer protection, etc., RBI had issued Master Directions on the subject of Issuance and operations of PPIs vide Ref: DPSS.CO.PD.No.1164/02.14.006/2017-18 dated 11.10.2017 (updated as on 29.12.2017).

RBI has mandated in the Master Directions on Issuance and Operation of PPIs that Bank should have a clear laid down policy, duly approved by their Board, for issuance of various types / categories of PPIs and all activities related thereto. The purpose of this policy is:

- To provide a framework for issuance of PPIs by the Bank.
- To implement and operate PPIs in a prudent manner while taking into account safety and security of transactions as well as systems along with customer protection and convenience.
- To provide for harmonization and interoperability of PPIs.

4.5.1. Definition & Classification

For the purpose of this Policy, the following definitions shall be applicable:

Classification of PPIs:

PPIs issued in the country are classified under three types viz. (i) Closed System PPIs, (ii) Semi-closed System PPIs, and (iii) Open System PPIs.

- Closed System PPIs: These PPIs are issued for facilitating the purchase of goods and services from a specific entity only and do not permit cash withdrawal. As these instruments cannot be used for payments or settlement for third party services, the issuance and operation of such instruments is not classified as payment systems requiring approval / authorization by the RBI.
- Semi-closed System PPIs: These PPIs are used for purchase of goods and services, including financial services, remittance facilities, etc., at a group of clearly identified merchant locations / establishments which have a specific contract with the Bank (or contract through a payment aggregator / payment gateway) to accept the PPIs as payment instruments. These instruments do not permit cash withdrawal.
- Open System PPIs: These PPIs are used at any merchant for purchase of goods and services, including financial services, remittance facilities, etc. These PPIs permit cash withdrawal at ATMs / Point of Sale (PoS) / Business Correspondents (BCs).

Our Bank is issuing only Open System PPIs in the form of RuPay Prepaid Cards (IB Cash Card), which can be used in any ATM and POS terminals connected to the RuPay network of NPCI.

- Holder: Individuals / Organizations who obtain / purchase PPIs from the Bank and use the same for purchase of goods and services, including financial services, remittance facilities, etc.

- Limits: All 'limits' in the value of instruments stated in this Policy indicate the maximum value of such instruments, denominated in INR, that shall be issued to any holder, unless otherwise specified.

4.5.2. Issuance, Loading & Reloading

1. Reloadable or non-reloadable Open System PPIs can be issued by the Bank based on business requirements.
2. Bank's name will be prominently displayed along with the PPI brand name in all instances.
3. No interest will be paid on PPI balances
4. PPIs can be loaded / reloaded by cash, by debit to a bank account, by credit and debit cards, and other PPIs (as permitted from time to time). The electronic loading / reloading of PPIs shall be through above payment instruments issued only by regulated entities in India and shall be in INR only
5. Cash loading to PPIs is limited to Rs.50,000/- per month subject to overall limit of the PPI.
6. Reloading of PPIs is permitted at branches. Provision of reloading of PPIs through Internet banking and Mobile banking shall be provided in due course.
7. Preservation of records and confidentiality of customer information shall be ensured by the branches issuing the PPIs.
8. There shall be no remittance without compliance to KYC requirements. It should be ensured that new PPIs are not created each time for facilitating cash-based remittances to other PPIs/ bank accounts. PPIs created for previous remittance by the same person shall be used.

4.5.3. Validity, Redemption, Limits and Refund

Validity and Redemption

- All PPIs issued by the Bank have a minimum validity period of one year from the date of issuance of the PPI.
- PPI holder will be cautioned at reasonable intervals, during the 45 days' period prior to expiry of the validity period of the PPI. The caution advice shall be sent by SMS / e-mail / post.
- Instructions on Depositor Education and Awareness Fund issued by Department of Banking Regulation, RBI, vide, circular DBOD. No. DEAF Cell. BC. 101/ 30.01.002/ 2013-14 dated March 21, 2014, as amended from time to time should also be followed for PPIs.
- The expiry period of the PPI shall be clearly conveyed to the customer at the time of issuance of PPIs. Such information is clearly enunciated in the terms and conditions of sale of PPI. It shall also clearly outlined in the Bank's website.
- PPIs with no financial transaction for a consecutive period of one year are made inactive after sending a notice to the PPI holder/s. These can be reactivated only after validation and applicable due diligence. These PPIs are being reported to RBI separately.
- Bank will not dishonour customer instructions for payments/transfer of money, at approved locations, if there is sufficient balance outstanding against the instrument.
- The holders of PPIs shall be permitted to redeem the outstanding balance in the PPI, if for any reason the scheme is being wound-up or is directed by RBI to be discontinued.

Transaction Limits

- All financial limits indicated against each type / categories of the PPI are strictly adhered to.
- The limit on cash withdrawal and purchase of goods and services using PPIs are defined as per the limits applicable on Debit cards and the holder is allowed to use the PPI for these purposes within the overall PPI limit applicable.

Handling Refunds

- Refund requests for the transactions performed using RuPay Prepaid cards are being handled by CO: ATM Service Centre.
- Refunds in case of failed / returned / rejected / cancelled transactions shall be applied to the respective PPI immediately, to the extent that payment was made initially by debit to the PPI, even if such application of funds results in exceeding the limits prescribed for that type / category of PPI. However, refunds in case of failed / returned / rejected / cancelled transactions using any other payment instrument shall not be credited to PPI.
- Complete details of such returns / refunds, etc. are being maintained and the same is being provided to RBI as and when called for.
- Necessary systems will be put in place to monitor frequent instances of refunds taking place in specific PPIs and should be substantiated with proof for audit / scrutiny purposes.

4.5.4. Categories of PPIs permitted by RBI:

Prepaid meal instruments:

Bank can issue PPIs in the form of prepaid meal instruments. It shall be ensured that these are issued only as semi-closed PPIs, are in electronic form and reloadable. No cash withdrawal or funds transfer shall be

permitted from such instruments. Such PPIs need not be issued as a separate category of PPI.

Gift instruments:

Banks shall issue prepaid gift instruments subject to the following conditions:

- Maximum value of each prepaid gift instrument shall not exceed Rs.10,000/-.
- These instruments shall not be reloadable.
- Cash-out or refund or funds transfer shall not be permitted for such instruments.
- KYC details of the purchasers of such instruments shall be maintained by the Bank. Separate KYC would not be required for customers who are issued such instruments against debit to their bank accounts in India.
- Bank shall adopt a risk based approach, duly approved by the Board, in deciding the number of such instruments which can be issued to a customer, transaction limits, etc.
- The gift instruments may be revalidated after date of expiry through issuance of new Prepaid Card instrument.
- The provisions of paragraph 11 on validity and redemption, as applicable, shall be adhered to.
- The features of such PPIs shall be clearly communicated to the PPI holder by SMS / e-mail / post or by any other means at the time of issuance of the PPI / before the first loading of funds
- PPIs for Mass Transit Systems (PPI-MTS)

