

**BANK POLICY ON
ISSUANCE AND
MANAGEMENT OF DEBIT
CARDS
FOR THE YEAR
2022-23**

Digital Payment and Transaction Banking Dept. Central Office.

INDEX

CHAPTER-1.....	4
1. <i>INTRODUCTION AND ELIGIBILITY</i>	<i>4</i>
CHAPTER-2.....	13
2. <i>ATM PIN MANAGEMENT.....</i>	<i>13</i>
CHAPTER-3.....	14
3. <i>ENHANCING SECURITY IN CARD TRANSACTION</i>	<i>14</i>
CHAPTER-4.....	16
4. <i>LOST/DAMAGED/STOLEN/COUNTERFEIT/EXPIRED CARDS</i>	<i>16</i>
CHAPTER-5.....	17
5. <i>DE-HOTLISTING/ RE ISSUANCE OF CARD IN PLACE OF LOST/DAMAGED.....</i>	<i>17</i>
<i>CARD</i>	<i>17</i>
CHAPTER-6.....	18
6. <i>ATM HELP DESK MENU.....</i>	<i>18</i>
CHAPTER-7.....	18
7. <i>NCMC NATIONAL COMMON MOBILITY CARD (NCMC)</i>	<i>18</i>
CHAPTER-8.....	19
8. <i>CASH WITHDRAWAL AT POINT OF SALE (POS) TERMINAL</i>	<i>19</i>
CHAPTER-9.....	21
9. <i>CONFIDENTIALITY</i>	<i>21</i>
CHAPTER-10.....	21
10. <i>COMPLIANCE</i>	<i>21</i>
CHAPTER-11.....	21
11. <i>CUSTOMER GRIEVANCE.....</i>	<i>21</i>
CHAPTER-12.....	22
12. <i>MONITORING OF CARD TRANSACTION –EFRMS</i>	<i>22</i>
CHAPTER-13.....	27
13 <i>CUSTOMER PROTECTION –LIMITED LIABILITY IN UNAUTHORISED</i>	<i>27</i>
<i>ELECTRONIC BANKING TRANSACTIONS</i>	<i>27</i>
CHAPTER-14.....	27

BANK POLICY ON ISSUANCE AND MANAGEMENT OF DEBIT CARDS

14. *FAILED TRANSACTION (CUSTOMER DISPUTES)* 27
CHAPTER-15..... 29

15. *UNSOLICITED COMUNICATION*..... 29
CHAPTER-16..... 29

16. *LOYALTY PROGRAM-ANMOL REWARDS*..... 29
CHAPTER-17..... 31

17. *INSURANCE TO CARD HOLDER* 31
CHAPTER-18..... 31

18. *CO-BRANDING* 31
CHAPTER-19..... 33

19. *TOKENIZATION* 33
CHAPTER-20..... 33

21. *E-Mandate on Debit Card:* 33
CHAPTER-21..... 35

21. *EMI ON DEBIT CARDS.* 35
CHAPTER-22..... 36

22. *SECOND FACTOR AUTHENTICATION /ONE TIME PASSWORD (OTP) FOR CASH WITHDRAWAL* 36
CHAPTER-23..... 36

23. *PERIODIC REVIEW OF DEBIT CARD POLICY & OPERATION* 36

CHAPTER-1

1. INTRODUCTION AND ELIGIBILITY

Central Bank of India has introduced Debit Card products in 2005. Debit card is a special plastic card and are linked to a bank account which is used for cash withdrawal on any Bank ATM, Purchase of goods and services at permitted Point of Sale (POS) terminal or for on-line payments for E-Commerce (E-Com) and for payment of utility services. Debit cards are issued for transactions where there is immediate debit to the customer's account and where straight through processing is involved. However Debit card with National Common Mobility Card (NCMC) features/Wallet features are issued allowing offline debit transactions with limited purpose (Close loop/Open loop) and with limited amount. Debit Cards also can be used for funds transfer from one person to another account subject to prescribed limit and conditions. The emerging Less Cash Economy provides huge opportunity for growth in debit card business. Central Bank of India, as a part of its business strategy to encash the emerging opportunities, issues Basic as well as Premium cards of different Card Network such as **RuPay, MasterCard, Visa etc. to different categories of customers.** Customer may be offered one or more cards of different variant.

1.1 While drawing up the Policy, following major sources have been considered:

1. **RBI's Master circular (RBI /2022-23-92 Dor.AUT.REC.No.27/24.01.041/2022-23 dated 21st April 2022) on Debit Card Operations, RBI's Master Direction on Digital Payment & Security Controls and RBI's direction on Storage of Payment System Data.**
2. RBI's Master Circular on Customer Service.
3. RBI's Guidelines/Instructions through Notification on Security features in ATM, PoS and On-line Transactions.
4. **RBI circular on Harmonization of Turn Around Time(TAT) and Customer Compensation for Failed Transactions Using Authorised Payment Systems dated September 20,2019**
5. Government of India Guidelines if any for digital penetration
6. Relevant Guidelines of IBA.
7. BCSBI's code.
8. NPCI Guidelines
9. Our internal circulars.
10. RuPay, Master card and Visa international relevant guidelines.

1.2 Objectives

The Policy is to provide a framework of rules/regulations/standards/practices to the Debit card operations as an Issuer and Acquirer Bank, to ensure that the same are in alignment with the best customer practices. The Policy is also intended to comply with Reserve Bank of India (RBI)'s instructions to Banks for adoption of adequate safeguards and implement the guidelines in order to ensure that card operations are run on sound, prudent and customer friendly manner. This Policy is expected to serve as a reference document for all staff involved in card operations of the Bank.

1.3 Eligible Branches for issuance of Debit Cards:

All Branches (other than specialized branches like; CCPB, ARB, SAMB and Virtual Branch etc.) are eligible for issuing debit cards.

