Cards Business Policy

For

SOUTH INDIAN Bank
EXPERIENCE NEXT-GEN BANKING

PART A

Credit Card Business Policy

For

Version Number: 4.1

Dated: 04th February 2025

TABLE OF CONTENTS

1. DOCUMENT UPDATE HISTORY

Version No	Date	Department
1.0	DBR/RBD/S-087/2021-22 DATED 15.06.2021	RBD
2.0	DBR/RBD/S-043 /2022-23 DATED 07.06.2022	RBD
3.0	DBR/RBD/S-158 /2023-24 DATED 24.08.2023	RBD
4.0	DBR/RBD/S-136/2024-25 DATED 26-09-2024	RBD

2. BACKGROUND:

South Indian Bank currently has issuance of Debit Cards, Prepaid Cards, FasTag, and co-branded credit cards. Bank may also issue Bank's own organic credit card, White Label Credit Cards in partnership with other banks or its own co-branded credit cards in partnership with non-banking entities.

3. GENERAL OBJECTIVE:

In the light of RBI Guidelines on card business, policy for credit card business is formulated. The policy has been framed within the ambit of Payment and Settlement System Act 2007 and Master Direction – Credit Card and Debit Card – Issuance and Conduct Directions, 2022 amended on March 07,2024. The objective of this document is to define the policy under which the bank offers credit card services to customers of the bank keeping in mind the key aspects which are listed below:

- To provide a framework of rules/regulations/standards/practices for credit card business in order to ensure that the same are in alignment with the best customer practices.
- To ensure adherence of KYC/AML/CFT norms specified by RBI with respect to card business from time to time.
- Growing demand from customers.
- Addressing the risk involved in card issuance business and necessary risk mitigation measures.
- Increased efficiency by offering a cost effective delivery channel for banking services.
- 24x7 Service availability.
- Security issues related to card issuance business.
- Grievance mechanism policy

The Board approved credit card policy shall be made available on the website of the bank.

4. TYPES OF CREDIT CARDS

In line with RBI guidelines, Bank can undertake credit card business either departmentally or through a subsidiary company set up for the purpose or by entering into tie-up arrangement with one of the banks already having arrangements for issue of co-branded credit cards or issue

credit cards in co-branding with non-banking entities. Prior approval of RBI is not necessary for banks desirous of undertaking credit card business either independently or in tie-up arrangement with other card issuing banks. Banks can do so with the approval of their Boards. However, only banks with net worth of Rs.100 Crore and above should undertake credit card business. Banks desirous of setting up separate subsidiaries for undertaking credit card business would, however, require prior approval of the Reserve Bank. While issuing co-branded credit cards, banks must undertake due diligence on the non-bank entity to protect themselves against the reputation risk to which they are exposed to in such an arrangement.

Bank may issue credit cards including co-branded credit cards, secured credit card against Banks deposit, Business credit card, corporate credit cards to the employees of bank's corporate customers, charge card, as well as add-on credit cards. Bank may issue business credit cards to business entities/individuals for business expenses. The business credit cards may also be issued as charge cards, corporate credit cards or by linking a credit facility such as overdraft/cash credit provided for business purpose as per the terms and conditions stipulated for the facility concerned. Bank shall put in place an effective mechanism to monitor end use of funds. Business credit cards can be issued together with add-on cards wherever required.

The add-on cards shall be issued only to the persons specifically identified by the principal cardholder under both personal and business credit card categories. Add-on cards shall be issued with the clear understanding that the liability will be that of the principal cardholder. Similarly, while issuing corporate credit cards, the responsibilities and liabilities of the corporate and its employees shall be clearly specified. The liability of the corporate/business entity shall form part of its assessed credits.

5. CREDIT CARD IN CO-BRANDING WITH NON-BANKING ENTITIES

5.1 TERMS AND CONDITIONS:

1. Bank shall ensure prudence while issuing credit cards and independently assess the credit risk while issuing cards to persons, taking into account independent financial means of applicants.
2. The Bank shall issue cards only to customers who fully comply with KYC/AML/CFT norms stipulated by RBI from time to time.

3. As Credit Card issuer, it should be ensured that all Core functions with regard to Credit Card Issuance and Liability remains with the Bank.
4. The issue of credit cards as a payment mechanism would be subject to relevant guidelines including guidelines issued by the Department of Payment and Settlement Systems of RBI under the Payment and Settlement Systems Act, 2007 & Master Direction – Credit Card and Debit Card – Issuance and Conduct Directions, 2022 as amended from time to time.
5. The credit card customer assessment & issuance will be carried out strictly in adherence to the Credit Card Lending policy under the ownership of Credit Department as amended from time to time.
6. Bank shall assess the credit limit for a credit card customer having regard to the limits enjoyed by the cardholder from other banks on the basis of self- declaration/ credit information obtained from a CIC.
7. In case of rejection of a Credit Card application bank shall convey in writing the specific reason/reasons which have led to the rejection of the credit card application.
8. Generally, credit cards issued/reissued by the Bank (physical and virtual) shall be enabled for use only at contact based points of usage [viz. ATMs and Point of Sale (PoS) devices] within India. Bank shall provide credit cardholders a facility for enabling card not present (domestic and international) transactions, card present (international) transactions and contactless transactions, as per the process outlined in para 8 below. The card issuance shall also be subject to directions issued under FEMA 1999 as amended from time to time and Reserve Bank of India guidelines (RBI Instructions in this regard shall be adhered)
9. Additionally, bank shall provide to all credit cardholders:
    - facility to switch on / off and set / modify transaction limits (within the overall card limit, if any, set by the issuer) for all types of transactions – domestic and international, at PoS / ATMs / online transactions / contactless transactions, etc.
    - the above facility on a 24x7 basis through mobile application.
    - may provide facility to enable /disable over limit facility
    - alerts / information / status, etc., through SMS / e-mail, as and when there is any change in status of the card. The Bank shall not dispatch a card to customer unsolicited. In case of renewal of an existing card, the bank may provide the cardholder an option to decline the same if he/she wants to do so before dispatching the renewed card. In case a card is blocked at the request of the cardholder,

replacement card in lieu of the blocked card shall be issued with the explicit consent of the cardholder.

10. The relationship between the Bank and the card holder shall be contractual.
11. The Bank shall make available to the cardholders in writing, a set of contractual terms and conditions governing the issue and use of such a card. Bank shall provide a one-page Key Fact Statement along with the credit card application containing the important aspects of the card such as rate of interest, quantum of charges, among others.
12. The Bank may alter the terms and conditions on card issuance/operations, but sufficient notice of the change shall be given to the cardholder to enable him to withdraw if he so chooses. A period shall be specified, after which time the cardholder would be deemed to have accepted the terms if he had not withdrawn during the specified period. This is in compliance with the terms of BCSBI (Banking Codes and Standards Board of India) code, accepted by the bank.
13. The bank shall not offer facility of credit Card to customers who do not provide mobile numbers & email ID to the bank.
14. The Bank shall put the cardholder under an obligation to take all appropriate steps to keep safe the card and the means (such as PIN, CVV, Expiry Date or One Time Password) which enable it to be used.
15. The Bank shall put the cardholder under an obligation not to record the PIN or OTP, in any form that would be intelligible or otherwise accessible to any third party if access is gained to such a record, either honestly or dishonestly.
16. Bank shall ask its customers to mandatorily register for SMS alerts and wherever available register for e-mail alerts, for electronic banking transactions. The SMS alerts shall mandatorily be sent to the customers, while email alerts may be sent, wherever registered. The name of the Merchant where transaction is being carried out shall be part of the message wherever made available by the acquirer.
17. The customers shall be advised to notify bank of any unauthorised electronic banking transaction at the earliest after the occurrence of such transaction, and informed that, the longer the time taken to notify the bank, the higher will be the risk of loss to the bank/ customer. To facilitate this, bank shall provide customers with 24x7 access through multiple channels (at a minimum, via website, phone banking, SMS, e-mail, IVR, a dedicated toll-free helpline,.) for reporting unauthorised transactions that have taken place and/ or loss or theft of payment instrument such as card, etc.

18. Bank shall also enable customers a prominently visible web-site link, phone banking, SMS, e-mail, IVR, a dedicated toll- free helpline, reporting to home branch, etc. for reporting unauthorized transactions and initiating blocking of card.
19. The loss/ fraud reporting system shall also ensure that immediate response (including auto response) is sent to the customers acknowledging the complaint along with the registered complaint number. The communication systems used by bank to send alerts and receive their responses thereto shall record the time and date of delivery of the message and receipt of customer's response, if any. This shall be important in determining the extent of a customer's liability.
20. On receipt of report of an unauthorised transaction from the customer, bank shall take immediate steps to prevent further unauthorised transactions in the card.
21. Related clause shall form an integral part of the terms & conditions. This is in line with RBI circular on Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions.
22. The Bank shall exercise care when issuing PINs or OTP and shall be under an obligation not to disclose the cardholder's PIN or OTP, except to the cardholders.
23. Limited Liability of a Customer.
    a. Zero Liability of a Customer

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

    i. Contributory fraud/ negligence/ deficiency on the part of the bank (irrespective of whether or not the transaction is reported by the customer).
    ii. Third party breach where the deficiency lies neither with the bank nor with the customer but lies elsewhere in the system, and the customer notifies the bank within three working days of receiving the communication from the bank regarding the unauthorised transaction.

    b. Limited Liability of a Customer

    A customer shall be liable for the loss occurring due to unauthorised transactions in the following cases:

    i. In cases where the loss is due to negligence by a customer, such as where he has shared the payment credentials, the customer will bear the entire loss until

he reports the unauthorised transaction to the bank. Any loss occurring after the reporting of the unauthorised transaction shall be borne by the bank.

ii. In cases where the responsibility for the unauthorised electronic banking transaction lies neither with the bank nor with the customer, but lies elsewhere in the system and when there is a delay (of four to seven working days after receiving the communication from the bank) on the part of the customer in notifying the bank of such a transaction, the per transaction liability of the customer shall be limited to the transaction value or the amount mentioned in Table 1, whichever is lower.

Table 1
Maximum Liability of a Customer

• Type of Account	Maximum Liability
• Credit cards with limit up to Rs.5 lakh	10,000
• Credit cards with limit above Rs.5 lakh	25,000

24. Further, if the delay in reporting is beyond seven working days, the customer liability shall be determined as per the bank's Policy on Customer Compensation. Bank shall provide the details of the policy in regard to customers' liability formulated in pursuance of these directions at the time of opening the accounts. Bank shall also display the approved policy in public domain for wider dissemination. The existing customers shall also be individually informed about the bank's policy.
25. Overall liability of the customer in third party breaches, as detailed in paragraph 13 (a) (ii) and paragraph 13 (b) (ii) above, where the deficiency lies neither with the bank nor with the customer but lies elsewhere in the system, is summarised in the Table below:

Table 2

Time taken to report the fraudulent transaction from the date of receiving the communication	**Customer's liability (₹)**
Within 3 working days	Zero liability
Within 4 to 7 working days	The transaction value or the amount mentioned in Table 1, whichever is lower
Beyond 7 working days	As per bank's Board approved policy

26. The Bank may charge the customer for issuance & usage of credit cards. The charges/ interest rates shall be made known to the customers. MD & CEO of the bank shall be the

authority to fix/revise the charges/interest rates and also shall have full power to add or remove any charges/interest rates. Interest shall be levied only on the outstanding amount, adjusted for payments/refunds/reversed transactions.

27. Cardholders shall be provided option to submit request for closure of credit card account through multiple channels such as mobile-app, helpline, Email-id or any other mode. Bank shall not insist on sending a closure request through post or any other means which may result in the delay of receipt of the request.
28. Any request for closure of a credit card shall be honoured within seven working days, subject to payment of all dues by the cardholder. Subsequent to the closure of credit card, the cardholder shall be immediately notified about the closure through email, SMS, etc. In case of secured cards, once the card closure is completed, the deposit will be delinked and lien will be lifted within T+7 (working day).
29. Failure on the part of the Bank to complete the process of closure within seven working days shall result in a penalty of ₹500 per calendar day of delay payable to the cardholder, till the closure of the account provided there is no outstanding in the account.
30. If a credit card has not been used for a period of more than one year, the process to close the card shall be initiated after intimating the cardholder. If no reply is received from the cardholder within a period of 30 days, the card account shall be closed by the bank, subject to payment of all dues by the cardholder.
31. The information regarding the closure of card account shall be updated with the Credit Information Company/ies within a period of 30 days.
32. Bank will not report any credit information relating to a new credit card account to Credit Information Companies prior to activation of the card.
33. Bank shall seek written consent of the applicant before issuing a credit card. Alternatively, bank may use other digital modes with multifactor authentication to obtain explicit customer consent. Such alternative digital modes, shall be communicated to RBI.
34. Bank shall seek One Time Password (OTP) based consent from the cardholder for activating a credit card, if the same has not been activated by the customer for more than 30 days from the date of issuance. If no consent is received for activating the card, bank shall close the credit card account without any cost to the customer within seven working days from date of seeking confirmation from the customer. In case of a renewed or replaced card, the closure of an inactivated card shall be subject to payment of all dues by the cardholder.