- These semi-closed PPIs shall be issued by mass transit system operators after authorization to issue and operate such PPIs under the PSS Act.
- The PPI-MTS shall necessarily contain the Automated Fare Collection application related to the transit service to qualify as PPI-MTS.
- Apart from the mass transit system, such PPI-MTS shall be used only at other merchants whose activities are allied / related to or are carried on within the premises of the transit system.
- Bank may decide about the customer details, if any, required to be obtained for issuance of such PPIs.
- The PPI-MTS issued shall be reloadable in nature and the maximum value outstanding in PPI cannot exceed the limit of Rs. 3,000/- at any point of time.
- Cash-out or refund or funds transfer shall not be permitted from these PPIs.
- Other requirements such as escrow arrangement, customer grievance redressal mechanism, agent due diligence, reporting and MIS requirements, etc. applicable to issuance of PPIs (as indicated under various paragraphs of this Policy and Master Directions of RBI) shall also be applicable in respect of PPI-MTS.
- These PPIs may be revalidated (including through issuance of new instrument) as per the Board approved policy of the Bank.
- The provisions of paragraph 10 on validity and redemption, as applicable, shall be adhered to.
- The features of such PPIs shall be clearly communicated to the PPI holder by SMS / e-mail / post or by any other means at the time of issuance of the PPI / before the first loading of funds.

Deployment of Money Collected

- The outstanding balance shall be part of the 'net demand and time liabilities' for the purpose of maintenance of reserve requirements. This position will be computed on the basis of the balances appearing in the books of the bank as on the date of reporting.

4.5.5. Security and Risk Mitigation

Security, Fraud prevention and Risk Management Framework

- A strong risk management system is necessary to meet the challenges of fraud and ensure customer protection. Adequate information and data security infrastructure and systems for prevention and detection of frauds shall be put in place.
- Existing Board approved Information Security policy of the Bank should be strictly adhered to for the safety and security of the payment systems operated the Bank, and security measures should be implemented in accordance with this policy to mitigate identified risks. The security measures shall be reviewed (a) on on-going basis but at least once a year, (b) after any security incident or breach, and (c) before / after a major change to their infrastructure or procedures.
- The transactions performed using PPIs issued as cards are passed through the existing Fraud Risk Management framework of the Bank.
- The facilities implemented in DCMS for enabling/ disabling transaction features and changing the daily usage limits as per RBI guidelines are available for IB cash cards also.
- Wallets are not currently being issued by our Bank. The following framework shall be put in place to address the safety and security

concerns, and for risk mitigation and fraud prevention, in case of wallets / Cards, as and when applicable:

- In case of wallets, if same login is provided for the PPI and other services offered by the Bank, then the same shall be clearly informed to the customer by SMS or email or post or by any other means. The option to logout from the website / mobile account shall be provided prominently.
- Appropriate mechanisms shall be put in place to restrict multiple invalid attempts to login / access to the PPI, inactivity, timeout features, etc.
- Every successive payment transaction in wallet should be authenticated by explicit customer consent.
- PPIs issued in the form of Cards (IB Cash Card) support OTP based additional factor of authentication (AFA) as required for debit cards.
- Customer induced options shall be provided for fixing a cap on number of transactions and transaction value for different types of transactions/ beneficiaries. Customers shall be allowed to change the caps, with additional authentication and validation.
- A limit on the number of beneficiaries that may be added in a day per PPI shall be put in place.
- A system of alert when a beneficiary is added should be introduced when wallet based PPIs are introduced by the Bank.
- Suitable cooling period shall be put in place for funds transfer upon opening the PPI or loading / reloading of funds into the PPI or after adding a beneficiary so as to mitigate the fraudulent use of PPIs.

- A mechanism to send alerts when transactions are done using the PPIs is put in place. In addition to the debit or credit amount intimation, the alert also indicates the balance available in the PPI after completion of the said transaction.
- A mechanism is put in place for velocity check on the number of transactions effected in a PPI per day.
- Escalation mechanisms have been put in place in our Centralized Call Centre for alerting the customer in case of suspicious transactions.

- A mechanism for monitoring, handling and follow-up of cyber security incidents and cyber security breaches has been established. Incidents will be reported immediately to DPSS, RBI, Central Office, Mumbai and CERT-IN.

Safeguards against Money Laundering (KYC / AML / CFT) Provisions

- The Know Your Customer (KYC) / Anti-Money Laundering (AML) / Combating Financing of Terrorism (CFT) guidelines issued by RBI and the Bank, as updated from time to time, should be scrupulously followed for each PPI holder.
- Provisions of Prevention of Money Laundering Act, 2002 and Rules framed there under, as amended from time to time shall be applicable. Necessary systems shall be put in place to ensure compliance with these guidelines.
- Log of all the transactions undertaken using the PPIs shall be maintained for at least ten years. This data shall be made available for scrutiny to RBI or any other agency / agencies as may be advised by RBI.
- Suspicious Transaction Reports (STRs) shall be filed to Financial Intelligence Unit-India (FIU-IND) as being done for other transactions.

4.5.6. Compliance to RBI Guidelines and Other Standards

RBI Guidelines applicable for different types of PPIs:

1. Semi-closed PPIs up to Rs.10,000/- by accepting minimum details of the PPI holder.

- These PPIs shall be issued only after obtaining minimum details of the PPI holder. The minimum details shall include mobile number verified with One Time Pin (OTP) and self-declaration of name and unique identification number of any of the 'officially valid document' defined under Rule 2(d) of the PML Rules 2005, as amended from time to time
- These PPIs shall be reloadable in nature and issued only in electronic form, including cards.
- The amount loaded in such PPIs during any month shall not exceed Rs.10,000/- and the total amount loaded during the financial year shall not exceed Rs.1,00,000/.
- The amount outstanding at any point of time in such PPIs shall not exceed Rs.10,000/-.
- The total amount debited from such PPIs during any given month shall not exceed Rs.10,000/-
- These PPIs shall be used only for purchase of goods and services. Funds transfer from such PPIs to bank accounts and also to PPIs of same / other issuers shall not be permitted. These limits will be decided as and when the Bank introduces Semi-closed PPIs.
- There is no separate limit on purchase of goods and services using PPIs and Bank may decide limit for these purposes within the overall PPI limit, when semi-closed PPIs are introduced by the Bank.
- These PPIs shall be converted into KYC compliant semi-closed PPIs (as defined in paragraph 7.2) within a period of 12 months from the date of

issue of PPI, failing which no further credit shall be allowed in such PPIs. However, the PPI holder shall be allowed to use the balance available in the PPI.

- This category of PPI shall not be issued to the same user in future using the same mobile number and same minimum details.
- The PPIs can be closed at any time by the PPI holder and outstanding balance, at the time of closure, shall be transferred at the request of the holder to the 'own bank account of the PPI holder' (duly verified by the Bank), after complying with KYC requirements of the PPI holder. The funds shall be transferred 'back to source' (payment source from where the PPI was loaded) at the time of closure.
- The features of such PPIs shall be clearly communicated to the PPI holder by SMS / e-mail / post or by any other means at the time of issuance of the PPI / before the first loading of funds.