PMJDY Card are also issued in accounts opened at BC Points by default with complete CIF details

1.4 Eligible Accounts:

1. Debit cards shall only be issued to customers having Savings Bank/Current Accounts.
2. No bank shall issue debit cards to cash credit/loan account holders. However, it will not preclude the banks from linking the overdraft facility provided along with Pradhan Mantri Jan Dhan Yojana accounts with a debit card.
3. Saving A/c of individuals including BSBD, PMJDY, Student, No Frill, NRE/Pension/Staff/Blind Person in a single name or joint names with operating instructions 'Either or Survivor', 'Former or Survivor' or 'Anyone or Survivor/s'.
4. Customers are eligible for ADD ON Card in CBS in the accounts with operating Instructions 'either or Survivor' or 'Anyone or Survivor/s'.
5. Individual Minor Savings Account holders having age of 10 and above can be issued Debit Cards.
6. Current A/c in individual name, Sole Proprietor and Partnership Firms, Card to be issued in the name of person and not in the name of the firm.
7. Overdraft (OD) A/c in individual name, Sole Proprietor and Joint names. OD A/c for business purpose is not eligible for this facility.
8. Staff Overdraft Account
In Joint / Partnership accounts, card issuance application form must be signed by all joint account holders / partners. The branch shall also ensure that the applicant has a clear mandate to operate the account.
9. For Issuance of ATM/Debit Cards, the Accounts shall be fully KYC/AML compliant as per RBI guidelines in force.
10. Debit Card is issued on CIF in CBS & Maximum three accounts can be linked to a Card as primary and secondary accounts.
11. For every CIF, only one card can be issued per card code in CBS. However if the same card code is requested by the customer, it can only be issued after hot listing existing card of same code.
12. Customer can choose an account for linking to the Card (Primary or Secondary, in that order, depending on clear balance available) for Cash withdrawal in our ATMs. For all other transaction, only primary account can be used.

Debit cards shall not to be issued in following accounts:

1. Institutional / Trust / Company Accounts/HUF/Club/Society & Associations.
2. Accounts, which are not eligible for issuance of cheque book facility.
3. CC/OD A/c sanctioned for business purpose (Such Customers/Account holders shall be encouraged to use the Net Banking facility.)
4. Term Loan/ Demand Loan accounts.
5. The instructions/guidelines on KYC/AML/CFT applicable to banks, issued by RBI from time to time have to be adhered to in respect of cards issued including co-branded cards.
6. Debit Cards shall not be issued in deceased Accounts.
7. Illiterate customers other than specified by Govt of India are not eligible.

1.5 Eligible Customers:

BANK POLICY ON ISSUANCE AND MANAGEMENT OF DEBIT CARDS

1. All individual customers with a fully KYC Compliant Bank Account and who are competent to enter into a valid contract with the Bank, are eligible to get ATM/Debit Card.
2. No customer shall be offered ATM/Debit Card unsolicited, meaning without explicit/written consent for it.
3. ATM/Debit Card shall be issued with customer mandate (marking Yes/NO) in Account Opening Form (under Section –Services required) or mandate obtained by separate Debit Card Application.
4. ATM/Debit Card being an important instrument to withdraw Cash from ATM/ Permitted Point of Sale (PoS), Payment for purchases made On-Line and at Point of Sale (Card Present, Point of Contact), it is important to promote issuance of ATM/Debit Card to all customers to reduce foot fall at Branches and increase Digital Transactions by our Customers. Therefore, Branches shall ensure to obtain consent for issuance of ATM/Debit Card by explaining/educating Customers about the benefits of taking Debit Cards.
5. Each Branch shall ensure issuance of ATM/Debit Card to 100 percent of our eligible customer for which front line staff shall be given requisite instructions.
6. Mobile number is mandatory for issuance of ATM/Debit card as customers is required to be intimated through SMS for any Financial / Non-Financial Transaction under taken by Customers and/or information about failed Transaction. Mobile number registration is also important as any fraudulent attempt and/or any fraudulent Transactions which is attempted and/or undertaken respectively without the knowledge of our Customers shall set an alert to customer to take precaution/report to bank to Hotlist the Card.
7. Bank shall issue only Rupay (Classic) cards to PMJDY/ Basic Saving Bank Deposit Scheme and similar no-frill/zero balance/ accounts where minimum balance maintenance is not stipulated. Rupay (Classic) cards shall be issued to CKCC and Mudra Account holders as per guidelines of RBI.
8. In existing accounts, where mandate was not obtained at the time of Account Opening, through Account Opening Application form, Branches to obtain fresh Debit Card Application form before issuance of debit card, “Bank may also provide option to customers to apply the card through digital/alternate delivery channels”, to comply with RBI instructions not to issue Debit Card unsolicited.

1.6 Security Features

ATM/Debit cards are convenient but if the card falls in wrong hands, this can cause a lot of damage to the account holder and cause reputational risk/loss too to the Bank. These cards shall be issued with mandated security to safe guard against misuse with features listed below:

1. **Card Design/Form:** Each Card to be issued by the Bank shall have standard size, Bank Logo, Card Network Logo, Unique Card Number (Sixteen Digit).
2. **Card Validity/Expiry Date:** Each Card shall have validity period with Month/Year printed/embossed on Face of Card.
3. **CVV Number:** Each Card has system generated CVV (Card Verification Value)/CVN (Card Verification Network) number (Three digit) written on the back of Card for E-com transaction. The CVV number is required to be entered to validate the transaction on Card Not Present Transaction mandatorily as a factor of authentication.
4. **EMV Card:** EMV stands for Euro pay, MasterCard and Visa. EMV is a global standard for Credit and Debit payment based on chip card technology. EMV Chip Card protects against counterfeit (Skimming) card frauds. All variant of Cards of the Bank shall be EMV Card.

BANK POLICY ON ISSUANCE AND MANAGEMENT OF DEBIT CARDS

5. **Personal Identification Number (PIN):** PIN is a four digit secret number/code which is given to customer at the time of issuing a Debit Card for purpose of security. Alternatively, it can be generated by the customer using different channel such as Mobile App, Internet Banking, ATM Terminal and by way of Interactive Voice Response (IVR) Mode, called Green PIN. Each card can be used in combination with the Personal Identification Number (PIN) for cash withdrawal at ATM, for payment for Merchandise purchases at Point of Sale (Card Present situations) and Cash withdrawal at permitted POS/Service Points such as Banking Correspondences. PIN not required for Online/Offline contactless transactions to the extent permitted by RBI.
6. **Signature:**

On the backside of the card, there is a provision of a strip where the card owner needs to sign. This is for a counter check with signature on the customer copy when customer makes a purchase at a POS.

Customer is required to sign on the marked 'Strip' after receipt of it from Bank. Merchandise may refuse to accept payment from an un-signed Card for security reasons.
7. **Photograph:**

Some cards may have the photograph of the card holder as an additional security feature if customer so desires. This facility shall be available to personalized Cards only.