35. The MITC, shall be published/sent to the customers, at the acceptance stage (welcome kit) and in important subsequent communications. The MITC shall be provided to the customer at the time of on boarding and each time, a condition is modified with notice to the customer. The MITC and copy of the agreement signed between the Bank and cardholder shall be sent to the registered email address of the cardholder or postal address as per the choice of the customer.
36. In case Bank, at its discretion, decide to block/deactivate/suspend a credit card, bank shall ensure necessary customer communications to eliminate customer inconvenience. Presently this is undertaken in scenarios like card delinquency/NPA, instances of identified fraud, instances of card compromises reported by network or regulator, card dormancy. The operating procedure on the above scenarios will be included in the Standard Operating Procedure [SOP] for Credit cards.
37. It shall be ensured that blocking/deactivating/suspending a card or withdrawal of benefits available on any card is immediately intimated to the cardholder along with reasons thereof through electronic means (SMS, email, etc.) and other available modes.
38. The terms shall clearly specify the time-period for reversal of unsuccessful/failed transactions and the compensation payable for failure to meet the specified timeline.
39. The terms may be altered by the Bank, but 30 days' notice of the change shall be given to the cardholder to enable him/her to withdraw if he/she so chooses. After the notice period of 30 days, the cardholder would be deemed to have accepted the terms if he/she had not withdrawn during the specified period. The change in terms shall be notified to the cardholder through all the communication channels available.
40. The terms shall put the cardholder under an obligation to take all appropriate steps to keep the card safe and not to record the PIN or code, in any form that would be intelligible or otherwise accessible to any third party if access is gained to such a record, either honestly or dishonestly.
41. The terms shall specify that the Bank shall exercise care when issuing PINs or codes and shall be under an obligation not to disclose the cardholder's PIN or code to anyone, except to the cardholder.

5.2 ROLES & RESPONSIBILITY:

As part of a co-branded credit card issuance model, there shall be two parties viz the bank and Co-branding entity.

1. Bank shall implement systems for card issuance & processing, authentication, authorization, reconciliation & settlement, customer grievance redressal, repayment and Fraud Risk Management, on its own/ through a Technology service provider. Bank at its discretion may outsource various activities of the credit card operations in accordance with Banks outsourcing policy and in adherence to the 'Master Directions on Outsourcing of Information Technology Services, dated April 10, 2023' and 'Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services', as amended from time to time.
2. Further, Bank shall not share card data (including transaction data) of the cardholders with the outsourcing partners unless sharing of such data is essential to discharge the functions assigned to the latter. In case of sharing of any data as stated above, explicit consent from the cardholder shall be obtained. It shall also be ensured that the storage and the ownership of card data remains with the Bank.
3. The ownership of the Credit card business of the bank in case of co-branding with non-banking entity shall remain with Retail Banking Department and persons handling the related work should have the complete working knowledge and understanding of operational elements of credit cards.
4. Roles of the non-banking co-branding partner

   Co-branding entity shall only be responsible for the marketing/distribution of the cards and providing access to the cardholder for the goods/services that are offered. The co-branding partner (CBP) shall not have access to information relating to transactions undertaken through the co-branded card. Post issuance of the card, the co-branding partner shall not be involved in any of the processes or the controls relating to the co-branded card except for being the initial point of contact in case of grievances. However, for the purpose of cardholder's convenience, card transaction related data may be drawn directly from the Bank's system in an encrypted form and displayed in the CBP platform with robust security. The information displayed through the CBP's platform shall be visible only to the cardholder and shall neither be accessed nor be stored by the CBP
5. Outsourcing of credit card operations

Bank at its discretion may outsource the following activities to facilitate credit card operations to the TSP in accordance with Banks outsourcing policy.

a. Customer onboarding assistance– Using Bank approved KYC modes as regulated by RBI from time to time.
b. Facilitates card issuance – To customers based on the Credit Card Lending policy of the Bank.
c. Physical card preparation and dispatch
d. Aids in customer lifecycle management – Including transaction authorization & processing, customer grievances, chargeback, refunds and all day to day activities for servicing and enabling the seamless usage of the credit card issued under the arrangement shall be handled by the TSP.
e. Credit Limit Maintenance & Management – The Credit limit to onboarded customers shall be allocated based on bank's Credit Card Lending Policy. Accounting of transactions, limit utilization, EMI conversion, interest calculation, late payment fees, other charges, repayments etc related to the credit limit utilized by the customer shall be implemented in the credit management system in accordance with MITC updated time to time.
f. Reconciliation of customer accounts – Reconciliation may be handled by the TSP, including management of customer complaints, chargebacks, refunds and tallying of ledgers maintained at the bank with respect to the scheme settlement.
g. Reports & MIS –The TSP shall provide all regulatory and scheme related reports to the bank for onward submission and all necessary MIS as requested by the bank from time to time shall be provided by the TSP.

6. Responsibility of the activities related to credit card.
   a. Responsibility of all activities performed by the TSP and Co-Branding Partner shall be with the bank

Activity	Description	Ownership
Product Features	The features and offers to be made available on the Credit Card	RBD
Card Scheme related activities	All activities pertaining to the card schemes.	Technology – DTD Business – RBD

		Operations & Processing - BOG
Customer Identification & limit assignment	Customer segment identification, risk & underwriting	Credit/IRMD
Customer Onboarding	Onboarding customer including KYC	DTD/Compliance/ BOG/RBD
Card Issuance	Physical Card issuance & delivery to customer	RBD
AML & Customer Due Diligence	AML & CDD checks for customers	Compliance & RBD
Transaction Processing & Authorisation	Enabling customers to transact using the Credit Card	DTD
Reconciliation of Credit Card transactions	Daily recon activities of Transaction processing	BOG under guidance of CFM
Reconciliation of Interest application, collection, charges etc	Interest calculation, interest posting, reversals etc	Credit/CFM
Statutory Audit Compliance	All activities relating to statutory audit compliance	CFM
Profitability review, costs & tax.	Profitability review, review of cost of funds, and other costs & all tax Matters	CFM
Customer Service	Customer complaints, dispute resolution, grievance mechanism	FMG/RBD-CEG
Collections recovery & NPA Management	Collection of dues, repayments, NPA reporting & management	Credit-Recovery

b. Bank shall put in place a detailed Standard Operating procedure for the entire Credit Card system & lifecycle management approved by PPAC. All applications/systems which may be used by Bank/Customers/third party shall be explicitly mentioned in SOP.
c. The overview, implementation and compliance of new services related to card business shall be the responsibility of Retail Banking Department in co-ordination with DTD, Credit, CFM, Compliance, Legal, IRMD, BOG and other divisions of the Bank.
d. Under the guidance of CFM Department, BOG shall maintain all the accounts required as part of the credit card programme as per the approved SOP as amended from time to time.
e. IRMD/IS Audit/CISO/Inspection/CFM – Periodic/Concurrent audits shall be conducted to identify the effectiveness of the credit card systems and operations provided by the TSP and marketing/distribution activities of cobranding partner.

5.3 INTEREST RATES AND OTHER CHARGES

1. Bank shall be guided by the instructions on interest rate on advances issued by RBI and as amended from time to time, while determining the interest rate on credit card dues.
2. Bank shall also prescribe a ceiling rate of interest, including processing and other charges, in respect of credit cards.
3. Bank shall maintain transparency in levying of differential interest rates, wherever applicable (i.e. if higher interest rate is charged to the cardholder on account of his payment/default history, the same shall be made known to the cardholder)
4. Bank shall upfront indicate to the credit card holder, the methodology of calculation of finance charges with illustrative examples, particularly in situations where a part of the amount outstanding is only paid by the customer.
5. Bank shall ensure that there is no delay in dispatching bills/statements and the customer has sufficient number of days (at least one fortnight) for making payment before the interest starts getting charged
6. Bank shall quote Annualized Percentage Rates (APR) on card products (separately for retail purchase and for cash advance, if different).
7. The late payment charges, including the method of calculation of such charges and the number of days, shall be prominently indicated.

8. The manner in which the outstanding unpaid amount will be included for calculation of interest shall also be specifically shown with prominence in all monthly statements.
9. Even where the minimum amount indicated to keep the card valid has been paid, it shall be indicated in bold letters that the interest will be charged on the amount due after the due date of payment.
10. A legend/notice to the effect that "Making only the minimum payment every month would result in the repayment stretching over years with consequent interest payment on your outstanding balance" shall be prominently displayed in all the monthly statements so as to caution the customers about the pitfalls in paying only the minimum amount due.
11. The "Most Important Terms and Conditions" shall specifically explain that the 'interest-free credit period' is lost if any balance of the previous month's bill is outstanding with illustrative examples.
12. Bank shall follow uniform method of determining over-due status for credit card accounts while reporting to credit information companies and for the purpose of levying penal charges viz., late payment charges.
13. Banks shall not levy any charge that was not explicitly indicated to the credit card holder at the time of issue of the card and without getting his/her consent. However, this would not be applicable to charges like service taxes, etc. which may subsequently be levied by the Government or any other statutory authority.
14. The terms and conditions for payment of credit card dues, including the minimum payment due, shall be stipulated so as to ensure that there is no negative amortization. The unpaid charges/levies/taxes shall not be capitalized for charging/compounding of interest.
15. Changes in charges shall be made only with prospective effect giving prior notice of at least one month. If a cardholder desires to surrender his/her card on account of any change in charges to his/her disadvantage, he/she shall be permitted to do so without levying any extra charge for such closure other than what is already agreed at the time of card issuance, subject to payment of all dues by the cardholder.
16. There shall be transparency (without any hidden charges) in issuing credit cards.
17. Bank shall ensure complete transparency in the conversion of credit card transactions to Equated Monthly Instalments (EMIs) by clearly indicating the principal, interest and upfront discount provided by the merchant/Bank (to make it no cost), prior to the

conversion. The same shall also be separately indicated in the credit card bill/statement. EMI conversion with interest component shall not be camouflaged as zero-interest/no-cost EMI.

18. Bank shall ensure that the credit limit as sanctioned and advised to the cardholder is not breached at any point in time without seeking explicit consent from the cardholder.
19. The convenience fee, if any charged on specific transactions, shall be indicated to the cardholder in a transparent manner, prior to the transaction.

5. 4 BILLING

1. Bank shall ensure that wrong bills are not raised and issued to cardholders. In case, a cardholder protests any bill, the bank shall provide explanation and, wherever applicable, documentary evidence shall be provided to the cardholder within a maximum period of 30 days from the date of complaint.
2. Bank shall ensure that there is no delay in sending/dispatching/emailing bills/statements and the customer has sufficient number of days (at least one fortnight) for making payment before the interest starts getting charged. In order to obviate frequent complaints of delayed billing, bank may consider providing bills and statements of accounts through internet/mobile banking with the explicit consent of the cardholder. Bank shall put in place a mechanism to ensure that the cardholder is in receipt of the billing statement.
3. No charges shall be levied on transactions disputed as 'fraud' by the cardholder until the dispute is resolved.
4. Bank shall provide cardholders an option to modify the billing cycle of the credit card at least once as per their convenience.
5. Any credit amount arising out of refund/failed/reversed transactions or similar transactions before the due date of payment for which payment has not been made by the cardholder, shall be immediately adjusted against the 'payment due' and notified to the cardholder.
6. Bank shall seek explicit consent of the cardholder to adjust credit amount beyond a cut-off, one percent of the credit limit or ₹5000, whichever is lower, arising out of refund/failed/reversed transactions or similar transactions against the credit limit for which payment has already been made by the cardholder. The consent shall be obtained through e-mail or SMS within seven days of the credit transaction. The bank shall

reverse the credit transaction to the cardholder's bank account, if no consent/response is received from the cardholder. Notwithstanding the cut-off, if a cardholder makes a request to the bank for reversal of the credit amount outstanding in the card account into his/her bank account, the bank shall do it within three working days from the receipt of such request.

7. Bank shall provide the list of payment modes authorised by them for making payment towards the credit card dues, in their websites and billing statements. Further, Bank shall advise cardholders to exercise due caution and refrain from making payments through modes other than those authorised by them.
8. Any debit to the credit card account shall be done as per the authentication framework prescribed by the Reserve Bank from time to time, and not through any other mode/instrument
9. For business credit cards wherein the liability rests fully with the corporate or business entity (principal account holder), timeframe provided for payment of dues and adjustment of refunds may be as agreed between the Bank and the principal account holder

5.5 USE OF DIRECT SALES AGENT (DSAS)/DIRECT MARKETING AGENTS (DMAS) AND OTHER AGENTS

1. Bank may outsource the various credit card operations, however, it shall be ensured that, the appointment of such service providers does not compromise with the quality of the customer service and bank's ability to manage credit, liquidity and operational risks. Confidentiality of the customer's records, respect for customer privacy, and adherence to fair practices in debt collection shall be ensured at all times.
2. The decision-making power for issue of credit card to a customer shall remain only with the Bank and the role of the Direct Sales Agent (DSA)/Direct Marketing Agent (DMA)/other agents shall remain limited to soliciting/servicing the customer/ account.
3. A Code of Conduct for the DSAs engaged by bank for marketing the products/services shall be prescribed. Bank shall ensure that, the DSAs engaged for marketing credit card products scrupulously adhere to the Code of Conduct for Credit Card operations of the

bank which shall be displayed on the website of the bank and be available easily to any credit card holder.

4. Bank shall have a system of random checks and mystery shopping to ensure that the agents have been properly briefed and trained in order to handle with care and caution their responsibilities, particularly in the aspects like soliciting customers, hours for calling, privacy of customer information, conveying the correct terms and conditions of the product on offer, etc.
5. Bank shall ensure that only telemarketers who comply 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)" are engaged for the purpose. The bank representatives shall contact the customers only between 10:00 hrs and 19:00 hrs.