2. Semi-closed PPIs up to Rs.1,00,000/- after completing KYC of the PPI holder

- These PPIs shall be issued after completing KYC of the PPI holder.
- These PPIs shall be reloadable in nature and issued only in electronic form, including cards.
- The amount outstanding shall not exceed Rs.1,00,000/- at any point of time.
- The funds can be transferred 'back to source' (payment source from where the PPI was loaded) or 'own bank account of the PPI holder' (duly verified by the Bank). However, Bank shall set limits taking into account the risk profile of the PPI holders, other operational risks, etc.

- Facility of 'pre-registered beneficiaries' shall be provided whereby the PPI holder can register the beneficiaries by providing their bank account details, details of PPIs issued by our Bank / other Bank etc as permitted by RBI. In case of such pre-registered beneficiaries, the funds transfer limit shall not exceed Rs.1,00,000/- per month per beneficiary. The limits shall be set by the Bank within this ceiling taking into account the risk profile of the PPI holders, other operational risks, etc.
- The fund transfer limits for all other cases shall be restricted to Rs.10,000/- per month.
- There is no separate limit on purchase of goods and services using PPIs and Bank may decide limit for these purposes within the overall PPI limit, from time to time. These limits shall be clearly indicated to the PPI holders and necessary options may be provided to PPI holders to set their own fund transfer limits. Such option is provided in our Bank's IB smart remote mobile application.
- Option shall be provided to close the PPI and transfer the balance as per the applicable limits of this type of PPI. For this purpose, an option shall be provided to the PPI holder at the time of issuing the PPI to provide details of pre-designated bank account or other PPIs of same issuer (or other issuers as and when permitted by RBI) to which the balance amount available in the PPI shall be transferred in the event of (a) closure of PPI (b) expiry of validity period of such PPIs, etc.
- The features of such PPIs shall be clearly communicated to the PPI holder by SMS / e-mail / post or by any other means at the time of issuance of the PPI / before the first loading of funds.

3. New type of semi-closed Prepaid Payment Instrument (PPI) – PPIs upto ₹10,000/- with loading only from bank account

- Such PPIs can be issued by the bank after obtaining minimum details of the PPI holder.
- The minimum details shall necessarily include a mobile number verified with One Time Pin (OTP) and a self-declaration of name and unique identity / identification number of any 'mandatory document' or 'officially valid document' (OVD) listed in the 'Master Direction - Know Your Customer (KYC) Direction, 2016' issued by Department of Regulation, Reserve Bank of India, as amended from time to time.
- These PPIs shall be reloadable in nature and issued in card or electronic form. Loading/ Reloading shall be only from a bank account.
- The amount loaded in such PPIs during any month shall not exceed Rs.10,000 and the total amount loaded during the financial year shall not exceed Rs.1,20,000.
- The amount outstanding at any point of time in such PPIs shall not exceed Rs.10,000.
- These PPIs shall be used only for purchase of goods and services and not for funds transfer.
- Bank shall provide an option to close the PPI at any time and also allow to transfer the funds 'back to source' (payment source from where the PPI was loaded) at the time of closure.
- The features of such PPIs shall be clearly communicated to the PPI holder by SMS / e-mail / post or by any other means at the time of issuance of the PPI / before the first loading of funds.

4. Open system PPIs after completing KYC of the PPI holder

- These PPIs shall be issued after completing KYC of the PPI holder (as indicated in paragraph 4).
- These PPIs shall be reloadable in nature and issued only in electronic form, including cards.
- The amount outstanding shall not exceed Rs.1,00,000/- at any point of time.
- The funds can be transferred 'back to source' (payment source from where the PPI was loaded) or 'own bank account of the PPI holder' (duly verified by the Bank). However, Bank shall set limits taking into account the risk profile of the PPI holders, other operational risks, etc. This can be done if the initial loading at the branch was done by debiting an individual's account with our Bank. Closure of card is permitted in any Branch of our Bank by transferring the balance amount to another full KYC account with our Bank of the same card holder.
- Facility of 'pre-registered beneficiaries' shall be provided whereby the PPI holder can register the beneficiaries by providing their bank account details, details of PPIs issued by our Bank / other Bank etc as permitted by RBI. In case of such pre-registered beneficiaries, the funds transfer limit shall not exceed Rs.1,00,000/- per month per beneficiary. The limits shall be set by the Bank within this ceiling taking into account the risk profile of the PPI holders, other operational risks, etc. Currently this facility is not being provided by our Bank.
- The fund transfer limits for all other cases shall be restricted to Rs.10,000/- per month.

- Funds transfer from such PPIs to other open system PPIs, debit cards and credit cards is permitted as per the limits given above.
- There is no separate limit on purchase of goods and services using PPIs and Bank may decide limit for these purposes within the overall PPI limit, from time to time. These limits shall be clearly indicated to the PPI holders and necessary options may be provided to PPI holders to set their own fund transfer limits. Currently the limit set for purchase of Goods & Services using RuPay Open System Prepaid Cards (IB Cash Card) is Rs.50,000/-. In addition to this, customers can set their own limits using Bank's mobile application IB Smart Remote.
- Option shall be provided to close the PPI and transfer the balance as per the applicable limits of this type of PPI. For this purpose, an option shall be provided to the PPI holder at the time of issuing the PPI to provide details of pre-designated bank account or other PPIs of same issuer (or other issuers as and when permitted by RBI) to which the balance amount available in the PPI shall be transferred in the event of (a) closure of PPI (b) expiry of validity period of such PPIs, etc.
- The features of such PPIs shall be clearly communicated to the PPI holder by SMS / e-mail / post or by any other means at the time of issuance of the PPI / before the first loading of funds. Our Bank is providing a Write-up about the Product features while issuing RuPay Open System Prepaid cards to customers.
- Cash withdrawal at Point of Sale (POS) terminals is permitted up to a limit of Rs.2000/- per day in rural areas and Rs.1000/- per day in other areas, subject to the same conditions as applicable hitherto to debit cards (for cash withdrawal at POS).

4.5.7. Customer Service

Customer Protection and Grievance Redressal Framework

- All important terms and conditions are disclosed in clear and simple language to the holders while issuing the instruments. These disclosures include:
    - All charges and fees associated with the use of the instrument.
    - The expiry period and the terms and conditions pertaining to expiration of the instrument.
- The existing formal, publicly disclosed customer grievance redressal framework, including designating a nodal officer will handle the customer complaints / grievances, the escalation matrix and turn-around-times for complaint resolution.
- Complaint facility is made available in Bank's website. The framework includes the following:
    - The information of the Bank's customer protection and grievance redressal policy.
    - Customer care contact details, including details of nodal officials for grievance redressal (telephone numbers, email address, postal address, etc.) on website, and cards.
    - Specific complaint numbers are provided for the complaints lodged along with the facility to track the status of the complaint by the customer.
    - Action will be initiated to resolve any customer complaint / grievance expeditiously, normally within 48 hours and the same

will be resolved not later than 30 days from the date of receipt of such complaint / grievance.