1.7 Issuance of Card through Authorized Card Network Operators

Bank shall issue Debit Card/Pre-paid Cards of such Card Network who are authorized by Reserve Bank of India under the Payment and Settlement Act, 2007 for setting up and Operating Payment Systems in India.

Cards of a particular Network shall be considered after due certification process. At present following Card Network are used for issuance of Card.

1. National Payments Corporation of India (NPCI) - RuPay Cards (debit cards/prepaid cards).
2. MasterCard Asia/ Pacific Pvt. Ltd., Singapore (Earlier MasterCard International Incorporated, USA was performing this activity) - MasterCard
3. Visa Worldwide Pvt. Limited, Singapore (Earlier Visa International Service Association, USA was performing this activity) - Visa Card

Bank may, as per need, consider issuance of Debit/Pre-Paid Card of any RBI Authorized Card Network with prior approval of Board.

Though Rupay Card launched by NPCI as a domestic, open loop, multilateral system which allows all Indian Banks and Financial Institutions in India to participate in electronic payments, NPCI has mutual/reciprocal arrangements with International Retail Payments system for Rupay Cards to make it an International Card. Bank may with prior approval of Board agree for issuance of co-Branded Cards as Issuer and Acquirer.

1.7.1 Following Rupay International Card issuance (Issuer) and Acquirer are approved and arrangement has been made for honoring these cards at international level:

1. Diners Club (Diners club International)
2. Discover (Discover Financial Services Company)
3. Pulse (Subsidiary of Discover Financial Services, USA)

4. JCB- (JCB International Company)

1.8 General Terms and Conditions applicable to issue of Debit Card to Customers

1. The relationship between the bank and the card holder shall be contractual. A set of contractual terms and conditions governing the issue and use of such a card shall be made available to the cardholders in writing. These terms shall maintain a fair balance between the interests of the parties concerned. The terms shall be expressed clearly.
2. It shall be ensured customer doesn't force to avail debit card facility and shall not link issuance of debit card to availment of any other facility from the bank.
3. The card shall not be dispatched to a customer unsolicited, except in the case where the card is a replacement/renewal of a card already held by the customer. 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 customer. Further, bank shall obtain explicit consent of the cardholder prior to the renewal of an existing card. The time line for issuance of Card is 10 days (3 days for Card file generation and 7 days for dispatch and delivery of card to the customer).
4. The term and condition for the issue and usage of a card shall be mentioned in clear and simple language (Preferably in English, Hindi and the local language) comprehensible to the cardholder with minimum font size Arial-12. As per RBI guidelines amended from time to time.
5. The terms shall specify the basis of any charge, but not necessarily the amount of charges at any point of time.
6. The terms shall specify the period within which the cardholder's account would normally be debited.
7. The terms may be altered by the bank, 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.
8. The terms shall put the cardholder under an obligation to take all appropriate steps to keep safe the card and the means (such as PIN or code) which enable it to be used.
9. The terms shall put the cardholder under an obligation 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.
10. The terms shall put the cardholder under an obligation to notify the bank immediately after becoming aware:
 - i. Of the loss or theft or copying of the card or the means which enable it to be used;
 - ii. Of the recording on the cardholder's account of any unauthorized transaction; and
 - iii. Of any error or other irregularity in the maintaining of that account by the bank.
11. The terms shall specify a contact point to which such notification can be made. Such notification can be made 24*7 at any time of the day or night.
12. The terms shall specify that the bank has exercised care when issuing PINs or codes and shall be under an obligation not to disclose the cardholder's PIN or code, except to the cardholders.
13. The terms shall specify that the bank shall be responsible for direct losses incurred by a cardholder due to a system malfunction directly within the bank's control. However, the bank shall not be held liable for any loss caused by a technical breakdown of the payment system if the breakdown of the system was recognizable for the cardholder by a message on the display of the device or otherwise known. The responsibility of the bank for the non-execution or defective execution of the transaction is limited to the principal sum and the loss of interest subject to the provisions of the law governing the terms.

14. Other Form Factors

- a) Scheduled Commercial Banks (other than RRBs) may issue other form factors in place of a plastic debit card such as wearables after obtaining explicit consent from the customer.
- b) Form factors issued in place of a debit card shall be subject to the specific and general guidelines applicable to debit cards.
- c) Banks shall provide options for disabling or blocking the form factor through mobile banking, internet banking, SMS, IVR or any other mode.
- d) Banks shall submit a detailed report to the Department of Regulation, Reserve Bank of India, prior to the issuance of any such form factors. Any bank that has already issued such product prior to the effective date of the Master Direction, shall submit a detailed report to Department of Regulation within 30 days from the effective date.

1.9 Selection of Vendor for Printing and End to End Solution for Issuance of ATM/Debit Card.

1. Bank shall follow strictly CVC Guidelines and internal Procurement Policies as applicable for selection of Vendor.
2. All debit cards to be procured shall strictly conform to the International Standard set vide ISO/IEC FDIS 7810:2003(E) and/or any other similar Standards by any Regulatory Authority which includes Reserve Bank of India as well as Card Network Services.
3. The eligibility criteria for Bidders shall be well defined in the offer documents to comply with security requirement of ATM/Debit Cards as stipulated by RBI, Card Network (RuPay, Master Card, Visa and any other Card System).

1.10 Process of card printing

Printing of card is a much secured process. For this, secured keys are provided by the Card Networks viz., Rupay, MasterCard and Visa. These are a set of 3-4 keys (depending on the card network) and issued to nominated custodians from the Bank. To initiate card printing process by selected vendor, these secured keys will be punched into the systems of the vendors (at their location) by 3-4 nominated custodians (Officers) after which only the card printing process can start. This key ceremony to be performed under supervision and after necessary approval from Vertical Head.

Procedure of handling Security Keys of Card Network

Security keys issued by card network viz., Rupay, Master Card and Visa are to be securely kept in the safe custody in MMO branch with access permission of 2 officers. Since the combination of all 3 keys compromised together only can lead to fraudulent activity, it is therefore mandatory to handover only one key to custodian.