5.6 ISSUE OF UNSOLICITED CARDS/FACILITIES

1. Unsolicited cards shall not be issued. In case, an unsolicited card is issued and activated without the written/explicit consent of the recipient and the latter is billed for the same, bank shall not only reverse the charges forthwith, but also pay a penalty without demur to the recipient amounting to twice the value of the charges reversed. Any loss arising out of misuse of such unsolicited cards will be the responsibility of the bank only and the person in whose name the card has been issued shall not be held responsible for the same.
2. In addition, the person in whose name the card is issued can also approach the Banking Ombudsman who would determine the amount of compensation payable bank to the recipient of the unsolicited card as per the provisions of the Banking Ombudsman Scheme 2006, i.e., for loss of complainant's time, expenses incurred, harassment and mental anguish suffered by him.
3. The consent for the cards issued or the other products offered along with the card shall be explicit and not implied.
4. Unsolicited loans or other credit facilities shall not be offered to the credit cardholders without seeking explicit consent. In case an unsolicited credit facility is extended without the written/explicit consent of the cardholder and the latter objects to the same, the Bank shall not only withdraw the facility, but also be liable to pay such penalty as may be considered appropriate by the RBI Ombudsman, if approached.

5. Bank shall not unilaterally upgrade credit cards and enhance credit limits. Explicit consent of the cardholder shall invariably be taken whenever there is/are any change/s in terms and conditions. In case of reduction in the credit limit, the Bank shall intimate the same to the cardholder.
6. Bank shall not dispatch a card to a customer unsolicited. In case of renewal of an existing card, the cardholder shall be provided an option to decline the same if he/she wants to do so before dispatching the renewed card. In case a card is blocked at the request of the customer, replacement card in lieu of the blocked card shall be issued with the explicit consent of the cardholder.

5.7 CUSTOMER CONFIDENTIALITY

1. Bank shall not reveal any information relating to customers obtained at the time of opening the account or issuing the 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. Explicit consent for the same shall be obtained during card application.
2. Further, in case where the customers give explicit consent to the bank for sharing the information provided by them with other agencies, bank shall clearly state and explain clearly to the customer the full meaning/ implications of the disclosure clause. The information being sought from customers should not be of such nature as will violate the provisions of the law relating to maintenance of secrecy in the transactions. Bank shall be solely responsible for the correctness or otherwise of the data provided for the purpose.
3. The disclosure to the DSAs/recovery agents shall 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 shall not be released by the bank. Bank shall ensure that the DSAs/DMAs do not transfer or misuse any customer information during marketing of credit card products.

5.8 REPORTING TO CREDIT INFORMATION COMPANIES (CICS)

1. For providing information relating to credit history/repayment record of the card holder to a Credit Information Company (that has obtained Certificate of Registration from

RBI), bank shall explicitly bring to the notice of the customer that such information is being provided in terms of the Credit Information Companies (Regulation) Act, 2005.

2. Before reporting default status of a credit card holder to a Credit Information Company which has obtained Certificate of Registration from RBI and of which the bank is a member, bank shall ensure that, a procedure, duly approved by the Board, including intimating the cardholder prior to reporting of the status. . The procedure shall also cover the notice period for such reporting as also the period within which such report will be withdrawn in the event the customer settles his dues after having been reported as defaulter. Bank shall be particularly careful in the case of cards where there are pending disputes. The disclosure/release of information, particularly about the default, shall be made only after the dispute is settled as far as possible. In all cases, a well laid down procedure shall be transparently followed. These procedures shall also be transparently made known as part of Most Important Terms & Conditions. In the event the customer settles his/her dues after having been reported as defaulter, Bank shall update the status with CIC within 30 days from the date of settlement. Bank shall be particularly careful in the case of cards where there are pending disputes. The disclosure/release of information, particularly about the default, shall be made only after the dispute is settled. In all cases, a well laid down procedure shall be transparently followed and be made a part of Most Important Terms & Conditions.
3. Bank shall report a credit card account as 'past due' to credit information companies (CICs) or levy penal charges, viz. late payment charges and other related charges, if any, only when a credit card account remains 'past due' for more than three days. The number of 'days past due' and late payment charges shall, however, be computed from the payment due date mentioned in the credit card statement, as specified under the regulatory instructions on ‘Prudential norms on Income Recognition, Asset Classification and Provisioning pertaining to Advances’ amended from time to time. Late payment charges and other related charges shall be levied only on the outstanding amount after the due date and not on the total amount due.

5.9 FAIR PRACTICES IN DEBT COLLECTION

1. In the matter of recovery of dues, it shall be ensured that bank, as also agents of bank, adhere to the extant instructions on Fair Practice Code for lenders (as also BCSBI’s Code of Bank’s Commitment to Customers).

2. With regard to appointment of third-party agencies for debt collection, it shall ensure that their agents refrain from actions that could damage their integrity and reputation and observe strict customer confidentiality. All communications issued by recovery agents must contain the name, email-id, telephone number and address of the concerned senior officer of the bank whom the customer can contact. Further, bank shall provide the name and contact details of the recovery agent to the cardholder immediately upon assigning the agent to the cardholder.
3. Bank/Bank's agents shall not resort to intimidation or harassment of any kind, either verbal or physical, against any person in debt collection efforts, including acts intended to humiliate publicly or intrude the privacy of the credit card holders' family members, referees and friends, making threatening and anonymous calls or making false and misleading representations.
4. Bank shall also ensure to comply with the extant guidelines in respect of engagement of recovery agents issued by RBI, as amended from time to time.
5. When outsourcing for various credit card related operations, bank shall be extremely careful that the appointment of such service providers do not compromise the quality of the customer service and banks' ability to manage credit, liquidity and operational risks. In the choice of the service provider, the bank shall be guided by the need to ensure confidentiality of the customer's records, respect customer privacy and adhere to fair practices in debt collection.
6. Bank shall ensure that their employees/agents do not indulge in mis-selling of credit cards by providing incomplete or incorrect information to the customers, prior to the issuance of a credit card. The bank shall also be liable for the acts of their agents. Repetitive complaints received in this regard against any employee/agent shall be taken on record by the Bank and appropriate action shall be initiated against them including blacklisting of such agents. A dedicated helpline and email-id shall be available for the cardholders to raise complaints against any act of mis-selling or harassment by the representative of the Bank.

5.10 REDRESSAL OF GRIEVANCES:

1. Generally, a time limit of 60 (sixty) days may be given to the customers for referring their complaints/grievances.

2. The Bank shall display customer support number for customer grievance on bank's website.
3. The Bank shall display their grievance redressal procedure of the bank and the time frame for responding to the complaints on bank's website.
4. The name and contact number of designated grievance redressal officer of the bank shall be mentioned on the credit card bills.
5. The Bank shall employ proper acknowledgement system for follow up by providing complaint number for customer's grievance/complaints. The designated officer should ensure that genuine grievances of credit card subscribers are redressed promptly without involving delay.
6. Bank shall adhere to RBI guidelines on Online Dispute Resolution (ODR) system for digital payments as amended from time to time.
7. Business Operations Group (BOG) in co-ordination with Corporate Financial Management (CFM) department shall be responsible for reconciliation of transactions using credit cards.
8. Bank shall ensure that the personnel attending customer queries/complaints is trained adequately to competently handle all customer complaints.
9. DPSS guidelines on timeframe for reconciliation of failed transactions at ATMs, PoS, ecommerce etc as amended from time to time should be complied in this regard. The RBI circular on Harmonisation of TAT and customer compensation for failed transactions using authorized payments systems shall form the basis of Bank's Grievance redressal system for credit cards.
10. RBI guidelines regarding Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions as amended from time to time shall be adhered to in this regard.
11. Bank shall also have a mechanism to escalate automatically unresolved complaints from a call center to higher authorities and the details of such mechanism shall be put in public domain through bank's website.
12. The grievance redressal procedure of the bank and the time frame fixed for responding to the complaints shall be placed on the bank's website. There shall be a system of acknowledging customers' complaints for follow up, such as complaint number/docket number, even if the complaints are received on phone.

13. If a complainant does not get satisfactory response from the bank within a maximum period of thirty (30) days from the date of his lodging the complaint, he will have the option to approach the Office of the concerned Banking Ombudsman for redressal of his grievance/s. The bank shall be liable to compensate the complainant for the loss of his time, expenses, financial loss as well as for the harassment and mental anguish suffered by him for the fault of the bank and where the grievance has not been redressed in time.
14. The nodal officer of the Bank for customer complaints shall also act as Grievance Redressal Officer with respect to card operations.
15. Management of customer grievances should be with the Bank. Outsourced party can at best be the first point of contact with verification access for the bank to L1 level.

5.11 OPERATIONAL ELEMENTS:

Retail Banking Department shall share responsibility for operational elements of card business along with the other departments of the Bank. The following operational elements should be considered prior to adding new credit card product/service.

1. **Planning and Deployment:** The development of any new credit card product/service shall encompass proper due diligence. Related hardware, software, obsolescence, support and other similar issues should be carefully evaluated.
2. **Marketing and Promotion:** Retail Banking Department shall conduct market survey and new services shall be introduced in coordination with DTD and the service provider. Bank, along with the service provider shall promote credit card usage at POS/Online by conducting various campaigns and by awarding gifts/cash back/reward points to customers based on card usage on its own or through an outsourced agency.
3. **Audit and Monitoring:** Audit and regulatory compliance risks shall be carefully evaluated and identified prior to implementation as well as on an ongoing basis.
4. **Vendors and Outsourcing:** In addition to own resources, the Bank may rely on third parties to provide credit card product and related services. Risk Management of the outsourced technology services which should also consider the third party's ability to provide the product/services from a standpoint of internal controls, security, maintenance & upkeep of the system and financial condition.

5. **Legal and Regulatory:** Credit card products & services should be evaluated on for legal and regulatory issues. Privacy issues should be addressed prior to introducing a product.
6. **Reconciliation:** Business Operations Group (BOG) in co-ordination with Corporate Financial Management (CFM) department shall be responsible for reconciliation of transactions using credit cards.
7. **Disaster Recovery and Contingency Plans:** Disaster recovery arrangements shall be set in line with regulatory guidelines.
8. **Operational Risk:** Portfolio performance shall be submitted by Credit Card team to IRMD on a monthly basis to assess the Portfolio risk. BOG shall carry out daily reconciliation & submit the reconciliation reports to CFM department on an ongoing basis for assessment & overview.
9. **IT Outsourcing Review –** Periodic review of IT outsourcing activities shall be conducted.

5.12 FRAUD CONTROL – SECURITY AND OTHER MEASURES

1. The Bank shall issue cards only to those customers who comply fully with KYC/AML/CFT norms stipulated by RBI from time to time.
2. The RBI guidelines on enhancing security of card transactions and all directions issued by Department of Payment and Settlement Systems from time to time shall be adhered.
3. Bank shall ensure compliance to RBI Master Direction on Digital Payment Security Controls as amended from time to time.
4. The Bank shall dispatch the card to the registered address of the customers.
5. The Bank shall be responsible for the losses incurred by party on account of breach of security or failure of the security mechanism of the bank.
6. The Bank shall keep internal records for a sufficient period of time for transactions to be traced and errors to be rectified.
7. The Bank shall send a text message/app notification to the customer's registered mobile number immediately, informing about the completed transaction (If mobile number is registered with Bank).
8. The Bank may implement its own or third party security system/mechanism for the protection of credit card of customer against fraud & security breach.

9. The Bank shall facilitate cardholder with a record of completed transaction within a reasonable period of time for transactions related to POS/ecommerce and ATMs.
10. The Bank shall provide to the cardholder the detailed procedure including a 24x7 helpline for notifying the bank with the loss, theft or unauthorised use of card or PIN.
11. Bank shall provide multiple channels such as a dedicated helpline, dedicated number for SMS, dedicated e-mail-id, Interactive Voice Response, clearly visible link on the website, internet banking and mobile-app or any other mode for reporting an unauthorized transaction on 24 x 7 basis and allow the customer to initiate the blocking of the card. The process for blocking the card, dedicated helpline as well as the SMS numbers, shall be adequately publicized and included in the billing statements.
12. Bank shall immediately send a confirmation to the cardholder subsequent to the blocking of a card.
13. The Bank shall take all actions in its power to stop further use of the card, when it is notified by customer for loss, theft or copying of the card.
14. Bank shall block a lost card immediately on being informed by the customer and formalities, if any, including lodging of FIR may follow within a reasonable period.
15. Bank may offer insurance cover to take care of the liabilities arising out of lost cards, card frauds, etc. In cases where the bank offering any insurance cover to their cardholders, in tie-up with insurance companies, the bank shall obtain explicit consent in writing or in digital mode from the cardholders along with the details of nominee/s.

6. CO-BRANDED CREDIT CARDS WITH BANKING ENTITIES:

Bank may offer credit cards to customers/non-customers under a co-branding arrangement in association with other banking entities after taking approval from the Board. In such co-branding association, the responsibility of the bank shall be limited to marketing of cards and card issuance, risk and underwriting would be managed by the partner bank.

7. INTERNAL CONTROL AND MONITORING SYSTEMS:

A comprehensive Review Report on credit card business on half-yearly basis as at the end of September and March of each accounting year may be placed to the Board/Management Committee of the Board, which shall cover essential data on credit card business, such as category and number of cards issued and outstanding, number of active cards, average turnover per card, number of establishments covered, average time taken for recovery of dues from the

card holders, debts classified as NPAs and provisions held there-against or amounts written off, details of frauds on credit cards, steps taken to recover the dues, profitability analysis of the business, etc.

Bank shall put in place a mechanism for review of their credit card operations on half-yearly basis by the Audit Committee of the Board of Directors. The review shall include, inter-alia, customer service, frauds, complaints and grievance redressal, card usage analysis including cards not used for long durations and the inherent risks therein.

Bank shall have in place a suitable monitoring mechanism to randomly check the genuineness of merchant transactions.