- Sufficient awareness shall be created and customers shall be educated in the secure use of the PPIs, including the need for keeping passwords confidential, procedure to be followed in case of loss or theft of card or authentication data or if any fraud / abuse is detected, etc.
- The amount and process of determining customer liability in case of unauthorized / fraudulent transactions involving PPIs shall be clearly outlined. RBI's circular DBR.No.Leg.BC.78/09.07.005/2017-18 dated July 6, 2017 on Customer Protection – Limiting Liability of Customers in Unauthorized Electronic Banking Transactions shall be followed in this regard.
- PPI holders are provided an option to generate mini statements through ATMs. Additionally, account statement for at least past 6 months and transaction history for at least 10 transactions shall be provided at the branches, if required by the PPI holder, after verifying the identity for KYC compliance.
- Customers will have recourse to the Banking Ombudsman Scheme for grievance redressal.
- PPI issuers shall ensure transparency in pricing and the charge structure by disclosing the charges for various types of transactions on its website, mobile app, agent locations, etc. If card is lost, based on request from the card holder, duplicate card can be issued. The charges for issuance of duplicate card is Rs.50/- (plus appl. Taxes) and duplicate PIN mailer is Rs.25/- (plus appl. Taxes)

- The amount collected from the customer shall be acknowledged by issuing a receipt (printed or electronic).
- Bank shall be responsible for addressing all customer service aspects related to all PPIs (including co-branded PPIs) issued by the Bank.
- Frequently Asked Questions (FAQs) related to the PPIs is displayed on the Bank's website.

4.5.8. Co-branded PPI Cards

- Co-branded prepaid cards can be issued to corporate entities who wish to issue prepaid cards to their employees with their corporate logo embedded on the card.
- Such instruments may be co-branded with the name / logo of the company for whose customers / beneficiaries such co-branded instruments are to be issued. The name of the Bank will be prominently visible on the payment instrument.
- The co-branding partner shall be a company incorporated in India and registered under the Companies Act 1956 / Companies Act 2013. In case the co-branding partner is a bank, then the same shall be a bank licensed by RBI.
- Due diligence in respect of the co-branding partner shall be carried out to protect the interests of the Bank against the reputation risk exposed to in such an arrangement. In case of proposed tie up with a financial entity, whether the entity has the approval of its regulator for entering into such arrangement shall be ensured.
- Since Bank is answerable to RBI for all acts of the co-branding partner and for all customer-related aspects of the PPIs, the risk associated with such an arrangement including reputation risk shall be assessed for each

corporate identified and risk clearance shall be obtained for any such co-branding arrangement as per RBI guidelines.

- In case of co-branding arrangements between the bank and a non-bank entity, the role of the non-bank entity shall be limited to marketing / distribution of the PPIs or providing access to the PPI holder to the services that are offered.
- In case of co-branding arrangement between two banks, the PPI issuing bank shall ensure compliance to above instructions.
- The instructions / guidelines on KYC / AML / CFT (as indicated in paragraph 4) shall be adhered to, in respect of all PPIs issued under the co-branding arrangement as well.
- Any new arrangement will be reported by CO: Digital Banking Division to RBI within seven days of finalization of arrangement.
- Bank should not reveal any information related to customers obtained at the time of issuance of the co-branded PPI and the co-branding non-banking entity should not be permitted to access any details of customers' accounts that may violate Bank's secrecy obligations.
- In case of outsourcing the activity, it shall be strictly guided by the Outsourcing policy of the Bank.

4.5.9. Information System Audit and Interoperability

Scope of the Audit conducted on PPI system included the following as per RBI guidelines:

- Security controls were tested both for effectiveness of control design (Test of Design – ToD) and control operating effectiveness (Test of Operating Effectiveness – ToE).

- Technology deployed so as to ensure that the authorised payment system was being operated in a safe, secure, sound and efficient manner.
- Evaluation of the hardware structure, operating systems and critical applications, security and controls in place, including access controls on key applications, disaster recovery plans, training of personnel managing systems and applications, documentation, etc.
- Evaluating adequacy of Information Security Governance and processes of those which support payment systems.
- Compliance as per security best practices, specifically the application security lifecycle and patch / vulnerability and change management aspects for the authorised system and adherence to the process flow approved by RBI.

The following framework is put in place:

- *Application Life Cycle Security:* The source code audits will be conducted by professionally competent personnel / service providers or have assurance from application providers / OEMs that the application is free from embedded malicious / fraudulent code.
- *Security Operations Centre (SOC):* Integration of system level (server), application level logs of mobile applications (PPIs) with SOC for centralised and co-ordinated monitoring and management of security related incidents.
- *Anti-Phishing*: Subscribing to anti-phishing / anti-rouge app services from external service providers for identifying and taking down phishing websites / rouge applications in the wake of increase of rogue mobile apps / phishing attacks.

- *Risk-based Transaction Monitoring:* Risk-based transaction monitoring or surveillance process is implemented as part of fraud risk management system for debit cards.

Vendor Risk Management

- Bank has an agreement with the service provider that amongst others provides for right of audit / inspection by the regulators of the country.
- RBI shall have access to all information resources (online / in person) that are consumed by the Bank, to be made accessible to RBI officials when sought, though the infrastructure / enabling resources may not physically be located in the Bank's premises.
- Relevant legal and regulatory requirements relating to geographical location of infrastructure and movement of data out of borders shall be adhered to.
- Security processes and controls being followed by service providers shall be reviewed regularly.
- Service agreements of the Bank with provider shall include a security clause on disclosing the security breaches if any happening specific to the Bank's ICT infrastructure or process including but not limited to software, application and data as part of Security incident Management standards, etc. The same will be incorporated in the agreement with service providers.
- *Disaster Recovery:* DR facility to achieve the Recovery Time Objective (RTO) / Recovery Point Objective (RPO) for the PPI system to recover rapidly from cyber-attacks / other incidents and safely resume critical operations aligned with RTO while ensuring security of processes and data is protected may be considered.

Interoperability

Interoperability is defined as the ability of customers to use a set of payment instruments seamlessly with other users within the segment. To ensure interoperability of PPIs, it has been decided by RBI vide Circular Ref: DPSS.CO.PD.No.808/02.14.006/2018-19 dated 16.10.2018 as under:

- Interoperability shall be enabled in phases for the PPIs.
- In the first phase, Bank shall make all KYC-compliant PPIs issued in the form of wallets interoperable through Unified Payments Interface (UPI).
- In subsequent phases, interoperability shall be enabled between wallets and bank accounts through UPI.
- Similarly, interoperability for PPIs issued in the form of cards shall also be enabled in due course. However, PPIs may be issued in association with authorized card networks, as hitherto.
- Technical and operational requirements for such interoperability, including those relating to safety and security, risk mitigation, etc. shall be adhered to.

Currently our Bank is issuing all PPIs as RuPay Prepaid Cards (IB Cash Card) which is interoperable across the terminals connected through RuPay network.

4.6 Daily Limits for Debit Card Transactions

With the increase in number of debit card holders and transaction channels, there is also an increase in the number of frauds and unauthorized usage of debit cards. Various types of frauds are being reported in the industry, with the Modus Operandi ranging from customer- targeted activities such as card skimming and vishing, to large scale attacks targeting the Banks such as ATM Cash Out attacks & Man in the middle attacks.

With new security threats emerging regularly, Banks are also making all efforts to secure the payment systems and customer data from attacks and to prevent cyber-attacks on the payment eco system and to avoid financial and reputational risks to the Bank. Reserve Bank of India is issuing various guidelines for strengthening the Information System Security procedures of the Banks.