1.11 CUSTOMER EDUCATION FOR SAFETY AND SECURE USE OF DEBIT CARDS

BANK POLICY ON ISSUANCE AND MANAGEMENT OF DEBIT CARDS

Debit Cards are linked to Customer Accounts and through use of Debit Card, a customer permitted to do multiple activities through Card Present and Card not Present situations. The Card is also used by customers for doing both Financial & Non-Financial Transactions, Identification for OTP and PIN Change etc. Misuse, Loss of Card and PIN information can lead to transfer of funds without the knowledge of Customer which may lead to loss to Customers and or Loss to the Bank, including Reputational Risk to Bank.

Therefore, it is desired that Bank educate the customers about safe guards against misuse and as well as safe keeping of Cards and PIN.

Besides handing over a Kit to Customers which shall contain instructions to customers, Bank's staff while handing over Cards and PIN to customer will educate customer about following suggestive but not exhaustive points:

What precautions to be taken while using debit cards

There are certain things that the bank does to ensure card safety but the customer must also take necessary precautions to so that the card is not misused. Given below are few precautions to be taken by the card holder and Branches to prevent misuse of the debit card:

- i. Customers shall Sign on the reverse of the Card
- ii. **Precaution for PIN:** Avoid writing the PIN number on the card or on a paper in wallet or on the cover of the card which can provoke misuse of the card. PIN number to be selected carefully, and preferably changed after the first transaction and should be updated from time to time. Customer should not keep card and PIN together. PIN and card details should not be shared with anybody.
- iii. **Keep the Helpline Number Handy:** It is advised to keep the helpline number handy/noted elsewhere so that customer can contact the bank for blocking of the lost/stolen card.
- iv. **Mobile Alerts:** At the time of account opening mandate to be obtained for SMS facility and it must be ensured that the SMS facility is activated, so that whenever card is used SMS alerts will be sent to the registered/linked mobile number.
- v. **Be Vigilant:** Extra care to be taken when the card is handed over to third person i.e. Merchant etc. for swiping, as card cloning is a very serious and rampant threat. It shall be ensured that the card number is not noted down or copied.
- vi. **Follow Rules:** The card holder shall be made aware about the precautions to be taken/safety measures to be adopted specially when travelling abroad and also about the rules pertaining to card use internationally.

1.12 CARD VARIANTS

Card can be issued under two categories: (i) Pre Generated Card (Across the Counter) and (ii) Personalized Card (Customer desiring their Names/Title/Photograph to be printed on Cards)

A. Pre generated Cards - Instant cards available in the Branch (Cards printed/issued without card holders name embossed). Such Cards can be issued by branches by linking the same to CIF/Account of the customer.

Supply of Pre-generated cards to Regional offices-As per Branch/Region request, Debit card department shall analyze the stock requirement and supply the cards to Regional Offices.

BANK POLICY ON ISSUANCE AND MANAGEMENT OF DEBIT CARDS

B. Personalised Cards-Cards issued on specific request of customer with name of the card holder embossed with or without photograph.
Name embossed on the card by default is name of the Card holders/Customer as mentioned in CIF. If any change in the name is required, customer has to specifically request for it with detail of the name in “Emboss Name” field of card application.

C. Classic & Premium Cards based on Customer Profile

Bank shall issue various types of cards depending upon the Category/Profile of Customers (such as PMJDY Accounts, Basic Savings Deposit Accounts (BSBD), Student Accounts, Premium/High Net worth Customers etc. with transaction limits, Transactions permissible in Domestic and/or International facilities. Classic and Premium Variants of Card shall also be different for different Card Network as per Card Network specifications.

D. Issue of international debit cards will also be subject to directions issued under Foreign Exchange Management Act, 1999, as amended from time to time. For the details of the cards which can be enabled for International transactions (On written request of the card holders).

1.13 Bank may levy charges for Issuing/Renewal/Annual/Usage of Debit Card by customers for Cash withdrawal (On Us/Issuer) Transactions through ATM, Transaction at Point of Sale (PoS) and On-Line payment by use of Debit Card subject to Regulatory Guidelines/ Government of India, charges shall be levied and charged.

Charges shall be levied and changed as per direction of Top Management under the regulatory guidelines of RBI/ Government of India.

Bank shall not levy any charges that were not explicitly indicated to the card holder at the time of issue of the card and without getting his /her explicit consent. However, this shall 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 debit cards shall be displayed on the Bank’s website.

The convenience fee, if any charged on specific transaction, shall be indicated to the card holder in a transparent manner, prior to the transaction.

The terms may be altered by the bank, but 30 days’ notice of the change shall be given to the card holder to enable him/her to withdraw if he/she so chooses after the notice period of 30 days, the card holder 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 card holder through all communication channels available.

1.14 SAFE KEEPING OF CARDS/PIN AT BRANCHES / REGIONAL OFFICE

Debit Cards and PINs are to be treated as Security Items and guidelines issued for safe keeping and handling of Security items are equally applicable to Debit Cards and PINs.

On receipt of Cards (Personalized / Pre-Gen) and sealed PIN Mailer from Central Office / Regional Office, the Branch shall enter these details in respective Registers (Format prescribed) and shall be kept in dual safe custody of the Branch.

1.15 DELIVERY OF CARDS:

- i. "Debit cards shall be delivered
 - a) Through Home Branch or
 - b) Through Home deliveredCustomer may opt for delivery of Card at Permanent address/Correspondence address/home branch. In case Card is not delivered at residential/correspondence address the same shall be delivered to home Branch. Home Branch shall arrange for delivery of the card to the customer.
- ii. Branch will inform to the customers to collect the cards personally from the branch.
- iii. When the customer visits the branch to collect his card, the branch should obtain His/her signature in Card Issuing Register and verify details from the branch records. Thereafter customer shall be advised to sign on the signature panel on the backside of the card.
- iv. In no case card shall be delivered to third person. However, in exceptional cases, Only with the written approval of the Branch Manager, Card can be delivered to any authorized persons under proper identification. The name of authorized person to be mentioned in the Card Delivery Register and his signature to be recorded in the Register for having received the Card.
- v. At the written request of Customer, a Card can be sent to a Branch/Office other than Home Branch for delivery to Customer. Procedure mentioned under I & II shall be followed in this case too.
- vi. Branches also can arrange to home delivery of Cards to Customers in case of Senior Citizen, Differently abled, Sick/indisposed to move cases. Members of Staff/Agents required obtaining signature while handing over card to Customer after duly convinced with the identity of customer. Other operating instructions issued by the Bank with respect to these categories of customers to be followed while issuing/delivering the cards.
- vii. Undelivered cards shall be kept under dual custody.
- viii. Bank will explore the arrangement to deliver the Card directly to customer registered address or to adopt Industry best practices for customer convenience while ensuring security and safety of the Card, not to land in wrong hands.