8. INFORMATION SYSTEM AUDIT & SECURITY

1. Bank shall be guided by RBI circulars DBS.CO.ITC.BC.No.6/31.02.008/2010-11 dated April 29, 2011, DBS.CO/CSITE/BC.11/33.01.001/2015-16 dated June 02, 2016, DCBS.CO.PCB.Cir.No.1/18.01.000/2018-19 dated October 19, 2018 (as applicable) and other relevant circulars on the subject, as amended from time to time
2. Bank shall, put in place the following framework:
    a) Application Life Cycle Security: The source code audits shall 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.
    b) Security Operations Centre (SOC): Integration of system level (server), application level logs of mobile applications with SOC for centralised and coordinated monitoring and management of security related incidents.
    c) Anti-Phishing: Subscribe 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.
    d) Risk-based Transaction Monitoring: Risk-based transaction monitoring or surveillance process shall be implemented as part of fraud risk management system.
    e) Vendor Risk Management: (i) Enter into an agreement with the service provider that amongst others provides for right of audit / inspection by the regulators of the country; (ii) RBI shall have access to all information resources (online / in

person) that are consumed by service provider, to be made accessible to RBI officials when sought, though the infrastructure / enabling resources may not physically be located in the premises of service provider; (iii) Adhere to the relevant legal and regulatory requirements relating to geographical location of infrastructure and movement of data out of borders; (iv) Review the security processes and controls being followed by service providers regularly; (v) Service agreements of bank with service provider shall include a security clause on disclosing the security breaches if any happening specific to issuer's infrastructure or process including not limited to software, application and data as part of Security incident Management standards, etc. (vi) maintain updated contact details of service providers, intermediaries, external agencies and other stakeholders for coordination in incident response. Bank shall put in place a mechanism with the stakeholders to update and verify such contact details.

f) Disaster Recovery (DR): Consider having DR facility to achieve the Recovery Time Objective (RTO) / Recovery Point Objective (RPO) for the systems 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.

g) Product Level Limits – Bank shall put in place appropriate product-level limits on the level of acceptable security risk, security objectives and performance criteria including quantitative benchmarks for evaluating the success of the security built into the card products & periodically compare actual results with projections and qualitative benchmarks to detect and address adverse trends or concerns in a timely manner and modify the business plan/ strategy involving the product, when appropriate, based on the security performance of the product or service.

h) Authentication Methodologies - Appropriate authentication methodologies shall be put in place based on an assessment of the risk posed for card based transactions. The risk shall be evaluated in light of the type of customer (e.g., retail/ corporate/ commercial); the customer transactional requirements/ pattern, the sensitivity of customer information and the volume, value of transactions involved. Customer acceptance, ease of use, reliable performance, scalability to accommodate growth, customer profile, location, transaction, etc., and

interoperability with other systems, wherever applicable shall also be taken into consideration while implementing authentication methodologies.

i) Bank shall provide information about the risks, benefits and liabilities of using card products and related services before offering them to customers. Customers shall also be informed clearly and precisely on their rights, obligations and responsibilities on matters relating to card payments, and, any problems that may arise from its service unavailability, processing errors and security breaches. The terms and conditions including customer privacy and security policy applying to card products and services shall be readily available to customers from the website. Cards shall be offered to customers on explicit request of customers and shall not be bundled without their knowledge.

j) Whenever new operating features or functions, particularly those relating to security, integrity and authentication, are introduced to cards, clear and effective communication followed by sufficient instructions to properly utilise such new features shall be provided to the customers.

k) Bank shall continuously create public awareness on the types of threats and attacks used against the consumers while using card products and precautionary measures to safeguard against the same. Customers shall be cautioned against commonly known threats in recent times like phishing, vishing, reverse-phishing, remote access of mobile devices and educated to secure and safeguard their account details, credentials, PIN, card details, devices, etc.

l) Bank shall ensure robust surveillance/ monitoring of card transactions and setting up of rules and limits. Bank shall put in place transaction limits at Card, BIN as well as at the Bank level. Such limits shall be mandatorily set at the card network switch itself. Bank shall put in place transaction control mechanisms with necessary caps (restrictions on transactions), if the above requirement is breached. A periodic review mechanism of such limits shall also be carried out. Transactions shall be monitored on 24x7 basis, including weekends, long holidays.

m) Bank shall ensure that card details of the customers are not stored in plain text at the bank and its vendor(s) locations, systems and applications. Bank shall also ensure that the processing of card details in readable format is performed in a secure manner to strictly avoid data leakage of sensitive customer information.

9. REPORTING:

1. Central Processing Centre, BOG shall provide/generate sufficient reports for the daily monitoring and operations. In addition to this, Retail Banking Department shall submit report to Board or Board committee or Executive committee designated by board for review on half yearly or as needed basis.
2. The Bank shall submit report on card business to Department of Payment Settlement Systems (DPSS) on monthly basis or as instructed by Reserve Bank of India.

10. SAFEGUARDS AGAINST MONEY LAUNDERING PROVISIONS

1. Bank shall adhere to the Know Your Customer (KYC) / Anti-Money Laundering (AML) / Combating Financing of Terrorism (CFT) guidelines issued by the Department of Regulation (DoR), RBI, in "Master Direction – Know Your Customer Direction, 2016", as updated from time to time.
2. Bank shall adhere to the Provisions of Prevention of Money Laundering Act, 2002 (PMLA) and Rules framed thereunder, as amended from time to time.
3. Bank shall maintain a log of all the transactions undertaken using cards 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. Bank shall also file Suspicious Transaction Reports (STRs) to Financial Intelligence Unit-India (FIU-IND).

11. REVIEW

The credit card business policy shall be reviewed on a yearly basis. The bank shall put in place adherence and monitoring mechanism with Best practices in industry towards risk mitigation and security measures.

PART B

Debit & Prepaid Cards Business Policy

For

Version Number: 2.1

Dated: 26th September 2024

TABLE OF CONTENTS

1. DOCUMENT UPDATE HISTORY

Version No	Date	Department
1.0	DBR/MKG/S-125/13-14 DATED 13-08-2013	Marketing
1.1	DBR/MKG/S-253/13-14 DATED 01-02-2014	Marketing
1.2	DBR/MKG/S-254/14-15 DATED 24-02-2015	Marketing
1.3	DBR/MKG/S-327/15-16 DATED 29-03-2016	Marketing
1.4	DBR/MKG/S-280/16-17 DATED 15-03-2017	Marketing
1.5	DBR/RBD/S-29/2018-19 DATED 14-05-2018	RBD
1.6	DBR/RBD/S-334/2018-19 DATED 26-03-2019	RBD
1.7	DBR/RBD/S-65/2020-21 DATED 29-04-2020	RBD
1.8	DBR/RBD/S-157/2021-22 DATED 18-08-2021	RBD
1.9	DBR/RBD/S-43/2022-23 DATED 07-06-2022	RBD
2.0	DBR/RBD/S-158 /2023-24 DATED 24.08.2023	RBD

2. BACKGROUND:

South Indian Bank started its card business in late 1990s with "Insta cash" offline debit cards which were issued to selected customers. In 2002, issuance of offline debit cards was discontinued on starting issuance of Online ATM cards. Subsequently, arrangements were made with MasterCard International, National Financial Switch (NFS), VISA International and National Payments Corporation of India (NPCI) for increasing the acceptability of our debit cards at ATMs/POS terminals worldwide and online websites. At present, South Indian Bank's card business comprises of EMV Chip Debit Cards, Contactless Debit Cards, Co-branded Contactless Chip Debit Cards, Contactless Debit cum Prepaid cards (National Common Mobility Card) supporting mobility payments, Virtual debit cards, multi-currency Contactless Chip Travel cards, Contactless Prepaid Gift Cards, Reloadable General purpose Prepaid Contactless Cards and Tap & Pay Form Factor (RuPay on The Go wearable KeyFob) . In future, bank may permit card less cash withdrawal.

3. GENERAL OBJECTIVE:

In the light of RBI Guidelines on card business, policy for debit card & prepaid card business is formulated. The policy has been framed within the ambit of Payment and Settlement System Act 2007. The objective of this document is to define the policy under which the bank offers card services to customers of the bank. Another objective is to establish roles & responsibilities for the bank's Debit Card Cell & Prepaid Card Cell keeping in mind the key aspects which are listed below:

- Addressing the risk involved in card issuance business and necessary risk mitigation measures.
- To ensure adherence of KYC/AML/CFT norms specified by RBI with respect to card business from time to time.
- For standardization of card issuance procedure among the branches.
- Increased competition from other banks and non banking financial companies.
- Growing demand from customers.
- Increased efficiency by offering a cost effective delivery channel for banking services.
- 24x7 Service availability.
- Anywhere banking option for customers.
- Security issues related to card issuance business.

- Grievance mechanism policy

4. DEBIT CARD

Debit Card is a physical or virtual payment instrument containing a means of identification, linked to a Saving Bank/Current Account which can be used to withdraw cash, make online payments, do PoS terminal/Quick Response (QR) code transactions, fund transfer, etc. subject to prescribed terms and conditions.

4.1 TERMS & CONDITIONS:

1. The Bank shall issue cards only to customers who fully comply with KYC/AML/CFT norms stipulated by RBI from time to time.
2. The Bank shall issue debit cards in all types of eligible Savings Bank Accounts, accounts of Society, Trusts, Foundations, Associations & Clubs, Charitable Institutions, Groups Current Accounts (Proprietorship, Partnership firms, Limited Liability Partnerships, One Person Company, Limited company and Private Non- financial corporation only) and Hindu Undivided Family. No debit cards shall be issued in cash credit/loan accounts, Staff OD, OD against Deposit. However, overdraft facility provided along with Pradhan Mantri Jan Dhan Yojana accounts or Kissan Credit card accounts can be linked with a debit card.

3. Bank may 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 the banks as lenders. As overdraft facility is a loan account an electronic card issued therein has been named as a type of credit card. These cards shall be issued as per the underlying terms and conditions associated with such loan facility.

4. Banks shall not force a customer to avail debit card facility and shall not link issuance of debit card to availment of any other facility from the bank.

5. For cards issued after 01.05.2020, in accounts with Mode of Operation as Self/Single, maximum Three LIVE cards will be permitted at any point of time. In accounts with mode of operation as Either or Survivor/Jointly, maximum of Three main and Three add-on cards shall be permitted for issuance. In accounts with mode of operation as anyone, maximum of one main card & four add-on cards shall be permitted by default. AGM & Above- of the Debit Card Product Owner Department will have to authority to sanction exceptions in the number of cards.

6. The issue of debit cards as a payment mechanism would be subject to relevant guidelines including guidelines on security issues and risk mitigation measures, card-to-card fund transfers, merchant discount rates structure, failed ATM transactions, etc, issued by the Department of Payment and Settlement Systems of RBI under the Payment and Settlement Systems Act, 2007, as amended from time to time.
7. Generally debit cards issued/reissued by the Bank (physical and virtual) shall be enabled for use only at contact based points of usage [viz. ATMs and Point of Sale (PoS) devices] within India. Bank shall provide debit cardholders a facility for enabling card not present (domestic and international) transactions, card present (international) transactions and contactless transactions, as per the process outlined in para 8 below. The card issuance shall also be subject to directions issued under FEMA 1999 as amended from time to time and Reserve Bank of India guidelines (RBI Instructions in this regard shall be adhered)
8. Additionally, bank shall provide to all debit cardholders:
   - facility to switch on / off and set / modify transaction limits (within the overall card limit, if any, set by the issuer) for all types of transactions – domestic and international, at PoS / ATMs / online transactions / contactless transactions, etc.
   - the above facility on a 24x7 basis through multiple channels - mobile application / internet banking / ATMs / Interactive Voice Response (IVR); this may also be offered at branches / offices;
9. Alerts / information / status, etc., through SMS / e-mail, as and when there is any change in status of the card. The Bank shall not dispatch a card to customer unsolicited, except in the case where the card is replacement for a card already held by the customer.
10. The relationship between the Bank and the card holder shall be contractual.
11. The Bank shall make available to the cardholders in writing, a set of contractual terms and conditions governing the issue and use of such a card.
12. The Bank shall put the cardholder under an obligation to take all appropriate steps to keep safe the card and the means (such as PIN, CVV, Expiry Date or One Time Password) which enable it to be used.
13. The Bank shall put the cardholder under an obligation not to record the PIN or OTP, in any form that would be intelligible or otherwise accessible to any third party if access is gained to such a record, either honestly or dishonestly.
14. Bank shall ask its customers to mandatorily register for SMS alerts and wherever available register for e-mail alerts, for electronic banking transactions. The SMS alerts shall

mandatorily be sent to the customers, while email alerts may be sent, wherever registered. The name of the Merchant where transaction is being carried out shall be part of the message wherever made available by the acquirer.

15. The customers shall be advised to notify their bank of any unauthorised electronic banking transaction at the earliest after the occurrence of such transaction, and informed that, the longer the time taken to notify the bank, the higher will be the risk of loss to the bank/ customer. To facilitate this, bank shall provide customers with 24x7 access through multiple channels (at a minimum, via website, phone banking, SMS, e-mail, IVR, a dedicated toll-free helpline, reporting to home branch, etc.) for reporting unauthorised transactions that have taken place and/ or loss or theft of payment instrument such as card, etc.
16. Bank shall also enable customers to instantly respond by "Reply" to the SMS and e-mail alerts and the customers should not be required to search for a web page or an e-mail address to notify the objection, if any. Further, a direct link for lodging the complaints, with specific option to report unauthorised electronic transactions shall be provided by bank on the home page of their website.
17. The loss/ fraud reporting system shall also ensure that immediate response (including auto response) is sent to the customers acknowledging the complaint along with the registered complaint number. The communication systems used by bank to send alerts and receive their responses shall record the time and date of delivery of the message and receipt of customer's response, if any, to them. This shall be important in determining the extent of a customer's liability.
18. The bank shall not offer facility of electronic transactions, other than ATM cash withdrawals, to customers who do not provide mobile numbers to the bank. On receipt of report of an unauthorised transaction from the customer, bank shall take immediate steps to prevent further unauthorised transactions in the account.
19. Related clause shall form an integral part of the terms & conditions. This is in line with RBI circular on Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions.
20. The Bank shall exercise care when issuing PINs or OTP and shall be under an obligation not to disclose the cardholder's PIN or OTP, except to the cardholders.
21. The Additional Factor of (AFA) requirements for Cards shall be mandatory for domestic transactions.