4.6.1. Debit Card Products and Defined Limits

Globally, debit cards are issued with a daily withdrawal limit defined either at the card level or at the BIN level. BIN (Bank Identification Number) represents the first 6 digits of the card number and usually denotes a particular card variant / product issued by the card issuing bank. Our Bank is issuing debit cards by defining the daily withdrawal / usage limit at the BIN level. Below is the daily usage limits defined at the ATM EFT switch for various card products:

S. No	Card Product	ATM Cash Limit (Rs.)	POS / E-Com Purchase Limit (Rs.)	Aggregate Limit (Rs.)
1	Domestic RuPay Classic Card	50,000	50,000	1,00,000

S. No	Card Product	ATM Cash Limit (Rs.)	POS / E-Com Purchase Limit (Rs.)	Aggregate Limit (Rs.)
2	Rupay Platinum Card	50,000	1,00,000	1,50,000
3	RuPay PMJDY Card	50,000	50,000	1,00,000
4	MasterCard World Card	50,000	1,00,000	1,50,000
5	MasterCard E-purse Card	50,000	50,000	1,00,000
6	RuPay Senior Citizen Card	25,000	50,000	75,000
7	RuPay Mudra Cards	10,000	10,000	20,000
8	RuPay KCC	50,000	50,000	1,00,000
11	MasterCard IB Surabhi cards	50,000	1,00,000	1,50,000
12	RuPay IB Digi cards	10,000	10,000	20,000
13	RUPAY Pungrain card (Arthia)	50,000	1,00,000	1,50,000
14	RUPAY Kishore Domestic NCMC Card	2,500	2,500	5,000
15	RUPAY Platinum International Debit Card (eALB)	1,00,000	2,00,000	2,00,000
16	VISA EMV International Debit Card	25,000	25,000	50,000
17	VISA Gold Debit Card	50,000	1,00,000	1,50,000

S. No	Card Product	ATM Cash Limit (Rs.)	POS / E-Com Purchase Limit (Rs.)	Aggregate Limit (Rs.)
18	VISA Platinum Debit Card	1,00,000	2,00,000	3,00,000
19	RuPay Debit Select Card	50,000 with an option to increase up to Rs.1,00,000 based on customer request and ZM recommendation.	1,00,000 with an option to increase up to Rs.4,00,000 based on customer request and ZM recommendation	1,50,000 with an option to increase up to Rs.4,50,000 based on customer request and ZM recommendation

For the following transactions, uniform limit will apply for all the card products:

Sl No.	Transaction Type	Daily Limit (Rs.)
1	Cash Withdrawal at POS	Rs.2,000/-
2	Offline Contactless Transaction (Tap & Go – Debit to Wallet Account)	Rs.2,000/-
3	Online Contactless Transaction (Debit to Main Account)	Rs.5,000/-

4.6.2. Applicability of Limits

During the recent years, a couple of security attacks on the Bank's payment network were reported in India, wherein the attacker could manage to get

unauthorized access to the Bank's network and make changes in the system to authorize fake transactions purported to be originated from a card issued by the Bank. As a result, multiple ATMs (both domestic and international) had dispensed cash based on the authorization received from the ATM EFT Switch leading to loss amounting to Crores of Rupees to the affected Bank.

In one of the incidents, a malware was installed in the ATM EFT switch to remove the transaction authorization rules such as PIN validation, Account balance check, Daily usage limit etc. In the other incident, a proxy ATM EFT switch was suspected to be injected for authorizing fake transactions and for dispensing cash from multiple ATMs across the globe.

In the wake of the above incidents of potential compromise of ATM switch/ ecosystem, Cyber Security & IT Examination Cell of Reserve Bank of India has issued an Advisory No.6/2018 dated 13.06.2018 which outlines the control measures to be implemented by the Banks urgently to strengthen the surveillance / monitoring of card transactions, especially overseas cash withdrawals.

As per the above advisory, Banks shall put in place transaction limits at Card, BIN as well as at bank level. Such limits shall be mandatorily set at the switch of the Card network itself. Banks shall put in place transaction control mechanism that has necessary Cap (restrictions on transactions), alerts, if any of the limits set as per the above requirement is breached. Such limits shall be set in terms of volume, value, velocity, geographic location of origination of transaction, etc. Transaction pattern in the past, customer profile, bank's size, etc., are some of the parameters that could be considered to arrive at the risk appetite for setting the limits.

Card Level Limits

Limit on transaction value

- While issuing new cards and replacement cards, daily limit for E-Com transactions, contactless transactions and Cash at POS transactions will be set to zero by default.
- Customers will be able to set separate daily transaction limits for ATM, POS, E-Commerce, Contactless and Cash at POS transactions within the maximum daily limit permitted by the Bank. This facility will be available for all existing and new cards in internet banking, mobile banking and at branches (through debit card management system).
- Also, all new debit cards will be enabled for use only at ATMs and Point of Sale (PoS) devices within India.
- Customers will be permitted to enable E-Com transactions, contactless transactions, Cash at POS transactions and international transactions (only on international debit cards) through internet Banking, mobile banking and also through branches.

Limit on transaction volume

- Transactions on all new and existing debit cards will be restricted to 5 transactions in ATMs and 10 transactions in POS (Including E-com and cash @ POS transactions) per day.
- The above limits will be set in the Fraud Risk Management (FRM) Software of ATM EFT Switch.
- Existing International Debit Cards which have been never used for international transactions will be disabled for international transactions with effect from 16.03.2020.

- Existing debit cards which have never been used for online (E-Com / Auto-debit transactions) transactions will be disabled for online transactions with effect from 16.03.2020.

Limit on transaction velocity

Below limits are set in the FRM Software of ATM EFT Switch for generating alerts based on the transaction velocity. Below are the rules configured based on transaction velocity:

Transaction Type	**Transaction Time**	**Transaction count**	**Transaction value**	**Action**
Domestic E-Com transaction	Within 10 minutes	> 3 transactions	-	Decline the transaction
International E-Com transaction	Within 24 Hrs	> 3 transactions	-	Decline
International POS purchase	Within 24 Hrs	> 3 transactions	-	Decline
Cash @ POS transaction	Within 24 Hrs	> 3 transactions	-	Decline
High Risk Merchants	-	All transactions	-	Decline
ATM transactions	between 23:00 Hrs & 00: 00 Hrs	All transactions	> Rs.25,000	Generate alert in FRM *
Card to Account fund transfer	Between 00:00 Hrs and 06: 00 Hrs and between	All transactions	> Rs.50,000	Generate alert in FRM

Transaction Type	Transaction Time	Transaction count	Transaction value	Action
	22:00 Hrs to 00: 00 Hrs			
All types of transactions	between 00:00 Hrs & 06: 00 Hrs	> 2 transactions	> Rs.20,000	Generate alert in FRM

* Based on the alert generated by FRM, our call centre agent will try to contact the customer to confirm the genuineness of the transaction. If the customer is not reachable or if the customer confirms that the transaction is unauthorized, call centre agent will change the card status to "RESRICTED" to prevent further debits in the customer's account.