1.16 ACTIVATION OF CARDS

A. Pre-generated Cards

- i. If branch can demand physical PIN in case of special case from Central office through centmail. then Pre-Gen card will become activate on next working day, if card is issued in the system prior to 4 pm.
- ii. Pre-Gen card is issued with Green PIN option then card will be activated on generation of Green PIN through Our Bank ATM/Mobile Banking/Net Banking,etc)

B. Personalised Cards

- i. Card can be activated by using Green PIN and Physical PIN. If branch select Green PIN option in CBS menu then card will be activated after using Green PIN.
- ii. Implementation of "Green PIN" functionality in CBS, Card is activated on generation of Green PIN.
- iii. Details of Green PIN are given in Chapter-II

AT PRESENT ACTIVE CARD HAS NO LIMITATION OF FIRST TRANSACTION. IT CAN BE USED AT ANY POS/ ECOM OR ATM INCLUDING OTHER BANK'S ATM.

1.17 Management of Cards in case of Deceased Customers

In case of death of the Card Holder, Debit/ATM card held by the deceased card holder should be surrendered by the Joint A/c Holders/Survivors/Legal Heirs of card holders. Branch should Block/Hotlist/Destroy such Card. Closure/continuation of such accounts to be dealt as per Operational guidelines on Saving/Current deposit accounts and guidelines on deceased accounts.

CHAPTER-2

2. ATM PIN MANAGEMENT

2.1 PHYSICAL PIN

- If branch can demand physical PIN in case of special case from Central office through cent mail.
- Card and PIN shall be dispatched separately to the respective branches.
- The Cards and the PINs being security items are to be kept separately under dual control in the branches.

2.2 GREEN PIN

Green PIN is a process of generation PIN digitally and physical PIN will not be generated/sent to customer. Green PIN option will replace physical PIN issuance for Debit Cards. On selecting the Green PIN option, the process of generating Green PIN is to be followed. Functionality to generate Green PIN through ATM, Mobile banking and Internet banking has been made available to the customers to whom new cards are issued in CBS with Green Pin option.

Functionality to generate Green PIN through IVR shall be offered as another mode.

2.3 FORGOT ATM PIN

- I. In case customer forgets his PIN or Branch has not received the PIN of any debit card, new PIN can be generated using Forgot PIN option on the our Bank ATM. The functionality to generate PIN for existing card holders through Mobile Banking/Net Banking/IVR shall be offered as other mode for customer's convenience. PIN generated through Forgot PIN option is by default activated after 48 hours. However, in case of urgency activation of PIN can be done by ANY branch on the same day using CBS menu option. The PIN activated by the branch can be used by customer after 2 hrs.
- II. If Re-PIN option (chargeable @ Rs 50/-) is selected from ATM helpdesk menu available at branch, Physical PIN so generated will be dispatched to the branch within 3 working days through authorized vendor.

2.4 ATM PIN CHANGE

CUSTOMER SHALL BE EDUCATED TO CHANGE THE PIN ON VERY FIRST USAGE OF CARD.

BANK POLICY ON ISSUANCE AND MANAGEMENT OF DEBIT CARDS

Customer can change the PIN Using Central Bank ATM by selecting following options in the main menu of the ATM

1. PIN Change.
2. Enter Current PIN.
3. Enter 4 Digit New PIN
4. Re Enter New PIN to Confirm

Functionality to change PIN through Mobile Banking/Net Banking/CBS/IVR is under development.

2.5 Compulsory PIN change after a certain specified period by Bank or as per Regulatory/Govt/ Guidelines.

CHAPTER-3

3. ENHANCING SECURITY IN CARD TRANSACTION

Over the years, the volume and value of transactions made through debit cards have been increased manifold. To improve user convenience and increase security of card transactions, following measures shall be implemented which will also empower customer/Cardholder to decide its usages at various points (ATM, PoS, On-Line E-Comm Transactions) both domestic and International locations respectively.

3.1 ISSUE OF CARD

At the time of issue / re-issue, all cards (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 take steps to provide cardholders a facility for enabling card not present (domestic and international) transactions, Card Present (International) transactions and Contactless transactions, as per the process outlined as under:

1. Facility to switch on /off and set / modify transaction limits (within the overall card limit, if any, set by Bank) for all types of transactions- domestic and international, at PoS /ATMs/ Online Transactions / contactless transactions/transfer etc.;
2. The above facility on a 24/7 basis through multiple channels- Mobile Application / Internet Banking /ATMs / Interactive Voice Response (IVR); this may also be offered at Branches / Offices.
3. Alerts / information / status etc, through SMS / E-Mail, as and when there is any change in status of the card.

Existing Active Cards which have never been used for online (Card Not Present)/ International / Contactless transactions shall be mandatorily disabled for this purpose and customer will have option to activate the same for the usage.

3.2 ATM CARD CONTROLLER

ATM Card Controller Menu is available in CBS, Mobile Banking and Net Banking. It can be used for enabling/ disabling international transaction. It can also be used for setting the transaction limits for Domestic/International on Debit Card for ATM, POS/E-Com separately. As per RBI mandate, International transactions can only be enabled on a card

BANK POLICY ON ISSUANCE AND MANAGEMENT OF DEBIT CARDS

on written/specific request of card holders/customers. Procedure to be followed for ATM Card Controller.

THE CHANGES MADE IN CARD CONTROLLER ARE TO BE EFFECTIVE IN REAL TIME.

Note: Branches shall educate the customers to use Mobile Banking or Internet Banking for enabling/ disabling International Txn , Blocking of Card etc on their Debit Cards.