22. Debit card shall be blocked for usage after multiple incorrect entries of the Additional Factor of authentication (PIN/OTP)
23. Limited Liability of a Customer.

a. Zero Liability of a Customer

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

i. Contributory fraud/ negligence/ deficiency on the part of the bank (irrespective of whether or not the transaction is reported by the customer).

ii. Third party breach where the deficiency lies neither with the bank nor with the customer but lies elsewhere in the system, and the customer notifies the bank within three working days of receiving the communication from the bank regarding the unauthorised transaction.

b. Limited Liability of a Customer

A customer shall be liable for the loss occurring due to unauthorised transactions in the following cases:

i. In cases where the loss is due to negligence by a customer, such as where he has shared the payment credentials, the customer will bear the entire loss until he reports the unauthorised transaction to the bank. Any loss occurring after the reporting of the unauthorised transaction shall be borne by the bank.

ii. ii. In cases where the responsibility for the unauthorised electronic banking transaction lies neither with the bank nor with the customer, but lies elsewhere in the system and when there is a delay (of four to seven working days after receiving the communication from the bank) on the part of the customer in notifying the bank of such a transaction, the per transaction liability of the customer shall be limited to the transaction value or the amount mentioned in Table 1, whichever is lower.

Table 1

Maximum Liability of a Customer under paragraph 13 (b) (ii)

• Type of Account	Maximum Liability
• BSBD Accounts	5,000

• All other SB accounts • Pre-paid Payment Instruments and Gift Cards • Current/ Cash Credit/ Overdraft Accounts of MSMEs • Current Accounts/ Cash Credit/ Overdraft Accounts of Individuals with annual average balance (during 365 days preceding the incidence of fraud)/ limit up to Rs.25 lakh • Credit cards with limit up to Rs.5 lakh	10,000
• All other Current/ Cash Credit/ Overdraft Accounts • Credit cards with limit above Rs.5 lakh	25,000

24. Further, if the delay in reporting is beyond seven working days, the customer liability shall be determined as per the bank's Board approved policy. Bank shall provide the details of the policy in regard to customers' liability formulated in pursuance of these directions at the time of opening the accounts. Bank shall also display the approved policy in public domain for wider dissemination. The existing customers shall also be individually informed about the bank's policy.

25. Overall liability of the customer in third party breaches, as detailed in paragraph 23 (a) (ii) and paragraph 23 (b) (ii) above, where the deficiency lies neither with the bank nor with the customer but lies elsewhere in the system, is summarised in the Table below:

Table 2

Time taken to report the fraudulent transaction from the date of receiving the communication	**Customer's liability (₹)**
Within 3 working days	Zero liability

Within 4 to 7 working days	The transaction value or the amount mentioned in Table 1, whichever is lower
Beyond 7 working days	As per bank's Board approved policy

26. Bank may enable cash withdrawal facility for debit and prepaid cards at Point of Sale terminals
27. The Bank may charge the customer for issuance & usage of debit cards. The charge shall be made known to the customers. Executive Director of the bank shall be the authority to fix/revise the charges and also shall have full power to add or remove any charges.
28. Executive Director is vested with the power to approve any feature additions and new products in debit card portfolio.
29. Process and Procedure related changes of cards and changes in the transaction limits shall be placed to PPAC for approval.
32. Bank shall not levy any charge that was not explicitly indicated to the cardholder at the time of issuance of the card and without getting the explicit consent. However, this will not be applicable to charges like service taxes which may subsequently be levied by the Government or any other statutory authority. The details of all the charges associated with cards shall be displayed on the bank website31. The Bank may alter the terms, but 30 days' notice of the change shall be given to the cardholder to enable him/her to withdraw if he/she chooses. After the notice period of 30 days, the cardholder would be deemed to have accepted the terms if he had not withdrawn during the specified period. The changes in terms shall be notified to the cardholder through all the communication channels available. This is in compliance with the terms of BCSBI (Banking Codes and Standards Board of India) code, accepted by the bank. The Bank will not reveal any information relating to customers obtained at the time of opening the account or issuing the card to any other person or organization without obtaining their explicit consent, with regard to the purpose/s for which the information will be used and the organizations with whom the information shall be shared. Further in cases where the customers give explicit consent for sharing the information with other agencies, bank will explicitly state and explain clearly to the customer the full meaning/implications of the disclosure clause. Bank will be solely responsible for the correctness or otherwise of the data provided for the purpose.
33. Bank shall not share card data (including transaction data) of the cardholders with the outsourcing partners unless sharing of such data is essential to discharge the functions

assigned to the latter. In case of sharing of any data as stated above, explicit consent from the cardholder shall be obtained. The storage and the ownership of card data remains with the Bank.

34. The Bank shall specify the period within which the cardholder's account would normally be debited.

4.2 SERVICES OFFERED THROUGH DEBIT CARD:

The following services are offered to the customers through debit card:

1. Available balance in the accounts linked to the card can be checked using balance enquiry option through ATMs.
2. Cash withdrawal can be made for the accounts linked to the card using Withdrawal and Fast Cash options available in ATMs. Cash withdrawal at Point of Sale (POS) may be enabled.
3. Last few transaction details (currently 9 transactions) can be obtained using the Mini statement option available in ATMs (Available in all NFS linked ATMs).
4. Fund transfer between the accounts linked to a card is possible through Fund Transfer option available in ATMs (Only in SIB ATMs).
5. Cheque book can be requested using cheque book request option in ATMs (Only in SIB ATMs).
6. ATM PIN can be changed by the customer using PIN Change option available in ATMs (Available in all NFS linked ATMs).
7. Mini statement and Pin change option is made available in our ATMs for other bank customers through NFS.
8. Debit cards are enabled for purchase transactions at POS terminals.
9. Debit cards are enabled for online transactions.
10. 'Cash Remittance' facility using SIB ATM cum debit cards is available to customers through cash deposit machines [CDM] and cash recycler machines [CRMs] installed by South Indian Bank or Other banks through the Interoperable Cash Deposit facility offered by NPCI.
11. Debit cards can be used for registration of NACH e-mandates and also used to schedule recurring transactions in their account as permitted by RBI.

12. ATM PIN can be self created/reset by the customers through GREEN PIN facility available across all South Indian Bank ATMs, SIB Mirror+ App & SIBerNet.
13. Inter-operable Mobile Banking Registration and Aadhar Seeding facility is also enabled at our ATMs through NPCI/NFS.
14. SIBerNet and SIB Mirror+ password reset using Debit Card credentials.
15. Contactless Debit cum Prepaid cards (National Common Mobility Card NCMC) enables customers to use the card as transit cards by making payments across all segments including metro, bus, suburban etc
16. Form Factor is the physical or virtual instrument that can be used in place of a debit card to undertake a payment/banking transaction. Contactless payment upto Rs 5000 without PIN and contactless transactions upto Rs 1,00,000 can be done with PIN.
17. South Indian Bank Offers Remittance Cards, which are used for the purpose of remitting cash into the card linked account at Cash Remittance Machines of South Indian Bank. Through the card, a maximum of Rs.5, 00,000 per day can be remitted to the account if PAN is updated in the account.
18. Interoperable Cash Deposit is a unique feature provided by National Payments Corporation of India, which enables customers of participating Member banks to deposit Cash in other Bank Cash Remittance Machines, thereby providing inter-bank operations in cash remittances at CRMs.

4.3 RESPONSIBILITY:

1. The ownership of the Debit card business of the bank shall remain with Retail Banking Department and persons handling the related work should have the complete working knowledge and understanding of operational elements of debit cards. However, the daily processing of cards and REPIN requests of customers shall be handled by Central Processing Centre, Banking Operations Group (BOG).

2. The overview, implementation and compliance of new services related to card business shall be the responsibility of Retail Banking Department in co-ordination with DTD, Compliance, Legal, IRMD and other divisions of the Bank.

3. Central processing Centre, BOG shall dispatch cards to branches or to customers as per the policy approved by the Product Apex Systems & Procedures Committee of the Bank from time to time. ATM Pin mailers shall be dispatched to branches only. Customers shall also be given

an option to create their own PIN through GREEN PIN facility available across SIB ATMs, SIB Mirror+ App & SIBerNet. In the case of debit cards, Welcome Kits dispatched to branches, branches shall be responsible for the safe custody and delivery of cards/ATM pin mailers to customers. In the case of debit cards dispatched to customers, if paper PIN is opted, branches shall be responsible for delivery of corresponding PIN mailer after identifying the customer.

4. Periodic reviews shall be conducted to identify the effectiveness of the debit card services offered to customers by the bank and also to suggest for improvements wherever required.

4.4 OPERATIONAL ELEMENTS:

The Debit Card Cell shall share responsibility for operational elements of card business along with the other departments of the Bank. The Product Procedures Apex Committee [PPAC] of the Bank represents each major department of the Bank and this committee has the primary responsibility for decision making on new services of card business. The following operational elements should be considered prior to adding new debit card product/service.

1. **Planning and Deployment:** The development of any new debit card product/service shall encompass proper due diligence. Related hardware, software, obsolescence, support and other similar issues should be carefully evaluated.
2. **Marketing and Promotion:** Retail Banking Department shall conduct market survey and new services shall be introduced with the help of DTD. Bank shall promote debit card usage at POS/Online by conducting various campaigns and by awarding gifts/cash back/reward points to customers based on card usage on its own or through an outsourced agency.
3. **Audit and Monitoring:** Audit and regulatory compliance risks shall be carefully evaluated and identified prior to implementation as well as on an ongoing basis.
4. **Vendors and Outsourcing:** In addition to own resources, the Bank may rely on third parties to provide debit card product/services. Third party selection may be based on the Information Security policy established already by the Bank. Risk Management of the outsourced technology services which should also consider the third party's ability to provide the product/services from a standpoint of internal controls, security, maintenance & upkeep of the system and financial condition.
5. **Legal and Regulatory:** Debit card products & services should be evaluated on for legal and regulatory issues. Privacy issues should be addressed prior to introducing a product.

6. **Reconciliation:** Banking Operations Department [BOG] in co-ordination with Corporate Financial Management (CFM) department shall be responsible for reconciliation of transactions using debit cards and prepaid cards including Fastag.

7. **Disaster Recovery and Contingency Plans:** Existing disaster recovery and contingency plans shall address debit card services. Plans should include the restoration of debit card services in the event of disaster. DTD & BOG shall have a system in place for storage of data related to debit cards and restoration of debit card services in the normal as well as in an event of disaster.

4.5 SECURITY & FRAUD PREVENTION SYSTEMS:

1. The Bank shall issue cards only to those customers who comply fully with KYC/AML/CFT norms stipulated by RBI from time to time.

2. The Bank shall dispatch the card to branches or to customers as per the policy approved by the Product Procedures Apex Committee [PPAC] of the Bank from time to time. ATM PIN mailers shall be dispatched separately to branches as per policy approved by the PPAC. Also, the customers shall be given an option to create their own PIN through the Green PIN facility available at all SIB ATMs, SIB Mirror+ app & SIBerNet.

3. The branch shall keep the card/Pin mailer safe & secure as per the guidelines provided to them by debit card cell.

4. The Bank shall be responsible for the losses incurred by party on account of breach of security or failure of the security mechanism of the bank.

5. The Bank shall keep internal records for a sufficient period of time for transactions to be traced and errors to be rectified.

6. The Bank shall send a text message to the customer's registered mobile number immediately, informing about the completed transaction (If mobile number is registered with Bank).

7. The Bank may implement its own or third party security system/mechanism for the protection of debit card of customer against fraud & security breach.

8. The Bank shall facilitate cardholder with a record of completed transaction within a reasonable period of time for transactions related to Online, POS &ATMs.

9. The Bank shall provide a 24x7 helpline to customers for notifying the bank with a loss, theft or copying of the card.

10. The Bank shall take all actions in its power to stop further use of the card, when it is notified by customer for loss, theft or copying of the card.

11. The cardholder will be provided with a record of the transactions after he/she has completed it, immediately in the form of receipt or another form such as the bank statement/email/SMS.

12. In case Bank, at their discretion, decide to block/deactivate/suspend a debit card, bank shall ensure necessary customer communications to eliminate customer inconvenience. Presently this is undertaken in instances of identified fraud, instances of card compromises reported by network or regulator & as part of network compliances. The operating procedure on the above scenarios will be included in the Standard Operating Procedure [SOP] for Debit cards.

13. Bank shall block a lost card immediately on being informed by the cardholder after due validations and formalities, if any, can follow within a reasonable period.

14. Bank will be providing cardholder the detailed procedure to report the loss, theft or unauthorised use of card or PIN. Bank will provide multiple channels such as a dedicated helpline, dedicated number for SMS, dedicated e-mail-id, IVR, clearly visible link on the website, internet banking and mobile-app or any other mode for reporting an unauthorized transaction on 24 x 7 basis and allow the customer to initiate the blocking of the card. The process for blocking the card, dedicated helpline as well as the SMS numbers, shall be adequately publicized and included in the billing statements.