Limit on geographic location of origination of transaction

- Transactions can be restricted in specific geographical locations (countries & cities) by setting the rules in the (FRM) Software of ATM EFT Switch. Below are some of the restrictions set based on the geographic locations of origination of transaction:
- Transactions are not permitted from different countries within 1 hour.
- By default, transactions are not permitted in high risk countries such as China, Cambodia, Thailand, Panama, Indonesia, Hungary and Kenya. Branches can submit online request through ATM website for enabling transactions in these countries based on specific request received from the card holder
- Card Not Present (e-com) transactions are not permitted if originated from Brazil.
- Only 3 transactions will be permitted in a day if the card is used abroad.

- Cards cannot be used for more than 5 transactions within 72 hours in LWE (Left-Wing Extremism) districts.

- POS transactions originated within India, but without PIN, are not permitted.

The restrictions in usage of high risk countries are informed to customers when they request for enabling / issuing cards for international usage. The cards are white-listed for use in these high risk countries on specific request received from the customers.

BIN Level Limits

Only the transaction value and transaction volume will be limited at BIN level:

- Transaction value will be limited to 150% of the maximum of total value used by the cards under the BIN in a day during last 6 months.

- Transaction volume will be limited to 150% of the maximum of total transactions done using the cards under the BIN in a day during last 6 months.

- Both the above limits will be set in the FRM software of ATM EFT switch separately for ATM channel and POS channel (including e-com). These limits will also be shared with the card networks (NPCI, MasterCard & Visa) for configuring the limits at their end.

- The above limits will be used only for generating alerts and no transaction will be declined if the above limits are breached.

- The limits will be renewed every six months for upward or downward revision as per clause (6) of this policy.

Bank wise limits

Similar to BIN wise limits, Bank wise limits will also be set only for the transaction value and transaction volume:

- Bank wise transaction value will be limited to the sum of transaction amount limit set for all the BINs combined.
- Similarly, Bank wise transaction volume will be limited to the sum of transaction volume limit set for all the BINs combined.
- Both the above limits will be set in the FRM software of ATM EFT switch separately for ATM channel and POS channel (including e-com). These limits will also be shared with the card networks (NPCI, MasterCard & Visa) for configuring the limits at their end.
- The transactions may be declined if Bank wise limit exceeds 150% for any particular day.
- The limits will be renewed every six months for upward or downward revision as per clause (6) of this policy.

4.6.3. Review of Limits

As the card base and transactions grow and new avenues are opened for usage of cards, the limits set on the transaction amount, transaction volume and other limits need to be reviewed periodically for upward or downward revisions as deemed fit.

Limits set at the BIN level and Bank level will be reviewed on a half-yearly basis by the Executive Director / IT Steering Committee by taking into consideration the actual utilization of transaction value and transaction amount as a percentage of the maximum limit set for BIN wise and Bank wise limits on transaction value and transaction amount.

Based on the review of the above data placed to the reviewing authority, the reviewing authority will decide / approve the changes to be made in the limits, if any.

5. Role of Internal Auditor

The functions and processes enumerated in this policy will be reviewed by the internal auditor as and when required by the bank.

6. Review of the Policy

Interpretation and amendments to the Policy

The MD & CEO / Executive Director is the authority for interpretation on any of the terms given in this Policy and also to amend the policy for business requirements during 2021-22 and seek ratification from the Board. Bank would also implement any statutory guidelines received afresh and incorporate the amendments made in the policy due to statutory guidelines at the time of annual review.

Digital Banking Division (DBD) will be the owner of the policy. The existing policy shall be reviewed by IT Strategy Committee / Audit Committee of the Board, before approval by Board of Directors. The policy will be reviewed once in a year or as and when changes are being introduced. MD & CEO / Executive Director is authorized for making any business model change as deemed necessary during the course of this policy till next revision.

All applicable RBI/ BCSBI/ Government guidelines issued from time to time will become part of this policy.

Apart from this regular review, under the following circumstances the policy will be reviewed:

1. On change of major technology

2. After completion of Audit- to discuss the audit findings and the impact on Policy
3. Before rolling out of major functionality-To discuss the impact on policy
4. Any regulatory change
5. Any other development which has a perceived impact on policy.

7. Annexures

7.1 Approval for PPI issuance by Bank (PPI issuance by Indian Bank)

- Permission to introduce Prepaid Gift Card and Prepaid Travel Card was accorded by the Board during the meeting held on 24.01.2011.
- Our Bank has been granted permission by RBI to issue General Purpose and Gift Prepaid cards vide Ref: DPSS.CO.AD/1629/02.144/2011-12 dated 05.03.2012.
- Banks have been granted general permission to issue rupee denominated co-branded prepaid instruments subject to the terms and conditions mentioned in the RBI Circular Ref: DBOD.No.FSD.BC. 67/24.01.019/2012-13 dated 12.12.2012.
- Permission has been granted by Board vide its meeting held on 21.09.2017 for issuance of co-branded prepaid cards to corporate entities who wish to issue prepaid cards to their employees / customers with their corporate logo embedded on the card. Executive Director has been authorised by the Board to approve such co-branding arrangements.

7.2 Reconciliation of Digital Transactions

There should be an approved reconciliation procedure for transaction reconciliation originated from all digital channels / alternate delivery channels.

The system of reconciliation to be framed in co-ordination with O&M Department and the same shall be put in place for any new digital product launched by the Bank on approval from competent authority.

Minimum three way reconciliation system to be put in place for all digital products including ATM transactions. For ATM transactions carried out in our ATMs, four way reconciliation to be followed using recon files from Source System, CBS, Interchange Settlement files & Electronic Journal (EJ) files.

Reconciliation to be carried out as per the Turnaround Time (TAT) prescribed for various digital products and the proactive refunds to be made to improve customer satisfaction.

Reconciliation process to be periodically reviewed to identify the gaps in the systems, process, procedures and initiate corrective measures to avoid fraudulent / suspected transactions.

7.3 Ombudsman Scheme for Digital Transactions, 2019

Reserve Bank of India has introduced the Ombudsman Scheme for Digital Transactions to facilitate the satisfaction or settlement of complaints regarding digital transactions undertaken by customers of System Participants. System Participant means any person other than a bank participating in a payment system as defined under Section 2 of the Payment and Settlement Systems Act, 2007. System participants do not include a System Provider, who operates an authorised payment system (e.g. NPCI, MasterCard & Visa).

The Scheme has come into force from January 31, 2019.