3.3 ADDITIONAL FACTOR OF AUTHENTICATION (AFA)

1. A system of providing for additional authentication/validation based on information not visible on the cards for all on-line Card Not Present (CNP) transactions are available with effect from 01.05.2009 and IVR transactions from 01.01.2011.
2. A system of "Online Alerts" to the cardholder for all 'card not present' transactions of the value of Rs. 5,000/ and above.
3. AFA in case of small value card present transactions for a maximum value of Rs 5,000/- per transaction; using Near Field Communication (NFC) contactless technology subject to adherence to EMV standards.
 - a. The limit of Rs.5000/- per transaction will be the limit set across all categories of merchants in the country where such contactless payments will be accepted without PIN; The limit specified Rs.5000/- shall be reviewed on the basis of regulatory guidelines.
 - b. Beyond this transaction limit, the card has to be processed as a contact payment and authentication with PIN (AFA) will be mandatory;
4. Even for transaction values below this limit, the customer may choose to make payment as a contact payment, which has to be facilitated by both issuing and acquiring banks. In other words, customers cannot be compelled to do a contactless payment.
5. Bank may facilitate the customers to set lower per-transaction limits. The responsibility for authorizing the contactless payment based on such card-based limits will lie with the card banks;
6. Suitable velocity checks (i.e., how many such small value transactions will be allowed in a day) shall be put in place by bank as considered appropriate; and
7. The contactless cards shall necessarily be chip cards adhering to EMV payment standard, so as to be acceptable across the existing card acceptance infrastructure which are EMV compliant based on the earlier mandate in this regard.
8. Further, in the interest of customer awareness and protection, the bank shall take following steps:
 - a. to clearly explain to customers about the technology, its use, and risks while issuing such contact less cards;
 - b. to create awareness among customers to look for / identify the "contactless" logo on the card (to distinguish them from other cards) as well as the merchant location / POS terminal (to identify that contactless payments are accepted at that location);
 - c. to clearly indicate to the customers that they can use the card in contactless mode (without PIN authentication) for transactions upto Rs.5000/- in locations where contactless payments are accepted and to make customers aware that they are free

BANK POLICY ON ISSUANCE AND MANAGEMENT OF DEBIT CARDS

to use the same card as a regular chip card (with PIN authentication) at any location irrespective of transaction value; The limit specified Rs.5000/- shall be reviewed on the basis of regulatory guidelines.

- d. to clearly indicate the maximum liability devolving on the customer, if any, at the time of issuance of such cards along with the responsibility of the customer to report the loss of such cards to the bank; and
 - e. to put in place robust mechanism for seamless reporting of lost/stolen cards, which can be accessed through multiple channels (website, phone banking, SMS, IVR etc.).
9. It may, however, be noted that the above relaxations shall not apply to:
- a. ATM transactions irrespective of transaction value; and
 - b. Card Not Present transactions (CNP).

As per RBI mandate, online transactions have to be processed with Two Factor Authentication(2FA).OTP Validation is the second factor of authentication and it is delivered vide text message on customer's mobile phone by issuer Authentication System(IAS).

CHAPTER-4

4. LOST/DAMAGED/STOLEN/COUNTERFEIT/EXPIRED CARDS

Following Procedure to be initiated immediately for Hot listing of card by different channels:

4.1 HOT-LISTING OF CARD:

Hot listing can be done by the branch or by the customers.

4.1.1 Hot listing By Branch

1. Hot listing of card refers to restrict the use of card when cardholder reports of having Lost/Damaged/Stolen card/Not Delivered/Counterfeit Card/Expired/Security Violation, then branch should obtain a written application for hot-listing the card. At times, branch may require hot listing of cards for the reasons e.g. unsatisfactory operations in the account, insolvency of cardholder, dispute among joint account holders, at the direction or orders of Court/Police Authorities, Customer deliberately violating Terms of offer of Card, Customer repeated offence of keeping Card/PIN insecurely etc.
2. If the cardholder is reporting over phone to the branch of having lost his card, then the branch staff should verify his/her request by enquiring about cardholder's details viz. name, card number, account number, address, telephone number, date of birth etc. The details should be confirmed from the branch record to identify the cardholder and to make sure that a right person is making the call for Hot listing of the card. Branch should hotlist the card immediately after credential of customer is identified without waiting for written request but making a proper record of such request, mode of request & Date/Time of such request.
3. On receipt of such request, the branch should enter the details in a register and feed up the required information in the hot-listing the card in CBS Menu.
4. If customer reports the lost card more than 3 times and it is observed the card is lost due to repeated/apparent negligence on the part of the card holder, then re-card/new

BANK POLICY ON ISSUANCE AND MANAGEMENT OF DEBIT CARDS

card shall be preferably issued to such card holders after doing the due diligence by the branch officials.

4.1.2 Hot listing by Customer

Reserve Bank of India has instructed Banks to put in place robust mechanism for seamless reporting of lost/stolen/cards, which can be accessed through multiple channels **on 24*7 basis**. (Website, Phone Banking, Mobile Banking .Net Banking, SMS, IVR etc.).

Bank shall provide multiple channels for reporting unauthorized transaction 24*7(Under Implementation INB and Mobile banking)

A Customer may request for hot listing of a Lost/stolen or fraudulently used card by way of SMS, Calling Toll Free Number, using Mobile and Net Banking and Interacting Voice Response Modes.

1. For Hot listing through SMS on 9967533228 from Registered mobile number in the following format
 - 1.1 LOST<Space><ACCOUNT NO> (Hotlist all cards linked to Account)
 - 1.2 LOST<Space>< Card Number> (Hotlist Specified Card)
 - 1.3 LOST(Hotlist all cards linked to CIF)
2. Call Toll Free number-1800-22-1911
3. Send mail to debitcard@centralbank.co.in.
4. Customer has option to Hotlist the card Through Cent Mobile Application/ Net Banking.
5. In case of the customer has Hot listed the card through SMS/Call Centers/Sending Mail/Cent Mobile Application/Net Banking/IVR, Branches to contact the customer for getting written request for Re-card/Issuance of New Card and immediately/forward the same to Debit card vertical CO.
6. Bank shall immediately send a confirmation to the card holder subsequent to the blocking of a card.

4.2 Auto Renewal of Expired Cards:

Auto-renewal of Expired Debit cards shall be done and new card will be issued against the expired debit card. With the explicit consent of the customer.

CHAPTER-5

5. DE-HOTLISTING/ RE ISSUANCE OF CARD IN PLACE OF LOST/DAMAGED CARD

5.1 DE-HOT LISTING OF CARDS/RE-ISSUANCE OF DAMAGED/LOST CARD:

1. If a card holder reports to the branch of having found his lost card, then the same card can be De-hot listed, provided the customer has not asked for a replacement card. Branch will generate request using Branch Helpdesk Menu ATM_Card Query – De-Hot listing. The card will be De-hot listed on the same day.
2. In case of damaged card, the branch should collect the damaged card from the cardholder, destroy it and maintain a register for destroyed / damaged cards. If same card number is required then existing card number should be entered in re-card screen.