15. Bank will immediately send a confirmation to the cardholder subsequent to the blocking of a card.

16. No card-issuer shall dispatch a card to a customer unsolicited. In case of renewal of an existing card, the cardholder shall be provided an option to decline the same if he/she wants to do so before dispatching the renewed card. Further, in case a card is blocked at the request of the cardholder, replacement card in lieu of the blocked card shall be issued with the explicit consent of the cardholder.

17. In case of an insurance cover provided with a card, bank will ensure that the relevant nomination details are recorded by the Insurance Company and the availability of insurance is included, along with other information, in every statement. The information shall also

include the details regarding the insurance cover, name/address and telephone number of the Insurance Company which will handle the claims relating to the insurance cover.

5. CO-BRANDED DEBIT CARDS:

Bank may issue co-branded debit cards in association with a co-branding partner and prior approval of RBI is not necessary for the issuance of Co-Branded Debit cards. All compliance points with respect to debit cards should be applicable to co-branded debit cards also. In addition to it, the following points are also to be complied:

1. The co-branded debit cards shall be issued only to the customers of the bank.
2. Prior to entering into tie up with a co-branding partner, the bank has to pertain about various risks associated with co-branding with a co-branding partner and the necessary risk mitigation measures needed, such entities should be KYC complied.
3. The Bank shall carry out due diligence in respect of the co-branding partner with which they intend to enter into tie-up for the issue of such cards. If the co-branding partner is a financial entity, necessary approvals from its regulator has to be obtained for entering into the co-branding arrangement
4. The Bank shall follow the guidelines of RBI on "Managing Risks and Code of conduct in outsourcing of financial services by banks" as amended from time to time. Bank shall ensure that cash backs, discounts and other offers advertised by a co-branding partner are delivered to the cardholder on time. Bank shall be liable for any delay or non-delivery of the same to the cardholders.
5. The Bank shall not disclose any information relating to customers obtained at the time of account opening or while issuing the card.
6. The Bank shall limit the role of co-branding partner in co-branding arrangement only to the extent of marketing & distribution of cards and providing access to the cardholder for the goods/services that are offered.
7. The co-branding partner shall not have access to information relating to transactions undertaken through the co-branded card. Post issuance of the card, the co-branding partner shall not be involved in any of the processes or the controls relating to the co-branded card except for being the initial point of contact in case of grievances.
8. The co-branding partner shall be prohibited from the access to customer's account details that may violate bank's secrecy obligations.

9. The co-branded debit card shall explicitly indicate that the card has been issued under a co-branding arrangement. The co-branding partner shall not advertise/market the co-branded card as its own product. In all marketing/advertising material, the name of the bank shall be clearly shown.
10. The co-branded card shall prominently bear the branding of the bank
11. The co-branding partner shall not be involved in any other process and shall not have access to the transaction data. However for the purpose of customer convenience, card transaction related data may be drawn directly from the card-issuer's system in an encrypted form and displayed in the CBP platform with robust security. The information displayed through the CBP's platform to the card holder neither be visible nor be accessible to the CBP and it should be a direct link to the card issuers system.
12. The information relating to revenue sharing between the bank and the co-branding partner entity shall be indicated to the cardholder and also displayed on the website of the bank.
13. The information relating to revenue sharing between the bank and the co-branding partner entity shall be indicated to the cardholder and also displayed on the website of the bank.
14. Head of Product Owner Department shall approve of any co-branding arrangement with institutions who are customers of South Indian Bank

6. PREPAID CARDS:

Prepaid instruments are instruments that facilitate purchase of goods and services, financial services, remittance facilities, etc., against the value stored therein. The Bank shall issue prepaid instruments after receiving prior approval from the Reserve Bank of India. Bank shall further enter into co-branding arrangements with other entities as permitted by RBI for issuance of Pre-paid instruments after taking approval from MD & CEO.

6.1 Categories of prepaid payment instruments:

As per RBI guidelines, the prepaid payment instruments issued by the Bank are classified under two categories viz.,

(i) Small PPIs, and (ii) Full-KYC PPIs

i. **Small PPIs** shall be issued after obtaining minimum details of the PPI holder. They shall be used only for purchase of goods and services. Funds transfer or cash withdrawal from such PPIs shall not be permitted. Small PPIs can be used at a group of clearly identified merchant locations / establishments which have a specific contract with the issuer (or contract through a payment aggregator / payment gateway) to accept the PPIs as payment instruments.

ii. **Full-KYC PPIs** shall be issued after completing Know Your Customer (KYC) of the PPI holder. These PPIs shall be used for purchase of goods and services, funds transfer or cash withdrawal.

6.2 Issuance, loading and reloading of PPIs

6.2.1 Bank shall issue reloadable or non-reloadable PPIs depending upon the permissible type / category of PPIs as laid down in RBI Master Direction on issuance of Prepaid instruments as amended from Time to time..

6.2.2 Bank's Prepaid Instrument issuance & operations shall be governed by this policy.

6.2.3 Bank shall ensure that its name is prominently displayed along with the PPI brand name (if any) in all instances. Bank shall also keep RBI informed in case any brand names employed / to be employed for its Prepaid products.

6.2.4 Bank shall not pay any interest on PPI balances.

6.2.5 Bank shall permit loading / reloading of PPIs by cash, debit to a bank account, credit and debit cards, PPIs (as permitted from time to time) and other payment instruments issued by regulated entities in India and shall be in INR only.

6.2.6 Cash loading to PPIs shall be limited to Rs.50,000/- per month subject to overall limit of the PPI.

6.2.7 PPIs shall be issued as cards, wallets, and in any such form / instrument which can be used to access the PPI and to use the amount therein. No PPI shall be issued in the form of paper vouchers.

6.2.8 Bank shall be load / reload PPIs through BCs subject to compliance with BC guidelines issued by RBI.

6.2.9 Bank shall load / reload PPIs through authorised outlets or through authorised / designated agents subject to the below framework:

a) Carrying out proper due diligence of the persons appointed as authorised / designated agents;

b) Bank shall be responsible as the principal for all acts of omission or commission of the authorised / designated agents, including safety and security aspects;

c) Preserving records and confidentiality of customer information with the bank as well as in the possession of the authorised / designated agents;

d) Monitoring regularly the activities of the authorised / designated agents and carrying out review of the performance of various agents engaged at least once in a year; and

e) Ensuring adherence to applicable laws of the land, including KYC / AML / CFT guidelines.

6.2.10 Bank shall ensure that there is no co-mingling of funds originating from any other activity that bank undertakes such as BC of bank/s, intermediary for payment aggregation, payment gateway, etc.

6.3 PPIS UNDER CO-BRANDING ARRANGEMENTS

a) MD & CEO shall be vested with the authority to approve any co-branding arrangement for prepaid instruments. Various risks including reputation risk shall be considered and necessary risk mitigation measures shall be put in place before entering into any such arrangements. Further, such co-branding arrangements shall be based on co-branding partnership agreements clearly defining the roles, responsibilities and obligations of each co-branding partner.

b) The co-branding partner shall be a company incorporated in India under the Companies Act, 1956 / 2013. The co-branding partner can also be a Government department / ministry. In case the co-branding partner is a bank, the same shall be licensed by RBI.

c) Bank shall carry out due diligence of the co-branding partner to protect against the reputation risk. In case of tie up with a financial entity, it may ensure that approval of co-branding partner's regulator for entering into such arrangement is available.

d) Instructions / Guidelines on KYC / AML / CFT shall be adhered to in respect of all PPIs issued under the co-branding arrangement.

e) Bank shall be liable for all acts of the co-branding partner. The bank shall also be responsible for all customer-related aspects of the PPIs.

f) Bank may co-brand instruments with the name / logo of the company for whose customers / beneficiaries such co-branded instruments are to be issued.

g) The name of bank shall be prominently visible on the payment instrument.

h) In case of co-branding arrangements between bank and non-bank entity, bank shall be the PPI issuer. Role of the non-bank entity shall be limited to marketing / distribution of the PPIs or providing access to the PPI holder to services that are offered.

i) In case of co-branding arrangements between two banks, the PPI issuing bank shall ensure compliance to above instructions

j) Bank shall adhere to instructions contained in circularDBR.No.FSD.BC.18/24.01.009/2015-16 dated July 1, 2015, as amended from time to time.

6.4 There shall be no remittance without compliance to KYC requirements. Bank or Bank's agent/s, shall not create new PPIs every time for facilitating cash-based remittances to other PPIs / bank accounts. PPIs created for previous remittance by the same person shall be used.

6.5 TYPES OF PPIs

6.5.1 Small PPIs (or Minimum-detail PPIs)

(i) PPIs upto Rs.10,000/- (with cash loading facility)

a) Bank shall issue such PPIs after obtaining minimum details of the PPI holder;

b) Minimum details shall necessarily include a mobile number verified with One Time Password (OTP) and a self-declaration of name and unique identity / identification number of any 'mandatory document' or 'Officially Valid Document (OVD)' or any such document with any name listed for this purpose in the Master Direction on KYC, as amended from time to time;

c) Such PPIs shall be reloadable in nature;

d) 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/-;

e) Amount outstanding at any point of time in such PPIs shall not exceed Rs.10,000/-;

f) Total amount debited from such PPIs during any month shall not exceed Rs.10,000/;

g) These PPIs shall be used only for purchase of goods and services. Cash withdrawal or funds transfer from such PPIs shall not be permitted;

h) There shall be no separate limit for purchase of goods and services using PPIs;

i) These PPIs shall be converted into full-KYC PPIs within a period of 24 months from the date of issue of the 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;

j) This category of PPI shall not be issued to the same user in future using the same mobile number and same minimum details;

k) Bank shall give an option to close the PPI at any time. The closure proceeds can be transferred 'back to source account' (payment source from where the PPI was loaded). Alternatively, the closure proceeds can be transferred to a bank account after complying with KYC requirements of PPI holder; and

l) The features of such PPIs shall be clearly communicated to the PPI holder by SMS / e-mail / any other means at the time of issuance of the PPI / before the first loading of funds.

(ii) PPIs upto Rs.10,000/- (with no cash loading facility)

a) Bank shall issue such PPIs after obtaining minimum details of the PPI holder;

b) Minimum details shall necessarily include a mobile number verified with OTP and a self-declaration of name and unique identity / identification number of any 'mandatory document' or OVD or any such document with any name listed for this purpose in the Master Direction on KYC, as amended from time to time;

c) Such PPIs shall be reloadable in nature. Loading / Reloading shall be from a bank account / credit card / full-KYC PPI;

d) 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;

e) The amount outstanding at any point of time in such PPIs shall not exceed Rs.10,000;

f) These PPIs shall be used only for purchase of goods and services. Cash withdrawal or funds transfer from such PPIs shall not be permitted;

g) Bank shall give an option to close the PPI at any time. The closure proceeds can be transferred 'back to source account' (payment source from where the PPI was loaded). Alternatively, the closure proceeds can be transferred to a bank account after complying with KYC requirements of PPI holder;

h) The features of such PPIs shall be clearly communicated to the PPI holder by SMS / e-mail / any other means at the time of issuance of the PPI / before the first loading of funds;

6.5.2 FULL-KYC PPIs

a) Bank shall issue such PPIs after completing KYC of the PPI holder

b) The Video-based Customer Identification Process (V-CIP), as detailed in RBI's Master Direction on KYC dated February 25, 2016 (as amended from time to time), can be used to open full-KYC PPIs as well as to convert Small PPIs into full-KYC PPIs;

c) Such PPIs shall be reloadable in nature;

d) The amount outstanding shall not exceed Rs.2,00,000/- at any point of time;

e) The funds can be transferred 'back to source account' (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 the limits considering the risk profile of the PPI holders, other operational risks, etc. The same shall be approved by Head – Liabilities.

f) Bank shall provide the facility of 'pre-registered beneficiaries' whereby the PPI holder can register the beneficiaries by providing their bank account details, details of PPIs issued by same issuer (or different issuer as and when permitted), etc.;

g) In case of such pre-registered beneficiaries, the funds transfer limit shall not exceed Rs.2,00,000/- per month per beneficiary.

h) Funds transfer limits for all other cases shall be restricted to Rs.10,000/- per month;

i) Funds transfer from such PPIs shall also be permitted to other PPIs, debit cards and credit cards as per the limits given above;

j) There is no separate limit on purchase of goods and services using PPIs;

k) Bank shall indicate the limits to the PPI holders and provide necessary options to PPI holders to set their own fund transfer limits;

l) Bank shall also give an option to close the PPI and transfer the balance as per the applicable limits of this type of PPI. For this purpose, the issuer shall provide an option, including at the time of issuing the PPI, to the holder to provide details of pre-designated bank account or other PPIs of the bank (or other banks/issuers as and when permitted) to which the balance amount available in the PPI shall be transferred in the event of closure of PPI, expiry of validity period of such PPIs, etc.;

m) In case of bank's PPIs, cash withdrawal shall be permitted. However, cash withdrawal at PoS devices shall be subjected to a limit of Rs.2,000/- per transaction within an overall monthly limit of Rs.10,000/- across all locations (Tier 1 to 6 centres), subject to conditions stipulated in RBI circular DPSS.CO.PD.No.449/02.14.003/2015-16 dated August 27, 2015;

n) Features of such PPIs shall be clearly communicated to the PPI holder by SMS / e-mail / any other means at the time of issuance of the PPI / before the first loading of funds.