The Ombudsman for Digital Transactions shall receive and consider complaints relating to deficiency in services on the grounds mentioned below irrespective of the pecuniary value:

Grounds of Complaint

1. **Prepaid Payment Instruments: Non-adherence to the instructions of Reserve Bank by System Participants about Prepaid Payment Instruments on any of the following:**

   a) Failure in crediting merchant's account within reasonable time;
   b) Failure to load funds within reasonable time in wallets / cards;
   c) Unauthorized electronic fund transfer;
   d) Non-Transfer / Refusal to transfer/ failure to transfer within reasonable time, the balance in the Prepaid Payment Instruments to the holder's 'own' bank account or back to source at the time of closure, expiry of validity period etc., of the Prepaid Payment Instrument;
   e) Failure to refund within reasonable time / refusal to refund in case of unsuccessful / returned/ rejected / cancelled / transactions;
   f) Non-credit / delay in crediting the account of the Prepaid Payment Instrument holder as per the terms and conditions of the promotion offer(s) from time to time, if any;
   g) Non-adherence to any other instruction of the Reserve Bank on Prepaid Payment Instruments

2. **Mobile / Electronic Fund Transfers: Non-adherence to the instructions of the Reserve Bank on Mobile / Electronic fund transfers by System Participants on any of the following:**

   a) Failure to effect online payment / fund transfer within reasonable time;

b) Unauthorized electronic fund transfer;

c) Failure to act upon stop-payment instructions within the time frame and under the circumstances notified to the customers within prescribed timeline;

d) Failure to reverse the amount debited from customer account in cases of failed payment transactions within prescribed timeline;

e) Non-adherence to any other instruction of the Reserve Bank on Mobile / Electronic fund transfers

3. Non-adherence to instructions of Reserve Bank / respective System Provider to System Participants, on payment transactions through Unified Payments Interface (UPI) / Bharat Bill Payment System (BBPS) / Bharat QR Code / UPI QR Code on the following grounds:

a) Failure in crediting funds to the beneficiaries" account;

b) Failure to return within reasonable time the payment to the originating member in case of failure to credit the funds to the beneficiary's account;

c) Failure to / delay in refund of money back to account in case of transaction failure or declined transactions (i.e. failed transactions);

d) Non-adherence to any other instruction of the Reserve Bank on payment transactions / through Unified Payments Interface (UPI) / Bharat Bill Payment System (BBPS)/ Bharat QR Code / UPI QR Code.

e) Non-reversal / failure to reverse within reasonable time, funds wrongly transferred to the beneficiary account due to lapse at the end of System Participant.

f) Any other matter relating to the violation of the directives including on fees / charges, if any, issued by the Reserve Bank in relation to digital transactions. The System Participant covered under the Scheme shall

display clearly in their branches/websites, the fees/charges to be levied for various digital transactions.

Disposal of the complaints:

The Ombudsman, to the satisfaction of the parties involved, dispose of the complaint through:

- Settlement by agreement between parties; OR
- Conciliation and mediation between parties; OR
- Passing an Award as per the provisions of the Scheme.

Additional details on the Ombudsman Scheme for Digital Transactions, 2019 are available in RBI notification Ref. CEPD. PRS. No. 3370/13.01.010/2018-19 dated 31.01.2019.

7.4 RBI Circular on Card Tokenization

The Reserve Bank has issued guidelines on tokenization for debit / credit / prepaid card transactions as an endeavor to enhance the safety and security of the payment systems in the country. Tokenization involves a process in which a unique token masks sensitive card details. Thereafter, in lieu of actual card details, this token is used to perform card transactions in contactless mode at Point Of Sale (POS) terminals, Quick Response (QR) code payments, etc.

These guidelines permit authorised card payment networks to offer card tokenisation services to any token requestor (third party app provider), subject to conditions enumerated in these guidelines. A card holder may avail of these services by registering the card on the token requestor's app after giving explicit consent. No charges shall be recovered from the customer for availing this service. All extant instructions of Reserve Bank on safety and security of card transactions, including mandate for Additional

Factor of Authentication (AFA)/ PIN entry shall be applicable for tokenised card transactions also.

Additional details on Tokenisation of card transactions are available in RBI notification Ref. RBI/2018-19/103 DPSS.CO.PD No.1463/02.143/2018-19, dated January 08, 2019.

7.5 RBI Circular on storage of all payment data in India

RBI, referring the Statement on Development and Regulatory Policies of the First Bi-monthly Monetary Policy Statement for 2018-19 dated April 5, 2018, has informed that there have been considerable growth in the payment ecosystem in the country and such systems are also highly technology dependent, which necessitate adoption of safety and security measures, which are best in class, on a continuous basis.

Hence, in order to ensure better monitoring, it is important to have unfettered supervisory access to data stored with these system providers as also with their service providers / intermediaries / third party vendors and other entities in the payment ecosystem. It has, therefore, been decided that all system providers shall ensure that the entire data relating to payment systems operated by them are stored in a system only in India. This data should include the full end-to-end transaction details / information collected / carried / processed as part of the message / payment instruction. For the foreign leg of the transaction, if any, the data can also be stored in the foreign country, if required.

The System providers shall submit the System Audit Report (SAR) on completion of the above requirement through CERT-IN empanelled auditors certifying completion of activity stated above.

Additional details on Storage of Payment System Data are available in RBI notification Ref. RBI/2017-18/153 DPSS.CO.OD No.2785/06.085/2017-2018, dated April 06, 2018.

7.6 Harmonisation of Turnaround Time (TAT) and customer compensation for failed transactions using authorised Payment Systems

Reserve Bank has put in place a framework on Turn Around Time (TAT) for resolution of customer complaints and compensation framework across all authorized payment systems.

A 'failed transaction' is a transaction which has not been fully completed due to any reason not attributable to the customer such as failure in communication links, non-availability of cash in an ATM, time-out of sessions, etc. Failed transactions shall also include the credits which could not be effected to the beneficiary account on account of lack of full information or lack of proper information and delay in initiating a reversal transaction.

Turnaround Time applicable for various types of failed transactions is as follows:

Sl. no.	Description of the incident	Framework for auto-reversal and compensation	
		Timeline for auto-reversal	Compensation payable
I	II	III	IV
1.	**Automated Teller Machines (ATMs) including Micro-ATMs**		
A	Customer's account debited but cash not dispensed.	Pro-active reversal (R) of failed transaction within a maximum of T + 5	₹ 100/- per day of delay beyond T + 5 days, to the credit of

		days.	the account holder.
2.	**Card Transaction**		
A	Card to card transfer Card account debited but the beneficiary card account not credited.	Transaction to be reversed (R) latest within T + 1 day, if credit is not effected to the beneficiary account.	₹ 100/- per day of delay beyond T + 1 day.
B	Point of Sale (PoS) (Card Present) including Cash at PoS Account debited but confirmation not received at merchant location i.e., charge-slip not generated.	Auto-reversal within T + 5 days.	₹ 100/- per day of delay beyond T + 5 days.
C	Card Not Present (CNP) (e-commerce) Account debited but confirmation not received at merchant's system.		
3.	**Immediate Payment System (IMPS)**		
A	Account debited but the beneficiary account is not credited.	If unable to credit to beneficiary account, auto reversal (R) by the Beneficiary bank latest on T + 1 day.	₹100/- per day if delay is beyond T + 1 day.
4.	**Unified Payments Interface (UPI)**		
A	Account debited but the beneficiary account is not credited (transfer of funds).	If unable to credit the beneficiary account, auto reversal (R) by the Beneficiary bank latest on T + 1 day.	₹100/- per day if delay is beyond T + 1 day.
B	Account debited but	Auto-reversal within T	₹100/- per day