BANK POLICY ON ISSUANCE AND MANAGEMENT OF DEBIT CARDS

3. In case of lost card, it should be replaced by applying for New Card No and New PIN. It must be ensure that the branch should obtain written application from the cardholder for lost card.
4. On receipt of the written application as above, branch shall verify the signature / details from the branch record and it will initiate procedure for issuance of new card by entering the details in CBS Menu for Issuance of Re Card.
5. The replaced card will be of the same variant as the card which was reported lost by the Card holder (For example: Rupay card 652160 when hot listed, Recard for 652160 only should be issued.)

For generating a Re-Card request, first existing card is to be hot listed. A fresh card of same variant can only be issued once existing Card is hot listed. If Pre generated card has been hot listed then personalized card can be issued. Recard process to be initiated without waiting for request from the customer in case of lost/stolen card by blocking/hotlisting the card lost/stolen.

CHAPTER-6

6. ATM HELP DESK MENU

6.1 ATM HELP DESK MENU PURPOSE AND PROCEDURE.

Following functionality /options are available in Branch Help Desk Menu in the CBS for Branch level activities:

1. Account Link-Menu can be used for generation of request of Card linking/ De-linking in the account.
2. Card Hotlist-Menu can be used for generation of request of Card Hot listing if branch has hot listed the card in CBS but still showing Sent for Hot listing.
3. Card De-Hotlist-Menu can be used for generation of request of Card De-Hotlist if a customer report that lost card has been received.
4. Card Repin- Menu can be used for generation of request of Card Repin in the case of Forgot PIN.
5. Pre Generated Card (Not Activated) - Menu can be used for generation of request of Pre Gen Card issued but still showing Pending for activation in CBS.
6. Pre Generated Card (Card Activated in Wrong Account) - Menu can be used for generation of request of wrong card number punched in CBS.

CHAPTER-7

7. NCMC NATIONAL COMMON MOBILITY CARD (NCMC)

With vision of One Card for all Payment systems, Govt. has come out with a National Common Mobility Card (NCMC) to enable seamless payment for low value as well as high value payments across all use cases including travel by different metros and other transport systems across the country, retail shopping and purchases.

Banking sector is now shifting to contact less card system. Government of India has directed all Banks to issue NCMC cards to all new account holders as a part of under one nation one card.

7.1 NCMC

National Common Mobility Card (NCMC) is a Dual Interface Card having contact as well as contactless features. This single card will work as debit card and Wallet.

Minimum two accounts will be linked to the card, one for Debit Card portion and other for wallet portion. On issuance of NCMC card, a virtual account will be opened by the system automatically for wallet part and existing account(s) to be linked for debit card part.

7.1.1 National Common Mobility Card (NCMC) features (for Wallet) portion:

1. Can be used on POS.
2. Supports offline/Online transaction, multi utility card of its kind.
3. PIN is mandatory for all the transactions above the value of Rs.5000/- per transaction
4. Maximum transaction limit for wallet is Rs. 2000/- for the contactless transaction without PIN is Rs.5000/-.

7.1.2 Features of wallet

1. NCMC cards can be issued by Home branch only.
2. No physical contact required with the POS terminal for POS transactions for transaction up to Rs.2000/-.
3. Offline Transaction- For these transactions amount information will be stored in the card itself, and No authentication required (no connectivity required with the switch).
4. Maximum amount can be loaded in the wallet Rs.2000/-.
5. Maximum transaction can be done up to amount loaded in the card/Wallet and no minimum amount Specified for the transaction.
6. In case of card lost, Bank is not responsible for the outstanding balance on the Wallet.

Debit card part of NCMC will be as per variant of card selected. All new Cards to be issued by the Bank shall have NCMC feature including PMJDY Accounts/Basic Bank Accounts, CKCC Accounts & Platinum category of RuPay Cards. In future all card variants will be issued as NCMC after due Certification Process.

CHAPTER-8

8. CASH WITHDRAWAL AT POINT OF SALE (POS) TERMINAL

Initially, cash withdrawal facility using Debit Cards was available only at Automatic Teller Machines (ATMs). The use of debit cards at Point-of-Sale (POS) terminals at different merchant establishments has been steadily increasing. As a further step towards enhancing the customer convenience in using the plastic money, RBI has decided to permit cash withdrawals at POS terminals through Debit Cards issued by Bank. Under the facility of cash withdrawal at PoS terminals, cardholders can withdraw cash using their debit cards and open system prepaid cards issued by banks in India.

- 8.1 Under this facility, a cardholder can withdraw cash up to Rs.2,000/- per day per card in Tier III to VI centres. At Tier I and II centres, the withdrawal limit is Rs.1,000/-

BANK POLICY ON ISSUANCE AND MANAGEMENT OF DEBIT CARDS

per day per card. Based on DFS/ RBI and guidelines limit to be modified by taking approval of the Board.

- 8.2 Customer charges, if any, levied on cash withdrawals shall not exceed 1% of the transaction amount at all centres irrespective of the limit of Rs.1000 / Rs.2000.
- 8.3 The facility is made available at merchant establishments designated by the acquirer banks (i.e. the banks that deploy the PoS terminals) after a process of due diligence. The designated merchant establishments have to clearly indicate / display the availability of this facility along with the charges, if any, payable by the customer
- 8.4 Progressively, as permitted by RBI, the Bank shall introduce withdrawal of Cash at PoS terminals through Unified Payments Interface (UPI) as well as through use of electronic cards that are linked with overdraft facility provided along with Pradhan Mantri Jan Dhan Yojana (PMJDY) accounts.