6.6 SPECIFIC CATEGORIES OF PPIS

Bank shall not issue PPIs of any other category except as permitted under the following categories:

6.6.1 Gift PPIs

a) Maximum value of each such prepaid gift instrument shall not exceed Rs.10,000/-;

b) Such instrument shall not be reloadable;

c) Cash-out or funds transfer shall not be permitted for such instrument. However, the funds may be transferred 'back to source account' (account from where Gift PPI was loaded) after receiving consent of the PPI holder;

d) KYC details of the purchaser of such instrument shall be maintained by the bank. Separate KYC shall not be required for customers who are issued such instrument against debit to their KYC complied bank accounts and / or credit cards in India;

e) Bank shall adopt a risk-based approach, in deciding number of such instruments which can be issued to a customer. By default, a retail customer can be issued maximum of 20 Gift cards in a Financial Year. The authority to increase the number of cards permitted per customer shall be vested with Head Product Owner Department. In the case of corporate customers, no such restrictions on the number of cards permitted for issuance may be stipulated.

f) PPIs shall be revalidated (including through issuance of new instrument) as and when requested by the PPI holder;

g) Provisions on validity and redemption, as applicable for Prepaid instruments, shall be adhered to; and

h) Features of PPIs shall be clearly communicated to the PPI holder by SMS / e-mail / any other means at the time of issuance of the PPI / before the first loading of funds.

6.6.2 PPIS FOR MASS TRANSIT SYSTEMS (PPI-MTS)

a) Banks are permitted to issue such PPIs

b) Such PPIs shall contain the Automated Fare Collection application related to transit services, toll collection and parking.

c) Such PPIs shall be enabled only for payments across various modes of public transport such as metro, buses, rail, & waterways, tolls and parking;

d) These PPIs can be issued without KYC verification of the holders

e) These PPI can be reloadable in nature;

f) The amount outstanding, in such PPIs shall not exceed Rs. 3,000/- at any point of time.

g) These PPIs can have perpetual validity, i.e., the provisions of validity and redemption given in the clause no 6.10 of this policy shall not apply to PPI-MTS.

h) Cash-withdrawal, refund or funds transfer shall not be permitted in such PPIs.

6.6.3 PPIS TO FOREIGN NATIONALS / NON-RESIDENT INDIANS (NRIS) VISITING INDIA

a. Bank is permitted to issue PPIs in INR denominated full-KYC PPIs to foreign nationals / NRIs visiting India (to start with, this facility will be extended to travellers from the G-20 countries, arriving at select international airports). Such PPIs can also be issued in co-branding arrangement with entities authorised to deal in Foreign Exchange under FEMA;

b. The PPIs shall be issued after physical verification of Passport and Visa of the customers at the point of issuance. The PPI issuers shall ensure that such information and record thereof are maintained with them;

c. The PPIs can be issued in the form of wallets linked to UPI and can be used for merchant payments (P2M) only;

d. Loading / Reloading of such PPIs shall be against receipt of foreign exchange by cash or through any payment instrument;

e. The conversion to Indian Rupee shall be carried out only by entities authorised to deal in Foreign Exchange under FEMA;

f. The amount outstanding at any point of time in such PPIs shall not exceed the limit applicable on full-KYC PPIs;

g. Provisions of paragraph 13 on validity and redemption, as applicable, shall be adhered to. The unutilised balances in such PPIs can be encashed in foreign currency or transferred back to source (payment source from where the PPI was loaded), in compliance with foreign exchange regulations.

6.6.4 CROSS BOARDER TRANSACTIONS

The use of INR denominated PPIs for cross-border transactions shall not be permitted except as under:

1. PPIs for cross-border outward transactions

   a) Full-KYC PPIs issued by banks having AD-I licence shall be permitted to be used in cross-border outward transactions (only for permissible current account transactions under FEMA viz. purchase of goods and services), subject to adherence to extant norms governing such transactions;

   b) PPIs shall not be used for any cross-border outward fund transfer and / or for making payments under Liberalised Remittances Scheme (LRS). Prefunding of online merchants account shall not be permitted using such rupee denominated PPIs;

c) Bank will enable the facility of cross-border outward transactions only on explicit request of the PPI holders and shall apply a per transaction limit not exceeding Rs.10,000/-, while per month limit shall not exceed Rs.50,000/- for such cross-border transactions;

d) In case such PPIs are issued in card form, it will be ensured that they are EMV Chip and PIN compliant; and

e) Such PPIs may not be issued as a separate category of PPI.

2. PPIs for credit towards cross-border inward remittances

a) Bank appointed as Indian agent of authorised overseas principals, shall be permitted to issue full-KYC PPIs to beneficiaries of inward remittances under the Money Transfer Services Scheme (MTSS) of RBI;

b) Such PPIs shall be issued in adherence to extant norms under the MTSS Guidelines issued by Foreign Exchange Department (FED), RBI;

c) Amounts only upto Rs.50,000/- from individual inward MTSS remittances shall be permitted to be loaded / reloaded in full-KYC PPIs issued to beneficiaries. Amount in excess of Rs.50,000/- shall be paid by credit to a bank account of the beneficiary. Full details of the transactions shall be maintained on record for scrutiny;

d) Roles and responsibilities of PPI issuer shall be distinct from roles and responsibilities as Indian Agents under MTSS; and

e) Such PPIs may not be issued as a separate category of PPI.

3. Foreign Exchange PPIs: Entities authorised under FEMA to issue foreign exchange denominated PPIs shall be outside the purview of the master direction- Master Direction on PPIs- RBI/DPSS/2021-22/82 CO.DPSS.POLC.No.S-479/02.14.006/2021-22,updated on 10-02-2023

6.7. INTEROPERABILITY

6.7.1 Interoperability is the technical compatibility that enables a payment system to be used in conjunction with other payment systems.

6.7.2 Bank shall be guided by the technical specifications/standards/requirements for achieving interoperability through UPI and card networks as per the requirements of NPCI and the

respective card networks. NPCI and card networks shall facilitate participation by PPI issuer in UPI and card networks.

6.7.3 Bank shall have a Board approved policy for achieving PPI interoperability.

6.7.4 Where PPIs are issued in the form of wallets, interoperability across PPIs shall be enabled through UPI.

6.7.5 Where PPIs are issued in the form of cards (physical or virtual), the cards shall be affiliated to the authorised card networks(VISA, MasterCard & RuPay).

6.7.6 PPI-MTS shall remain exempted from interoperability, while Gift PPI issuer (both banks and non-banks) have the option to offer interoperability.

6.7.7 The interoperability shall be facilitated to all KYC-compliant PPIs and the entire acceptance infrastructure. It is the responsibility of the bank to give the holders of full-KYC PPIs (KYC-compliant PPIs) interoperability through authorised card networks(for PPIs in the form of cards) and UPI (for PPI in the form of wallets)

6.7.8 Bank shall adhere to all the requirements of card networks/UPI including membership type and criteria, merchant on-boarding, adherence to various standards, rules and regulations applicable to the specific payment system such as technical requirements, certifications and audit requirements, governance, etc

6.7.9 Bank shall ensure adherence to all guidelines / requirements of card networks/UPI in terms of reconciliation of positions at daily / weekly / monthly or more frequent basis, as the case may be.

6.7.10 Bank shall adhere to all dispute resolution and customer grievance redressal mechanisms as prescribed by the card networks/NPCI.

6.7.11. Bank shall facilitate all basic / standard features of interoperability of UPI.

6.7.12 Bank shall act as Payment System Providers (PSP) in UPI. NPCI shall issue handle to the bank as per its policy / guidelines taking risk management aspects into consideration.

6.7.13 PPI holders shall be on-boarded for UPI by Bank. Bank shall only link its customer wallets to the handle issued to it. Bank as PSP shall not on-board customers of any bank or any other PPI issuer.

6.7.14 Authentication shall be completed by the PPI holder as per her / his existing wallet credentials. In other words, a transaction will be pre-approved before it reaches the UPI.

6.8. SAFETY AND SECURITY

a) Bank shall ensure that all new PPIs issued in the form of cards are EMV Chip and PIN compliant.

b) Bank shall ensure that all reissuance / renewal of PPIs in the form of cards are EMV Chip and PIN compliant.

c) Gift PPIs may continue to be issued with or without EMV Chip and PIN enablement.

6.9 DEPLOYMENT OF MONEY COLLECTED

For the schemes operated by bank, 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 balances appearing in the books of the bank as on the date of reporting.

6.10. VALIDITY AND REDEMPTION

6.10.1 All PPIs issued by the bank shall have a minimum validity period of one year from the date of last loading / reloading in the PPI. PPIs can be issued with a longer validity as well. In case of PPIs issued in the form of card (with validity period mentioned on the card), the customer shall have the option to seek replacement of the card.

6.10.2 Bank shall caution the PPI holder 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 / any other means.

6.10.3 Bank shall be guided by the instructions on Depositor Education and Awareness Fund (DEA 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.

6.10.4 Bank shall clearly indicate the expiry period of the PPI to the customer at the time of issuance of PPIs. Such information shall be clearly enunciated in the terms and conditions of sale of PPI. Where applicable, it shall also be clearly outlined on the website / mobile application of the Bank.

6.10.5 PPIs with no financial transaction for a consecutive period of one year shall be made inactive by the Bank after sending a notice to the PPI holder/s. These can be reactivated only after validation and applicable due diligence. These PPIs shall be reported to RBI separately.

6.10.6 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.

6.11. TRANSACTIONS LIMITS

The PPI holder is allowed to use the PPI for purposes within the overall PPI limit applicable. Executive Director is vested with the authority to modify the limits associated with PPI instruments.

6.12. HANDLING REFUNDS

a) 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.

b) However, refunds in case of failed / returned / rejected / cancelled transactions using any other payment instrument shall not be credited to PPI.

c) Bank shall maintain complete details of such returns / refunds, etc., and be in readiness to provide them as and when called for.

d) Further, Bank shall also put in place necessary systems that enables to monitor frequent instances of refunds taking in place in specific PPIs and be in a position to substantiate with proof for audit / scrutiny purposes.

6.13. SECURITY, FRAUD PREVENTION AND RISK MANAGEMENT FRAMEWORK

6.13.1 Bank shall put in place information and data security infrastructure and systems for prevention and detection of frauds and shall be guided by the bank's approved Information Security Policy.

6.13.2 Bank shall review security measures (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 the infrastructure or procedures.

6.13.3 Bank shall ensure that the following framework is put in place to address the safety and security concerns, and for risk mitigation and fraud prevention:

a) In case of wallets, Bank shall ensure that if same login is provided for the PPI and other services offered by them, the same shall be clearly informed to the customer by SMS or email or any other means. The option to logout from the website/mobile account shall be provided prominently.

b) Bank shall put in place mechanisms to restrict multiple invalid attempts to login / access to the cards, inactivity, timeout features, etc.

c) Bank shall introduce a system where all wallet transactions involving debit to the wallet, including cash withdrawal transactions, shall be permitted only by validation through a Two Factor Authentication (2FA)

c) The Additional Factor of (AFA) requirements for Cards shall be mandatory for domestic transactions.

c) 2FA / AFA is not mandatory for PPIs issued under PPI-MITs and gift PPIs.

d) The transactions undertaken using PPIs through National Electronic Toll Collection (NETC) system shall be performed as per the instructions given in DPSS circular DPSS.CO.PD.No.1227/02.31.001/2019-20 dated December 30, 2019, as amended from time to time.

e) Processing of e-mandate for transactions undertaken using PPIs (cards and wallets) shall be performed, as per the instructions contained in DPSS circular DPSS.CO.PD.No. 447/02.14.003/2019-20 dated August 21, 2019, as amended from time to time.

f) Bank shall provide customer induced options 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.

g) A maximum number of five of beneficiaries may be added in a day per PPI.

j) Bank shall send an alert to the PPI holder when a beneficiary is added.

k) Bank shall put in place suitable cooling period for funds transfer and cash withdrawal 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.

l) Bank shall put in place a mechanism to send alerts when transactions are done using the PPIs including the name of the merchant where transaction is carried out (wherever made available by the acquirer). In addition to the debit or credit amount intimation, the alert shall also indicate the balance available / remaining in the PPI after completion of the said transaction. For transactions undertaken in offline mode, as allowed from time to time, the transaction alert shall be sent as soon as the details of transaction are received by the bank. Sending separate alert for each transaction is not required; however, details of each transaction shall be adequately conveyed as soon as such information reaches the bank.

m) Bank shall put in place velocity check on the number of transactions effected in a PPI per day / per beneficiary.

n) Bank shall also put in place suitable mechanism to prevent, detect and restrict occurrence of fraudulent transactions including loading / reloading funds into the PPI.

o) Bank shall put in place suitable internal and external escalation mechanisms in case of suspicious operations, besides alerting the customer in case of such transactions.

6.13.4 Bank shall put in place centralised database / management information system (MIS) to prevent multiple purchase of PPIs at different locations, leading to circumvention of limits, if any, prescribed for their issuance. In case of full-KYC PPIs issued for government departments,

the limit of Rs.2,00,000/- shall be for each PPI, provided the PPIs are issued for expenses of the concerned government department and the loading is from the bank account of the government department.

6.13.5 Where direct interface is provided to authorised / designated agents, bank shall ensure that compliance to regulatory requirements is strictly adhered to by these systems also.

6.13.6 Bank shall establish a mechanism for monitoring, handling and follow-up of cyber security incidents and cyber security breaches. The same shall be reported immediately to DPSS, CO, RBI, Mumbai. It shall also be reported to CERT-IN as per the details notified by CERT-IN.