	transaction confirmation not received at merchant location (payment to merchant).	+ 5 days.	if delay is beyond T + 5 days.
5.	**Aadhaar Enabled Payment System (including Aadhaar Pay)**		
A	Account debited but transaction confirmation not received at merchant location.	Acquirer to initiate "Credit Adjustment" within T + 5 days.	₹100/- per day if delay is beyond T + 5 days.
B	Account debited but beneficiary account not credited.		
6.	**Aadhaar Payment Bridge System (APBS)**		
A	Delay in crediting beneficiary's account.	Beneficiary bank to reverse the transaction within T + 1 day.	₹100/- per day if delay is beyond T + 1 day.
7.	**National Automated Clearing House (NACH)**		
A	Delay in crediting beneficiary's account or reversal of amount.	Beneficiary bank to reverse the uncredited transaction within T + 1 day.	₹100/- per day if delay is beyond T + 1 day.
B	Account debited despite revocation of debit mandate with the bank by the customer.	Customer's bank will be responsible for such debit. Resolution to be completed within T + 1 day.	
8.	**Prepaid Payment Instruments (PPIs) – Cards / Wallets**		
A	<u>Off-Us transaction</u> The transaction will ride on UPI, card network, IMPS, etc., as the case may be. The TAT and compensation rule of respective system shall apply.		
b	<u>On-Us transaction</u> Beneficiary's PPI not credited.	Reversal effected in Remitter's account within T + 1 day.	₹100/- per day if delay is beyond T + 1

	PPI debited but transaction confirmation not received at merchant location.		day.

- T is the day of transaction and refers to the calendar date.
- TAT prescribed above is the outer limit for resolution of failed transactions; and the bank will endeavour towards quicker resolution of such failed transactions.
- Wherever financial compensation is involved, the same shall be effected to the customer's account suo moto, without waiting for a complaint or claim from the customer.
- Customers, who do not get the benefit of redress of the failure as defined in the TAT, can register a complaint to the Banking Ombudsman of Reserve Bank of India.
- If the transaction is a 'credit-push' funds transfer and the beneficiary account is not credited while the debit to originator has been effected, then credit is to be effected within the prescribed time period failing which the penalty has to be paid to the beneficiary;
- If there is delay in initiation of a transaction at the originator bank's end beyond the TAT, then penalty has to be paid to the originator.
- R is the day on which the reversal is concluded and the funds are received by the issuer / originator. Reversal should be effected at the issuer / originator end on the same day when the funds are received from the beneficiary end.
- Domestic transactions i.e., those where both the originator and beneficiary are within India are covered under this framework.

7.7 RBI Master Circular on "Mobile Banking Transactions in India"

RBI Master Circular on "Mobile Banking Transactions in India" – Operative Guidelines to Banks

RBI vide notification Ref. DPSS.CO.PD.Mobile Banking. No./2/02.231/2016-17, dated July 01, 2016 (Updated on January 10, 2020) provides rules / regulations / procedures to be followed by Banks for operationalising Mobile Banking in India. With a view to simplify the procedure of registration for Mobile Banking, Reserve Bank of India has advised National Payment Corporation of India (NPCI) to develop the mobile banking registration service/option on National Financial Switch (NFS). Accordingly, all banks shall carry out necessary changes in their ATM switches to enable customer registration for mobile banking at all their ATMs.

7.8 RBI Circulars on Merchant Acquisition

I. GUIDELINES ON MDR FOR DEBIT CARD/ BHIM UPI/ AADHAR PAY TRANSACTIONS

(i) RBI circular: RBI/2016-17/59:DPSSCO.PD.No.639/02.143/2016-17 dated 01.09.2016

- MDR to be clearly unbundled for different categories of cards;
- Separate Agreements/Annexes within the same agreement for Debit , Credit and Prepaid Cards to be entered into to bring in more clarity and transparency;
- Merchants on-boarded to be educated regarding the charges associated with different categories of cards at the time of acquisition

(ii) RBI circular: RBI/2017-18/105: DPSS.CO.PD.No.1633/ 02.143/ 2017-18 dated 06.12.2017

Rationalisation of MDR for debit cards based on the following criteria:

- Categorisation of Merchants on the basis of turnover
- Adoption of differentiated MDR for QR –code based transactions
- Specifying a ceiling on the maximum permissible MDR for both 'Card Present' and 'Card not Present' transactions.

Accordingly, Maximum MDR for Debit cards transactions shall be as under:

Merchant Category	**Merchant Discount Rate (MDR) For Debit Card Transactions (as a % of transaction value)**	
	Physical POS infrastructure including online card transactions	QR code based card acceptance infrastructure
SMALL MERCHANTS (With turnover up to Rs. 20 lakhs during the previous financial year)	Not exceeding 0.40% (MDR cap of Rs. 200 per transaction)	Not exceeding 0.30% (MDR cap of Rs. 200 per transaction)
OTHER MERCHANTS (With turnover above Rs. 20 lakhs during the previous financial year)	Not exceeding 0.90% (MDR cap of Rs.1000 per transaction)	Not exceeding 0.80% (MDR cap of Rs. 1000 per transaction)

- MDR levied on the merchant shall not exceed the cap rates as prescribed above, irrespective of the entity which is deploying the card acceptance infrastructure at the merchant location

- Merchants on-boarded, shall not pass on the MDR charges to customers while accepting payments through Debit Cards

(iii) GOI Notification: No.6(19)/2017-DPD-1 issued by MEITY, dated 27.12.2017

No MDR for transaction value less than or equal to Rs.2,000/- using Debit Cards/Bhim UPI/ Aadhar pay

Merchants on-boarded, shall not pass on the MDR charges to customers while accepting payments through Debit Cards/Bhim UPI/Aadhar pay

An undertaking to be obtained from the merchants on-boarded, confirming that no extra charges are levied for usage of Debit Cards /Bhim UPI/ Aadhar pay

II. GOI Finance Bill: Amendment to Payment and Settlement Systems Act, 2007

Clause 194: In the payment and settlement systems act 2007, after the Section 10, the following section shall be inserted with effect from 01st day of November 2019, namely The Section 10A "Not withstanding anything in the said act, no bank or system provider shall impose any charge, upon anyone, either directly or indirectly for using the electronic modes of payment prescribed under Section 269SU of the income tax act 1961."

In exercise of powers conferred by Section 269SU in Income Tax 1961, CBDT vide notification number 32/2019 dated 30.12.2019 has inserted Sec119AA in the Income Tax rules 1962 prescribing the following electronic payment modes:

- Debit card powered by RUPAY,

- Unified Payment Interface(Bhim UPI/UPI) and
- Unified Payments Interface Quick Response Code (UPI QR Code) (BHIM-UPI QR Code).”

Further guidelines on Operations / MDR issued by RBI/ GOI from to time to be strictly adhered to.

III. Cash withdrawal using Point of Sale (PoS) terminals

RBI Notification DPSS.CO.PD.No.501/02.143/2019-20 dated 29.08.2019. Guidelines on Cash withdrawal at PoS devices enabled for all debit cards/o pen loop prepaid cards issued by banks.

The instructions outlined therein, limit –

- Cash withdrawal limit in Tier I and II centres is ₹ 1000/- per day and ₹ 2,000/- per day in Tier III to VI centres

Customer charges, if any, on such cash withdrawals to not more than 1% of the transaction amount. Bank may extend the facility of withdrawal of cash at any merchant establishment designated by them after a due diligence process