6.13.7 Bank shall also be guided by the following circulars:

a) DPSS.CO.PD No.1343/02.14.003/2019-20 dated January 15, 2020 (as amended from time to time) on 'Enhancing Security of Card Transactions'. This circular, inter alia, gives the facility to card holders to switch on / off and set / modify the transaction limits across multiple channels.

b) DPSS.CO.OD.No.1934/06.08.005/2019-20 dated June 22, 2020 (as amended from time to time) on Increasing Instances of Payment Frauds – Enhancing Public Awareness Campaigns Through Multiple Channels.

c) CO.DPSS.POLC.No.S-384/02.32.001/2021-2022 dated August 03, 2021 (as amended from time to time) on Framework for Outsourcing of Payment and Settlement-related Activities by PSOs. The bank shall be guided by the outsourcing related instructions issued by RBI.

6.14. CUSTOMER PROTECTION AND GRIEVANCE REDRESSAL FRAMEWORK

6.14.1 Bank shall disclose all important terms and conditions in clear and simple language. These disclosures shall include:

a) All charges and fees associated with the use of the instrument; and

b) The expiry period and the terms and conditions pertaining to expiration of the instrument.

6.14.2 Bank shall put in place a formal, publicly disclosed customer grievance redressal framework, including designating a nodal officer to handle the customer complaints / grievances, the escalation matrix and turn-around-times for complaint resolution. The complaint facility, if made available on website / mobile, shall be clear and easily accessible. The framework shall include, at the minimum, the following:

a) Bank shall disseminate the information of customer protection and grievance redressal policy in simple language.

b) Bank shall clearly indicate the customer care contact details, including details of nodal officials for grievance redressal (telephone numbers, email address, postal address, etc.) on website, mobile wallet apps, and cards.

c) Bank's agents shall display proper signage of the Bank and the customer care contact details as at (b) above.

d) Bank shall provide specific complaint numbers for the complaints lodged along with the facility to track the status of the complaint by the customer.

e) Bank shall initiate action to resolve any customer complaint / grievance expeditiously, preferably within 48 hours and endeavour to resolve the same not later than 30 days from the date of receipt of such complaint / grievance.

f) Bank shall display the detailed list of its authorised / designated agents (name, agent ID, address, contact details, etc.) on the website / mobile app.

6.14.3 Bank shall create sufficient awareness and educate customers 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.

6.14.4 Bank shall provide an option for the PPI holders to generate / receive account statements for at least past 6 months. The account statement shall, at the minimum, provide details such as date of transaction, debit / credit amount, net balance and description of transaction. Additionally, bank shall provide transaction history for at least 10 transactions.

6.14.5. Customers shall have recourse to the Reserve Bank-Integrated Ombudsman Scheme, 2021 for grievance redressal.

6.14.6 Bank shall ensure transparency in pricing and the charge structure as under:

a) Ensure uniformity in charges at agent level.

b) Disclosure of charges for various types of transactions on website, mobile app, agent locations, etc.

c) Specific agreements with agents prohibiting them from charging any fee to the customers directly for services rendered by them on behalf of the bank.

d) Require each retail outlet / sub-agent to post a signage indicating the status as service providers of the bank and the fees for all services available at the outlet.

e) The amount collected from the customer shall be acknowledged by issuing a receipt (printed or electronic) on behalf of the PPI issuer.

6.14.6 Bank shall be responsible for addressing all customer service aspects related to all PPIs (including co-branded PPIs) issued by the bank as well as agents.

6.14.7 Bank shall also display Frequently Asked Questions (FAQs) on its website / mobile app related to the PPIs.

6.14.8 Bank shall also be guided by the following DPSS circulars:

a) Harmonisation of Turn Around Time (TAT) and customer compensation for failed transactions using authorised Payment Systems issued vide DPSS circular DPSS.CO.PD No.629/02.01.014/2019-20 dated September 20, 2019 (as amended from time to time);

b) Online Dispute Resolution (ODR) system for resolving customer disputes and grievances pertaining to digital payments, using a system-driven and rule-based mechanism with zero or minimal manual intervention, issued vide DPSS circular DPSS.CO.PD No.116/02.12.004/2020-21 dated August 6, 2020 (as amended from time to time).

6.14.9 Bank shall continue to be guided by RBI circulars DBR.No.Leg.BC.78/09.07.005/2017-18 dated July 6, 2017 or DCBR.BPD.(PCB/RCB). Cir.No.06/12.05.001/2017-18 dated December 14, 2017, as applicable on Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions.

7. PREPAID TRAVEL CARD:

The Bank may enter the business of prepaid travel card either on its own or through a mutual tie-up with another Bank or entity within the framework of FEMA guidelines as amended from time to time and in compliance with RBI guidelines of card issuance. In addition to the above mentioned terms & conditions of prepaid cards, the following compliances shall also be followed during the issuance of prepaid travel currency cards

1. The minimum currency limit to be loaded in the card can be determined by the Bank and the maximum currency limit is as per FEMA guidelines.
2. The Bank shall issue prepaid foreign currency cards to the account holders/existing customers of the Bank or to walk in customers after obtaining their KYC details.
3. Executive Director of the Bank is vetted with the full discretion to fix / revise the charges for the issuance, usage of card, features and products in the travel card portfolio.
4. BOG- TFCPC (Trade Finance Central Processing Centre) shall be responsible for Foreign Currency loading, reloading, encashment and reconciliation of currency in the card.

8. INFORMATION SYSTEM AUDIT, PARA BANKING AUDIT, SECURITY & COMPLIANCE

8.1 Bank shall be guided by RBI circulars DBS.CO.ITC.BC.No.6/31.02.008/2010-11 dated April 29, 2011, DBS.CO/CSITE/BC.11/33.01.001/2015-16 dated June 02, 2016,

DCBS.CO.PCB.Cir.No.1/18.01.000/2018-19 dated October 19, 2018 (as applicable) and other relevant circulars on the subject, as amended from time to time

8.2 Bank shall, put in place the following framework:

a) Application Life Cycle Security: The source code audits shall 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.

b) Security Operations Centre (SOC): Integration of system level (server), application level logs of mobile applications with SOC for centralised and co-ordinated monitoring and management of security related incidents.

c) Anti-Phishing: Subscribe 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.

d) Risk-based Transaction Monitoring: Risk-based transaction monitoring or surveillance process shall be implemented as part of fraud risk management system.

e) Vendor Risk Management: (i) Enter into an agreement with the service provider that amongst others provides for right of audit / inspection by the regulators of the country; (ii) RBI shall have access to all information resources (online / in person) that are consumed by service provider, to be made accessible to RBI officials when sought, though the infrastructure / enabling resources may not physically be located in the premises of service provider; (iii) Adhere to the relevant legal and regulatory requirements relating to geographical location of infrastructure and movement of data out of borders; (iv) Review the security processes and controls being followed by service providers regularly; (v) Service agreements of bank with service provider shall include a security clause on disclosing the security breaches if any happening specific to issuer's infrastructure or process including not limited to software, application and data as part of Security incident Management standards, etc. (vi) maintain updated contact details of service providers, intermediaries, external agencies and other stakeholders for coordination in incident response. Bank shall put in place a mechanism with the stakeholders to update and verify such contact details.

f) Disaster Recovery (DR): Consider having DR facility to achieve the Recovery Time Objective (RTO) / Recovery Point Objective (RPO) for the systems 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.

g) Product Level Limits – Bank shall put in place appropriate product-level limits on the level of acceptable security risk, security objectives and performance criteria including quantitative benchmarks for evaluating the success of the security built into the card products & periodically compare actual results with projections and qualitative benchmarks to detect and address adverse trends or concerns in a timely manner and modify the business plan/ strategy involving the product, when appropriate, based on the security performance of the product or service.

h) Authentication Methodologies - Appropriate authentication methodologies shall be put in place based on an assessment of the risk posed for card based transactions. The risk shall be evaluated in light of the type of customer (e.g., retail/ corporate/ commercial); the customer transactional requirements/ pattern, the sensitivity of customer information and the volume, value of transactions involved. Customer acceptance, ease of use, reliable performance, scalability to accommodate growth, customer profile, location, transaction, etc., and interoperability with other systems, wherever applicable shall also be taken into consideration while implementing authentication methodologies.

(i) Bank shall provide information about the risks, benefits and liabilities of using card products and related services before offering them to customers. Customers shall also be informed clearly and precisely on their rights, obligations and responsibilities on matters relating to card payments, and, any problems that may arise from its service unavailability, processing errors and security breaches. The terms and conditions including customer privacy and security policy applying to card products and services shall be readily available to customers from the website. Cards shall be offered to customers on explicit request of customers and shall not be bundled without their knowledge.

(j) Whenever new operating features or functions, particularly those relating to security, integrity and authentication, are introduced to cards, clear and effective communication followed by sufficient instructions to properly utilise such new features shall be provided to the customers.

(k) Bank shall continuously create public awareness on the types of threats and attacks used against the consumers while using card products and precautionary measures to safeguard against the same. Customers shall be cautioned against commonly known threats in recent times like phishing, vishing, reverse-phishing, remote access of mobile devices and educated to secure and safeguard their account details, credentials, PIN, card details, devices, etc.

(l) Bank shall ensure robust surveillance/ monitoring of card transactions and setting up of rules and limits. Bank shall put in place transaction limits at Card, BIN as well as at the Bank level.

Such limits shall be mandatorily set at the card network switch itself. Bank shall put in place transaction control mechanisms with necessary caps (restrictions on transactions), if the above requirement is breached. A periodic review mechanism of such limits shall also be carried out. Transactions shall be monitored on 24x7 basis, including weekends, long holidays

(m) Bank shall ensure that card details of the customers are not stored in plain text at the bank and its vendor(s) locations, systems and applications. Bank shall also ensure that the processing of card details in readable format is performed in a secure manner to strictly avoid data leakage of sensitive customer information.

8.3 There shall be an audit for card business conducted by the bank and this shall be an integral part of Para-banking audit. Necessary system must be in place to ensure audit of the card issuance portfolio of the bank. Such audit should cover the following.

- Compliance by branches with respect to safe keeping of cards and pin mailers under dual custody.
- Adherence of instructions with regard to obtaining proper acknowledgement and retaining the same, while distributing cards and pin mailers.
- Compliance of stipulated systems, processes and procedures for secured delivery of pin mailers and cards to branches
- Compliance by department with regard to instructions on vendor selection for card personalization and sharing of card data.

The report of the audit shall have to be submitted to audit committee of the Board for review on quarterly basis.

9. REPORTING:

3. Central Processing Centre, BOG shall provide/generate sufficient reports for the daily monitoring and operations. In addition to this, Retail Banking Department shall submit report to Board or Board committee or Executive committee designated by board for review on half yearly or as needed basis.
4. The Bank shall submit report on card business to Department of Payment Settlement Systems (DPSS) on monthly basis or as instructed by Reserve Bank of India.

10. REDRESSAL OF GRIEVANCES:

1. The Bank shall display customer support number for customer grievance on bank's website.
2. The Bank shall display the grievance redressal procedure of the bank and the time frame for responding to the complaints on bank's website.
3. The Bank shall employ proper acknowledge system for follow up by providing complaint number for customer's grievance/complaints.
4. Banking Operations Group [BOG] in co-ordination with Corporate Financial Management (CFM) department shall be responsible for reconciliation of transactions using debit cards and prepaid cards including Fastag.
5. The hierarchy for the redressal of customer complaints related to failed transactions at ATMs/POS terminals/Online transactions shall be Branch Manager →Card cell at Banking Operations Group →Head of Department - BOG
6. DPSS guidelines on timeframe for reconciliation of failed transactions at ATMs, PoS, ecommerce etc as amended from time to time should be complied in this regard. The RBI circular on Harmonisation of TAT and customer compensation for failed transactions using authorized payments systems shall form the basis of Bank's Grievance redressal system for debit cards and prepaid cards including Fastag.
7. Bank shall be liable to compensate the complainant for the loss of his/her time, expenses, financial loss as well as for the harassment and mental anguish suffered by him/her for the fault of the card-issuer and where the grievance has not been redressed in time. If a complainant does not get satisfactory response from the card-issuer within a maximum period of 30 days from the date of lodging the complaint, he/she will have the option to approach the Office of the RBI Ombudsman under Integrated Ombudsman Scheme for redressal of his/her grievance/s.
8. Online Dispute Resolution (ODR) system for resolving customer disputes and grievances pertaining to digital payments, using a system-driven and rule-based mechanism with zero or minimal manual intervention, issued vide DPSS circular DPSS.CO.PD No.116/02.12.004/2020-21 dated August 6, 2020 (as amended from time to time)

9. RBI guidelines regarding Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions as amended from time to time shall be adhered to in this regard.
10. The nodal officer of the Bank for customer complaints shall also act as Grievance Redressal Officer with respect to card operations.

11. SAFEGUARDS AGAINST MONEY LAUNDERING PROVISIONS

11.1 Bank shall adhere to the Know Your Customer (KYC) / Anti-Money Laundering (AML) / Combating Financing of Terrorism (CFT) guidelines issued by the Department of Regulation (DoR), RBI, in "Master Direction – Know Your Customer Direction, 2016", as updated from time to time.

11.2 Bank shall adhere to the Provisions of Prevention of Money Laundering Act, 2002 (PMLA) and Rules framed thereunder, as amended from time to time.

11.3 Bank shall maintain a log of all the transactions undertaken using the PPIs 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. Bank shall also file Suspicious Transaction Reports (STRs) to Financial Intelligence Unit-India (FIU-IND).

12. REVIEW

The Debit & Prepaid card business policy must be reviewed on a half yearly basis. The review shall include, inter-alia, card usage analysis including cards not used for long durations and the inherent risks therein. The bank should put in place adherence and monitoring mechanism with Best practices in industry towards risk mitigation and security measures.

****