8.5 CASH WITHDRAWAL AT POINT OF SALE TERMINALS (POS) CASH@POS OR CASH@MERCHANT UNDER EASE

- a. The Department of Financial Services (DFS), Government of India is pushing various reform agenda through EASE in PSU Banks. In order to de-clutter the ATMs, Banks were advised for enabling cash withdrawal at Point of Sale (POS) called as Cash@Merchant or Cash@POS up to Rs.20000/ by transactions.
- b. Board has approved on 18/06/2019 for implementation of cash withdrawal facility and increase in per day transaction limit from Rs.2000/ to Rs.20000/ at Point of Sale terminals to implement EASE agenda.
- c. One time permission for cash withdrawal facility at Point of Sale terminals from the Reserve Bank of India was taken in terms of RBI letter No DBR No.BAPD.729/22. 03. 015/2019-20 dated 25/07/2019.
- d. Bank shall honour Cash payment of its Debit Card presented at selected PoS Terminals (as decided in Bank's own PoS Terminals as well as other Bank/Institutions PoS Terminals) upto a limit of Rs.20, 000/- on following Broad Policy.
 - i. Enablement of Cash@PoS across selective category of Merchants.
 - ii. Increase in per day Cash withdrawal limit to Rs.20, 000/- within 24 hours.
 - iii. Number of transactions on single card or day is restricted to 3.
 - iv. Minimum per day transaction limit is Rs.100/-
 - v. Merchant allowed for Cash@ PoS will not levy any charges to customers for dispensing of Cash.
 - vi. No charges will be levied to our customers (Debit/Prepaid card holders)
 - vii. As per Acquirer, the Bank will be getting 1% of the transaction amount or Rs.10/- per transaction whichever is less as an encouragement to provide such a withdrawal to such customers.
 - viii. Incentives to be paid to Merchants to encourage for providing such a withdrawal facility to customer as per Industry practice on minimum eligible withdrawal amount of Rs.500/ or more.

CHAPTER-9

9. CONFIDENTIALITY

Confidentiality of customer information

Any information relating to customers obtained at the time of opening the account or issuing the card shall not be revealed 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 will be shared. Bank shall ensure strict compliance to the extant legal framework on data protection. Further, in case where the customers give explicit consent for sharing the information with other agencies, Bank shall explicitly state and explain clearly to the customer the full meaning/implications of the disclosure clause. The information sought from customers shall not be of such nature which will violate the provisions of law relating to maintenance of secrecy in the transactions. The card-issuers shall be solely responsible for the correctness or otherwise of the data provided for the purpose. The co-branding non-banking entity shall not be permitted to access any details of customer's accounts that may violate bank's secrecy obligations.

CHAPTER-10

10. COMPLIANCE

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

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

CHAPTER-11

11. CUSTOMER GRIEVANCE

Redressal of grievances

It shall be ensured that an effective mechanism for redressal of customer complaints is put in place and Bank shall give wide publicity through electronic and print media. The name, designation, address and contact number of important executives as well as the Grievance Redressal Officer of the bank shall be displayed on the website. The designated officer shall ensure that grievances of cardholders are redressed promptly without any delay. Specific timelines may be stipulated as per in the Board approved policy for issuance of cards, redressal of grievances and compensation framework. The grievance redressal procedure and the Board approved policy shall be displayed on the website of the bank with a clearly visible link on the homepage. It shall be ensured that call centre staffs are trained adequately to competently handle and escalate, a complaint, if necessary. The Grievance Redressal process shall have a provision for automatic escalation of unresolved complaints from a call center/baselevel to higher authorities.

System of acknowledging customers' complaints for follow up, such as complaint number/docket number, even if the complaints are received on phone, If a complainant does not get satisfactory response, within a maximum period of one month from the date of his lodging the complaint, the customer will have the option to approach the Office of the concerned Banking Ombudsman for redressal of his grievance/s. DPSS guidelines on timeframe for reconciliation of failed transactions at ATMs as amended from time to time shall be complied with in this regard.

CHAPTER-12

12. MONITORING OF CARD TRANSACTION –EFRMS

Securing Card Transaction –Setting of Robust Risk Based Transaction Limit & Monitoring in Switch/Network/ATM Machine/CBS.
(RBI Advisory No 6/2018 dated 13/08/2018).

12.1 Scope of Monitoring Card Transaction

Financial and non-financial transactions are carried out by using Debit card issued by the banks through various switch networks (NFS, RGCS & IRGCS by NPCI/MasterCard international/VISA). These transactions are classified as “ONUS” (our bank card in our ATM), “ISSUER” (our Bank Card in other Bank ATM), “ACQUIRER” (other Bank card in our ATM), “POS” (Point of Sale) & “E-Com” (E-commerce through websites) contact less online and offline transaction. In addition to above, there is Micro ATM transaction, transactions by Bank correspondent.

In recent past, various instances of compromise of ATM Machine/Switch/Eco System across industry have come into light. In one of such cases ATM Switch was compromised and all the validations set at switch level were violated/ bypassed. There are other instances in the industry where the ATM Machines are compromised by installing skimming device (by miscreant) and cloning of the cards by data retrieved through such devices.

There is a need for continuous monitoring of transaction at Bank level, 24/7, to minimize the impact of fraudulent transaction, which included financial, reputation & legal risk and contagion effect in the Industry. Our endeavor is to have robust card transaction system in place.

12.2 RBI advisory

RBI has issued an advisory No: 06/2018 dated 13 August 2018 for Securing Card Transaction –Setting of Robust Risk Based Transaction Limit & Monitoring. They have instructed all banks to implement few measures for securing Card Transaction and setting up of rules, limits commensurate with the risk appetite of the bank and to put in place transaction limits at Card, BIN as well as at bank level. Such limits shall be mandatorily set at the Card network switch itself.

In the advisory following checks have been referred and our suggestions to implement the same:

1. Card-wise/BIN-wise Limits/Bank-wise Limits. - Banks shall put in place transaction limits at Card, BIN as well as at bank level. Such limits shall be mandatorily set at the Card network switch itself.
2. Banks shall put in place transaction control mechanism that has necessary Cap (restrictions on transactions), alerts, if any of the limits set as per the above requirement is breached.

BANK POLICY ON ISSUANCE AND MANAGEMENT OF DEBIT CARDS

Such limits shall be set in terms of volume, value, velocity, geographic location of origination of transaction, etc. Transaction pattern in the past, customer profile, bank's size, etc., are some of the parameters that could be considered to arrive at the risk appetite for setting the limits.

3. Periodic review mechanism of such limits set as per the risk appetite of the bank shall be put in place as per the Board approved policy of the bank.
4. Potential for such attacks appears more probable during weekend, long holidays, as seen from past incidents. Have a mechanism to monitor the breaches, if any, on 24X7 basis, including weekends, long holidays.
5. Have a robust incident response mechanism to mitigate the fraud loss, on account of suspicious transactions, if any. Contact details of nodal officers/persons at the bank/card network operator shall be kept up-to-date.
6. Ensure that card details of the customers are not stored in plain text at bank and its vendor(s) locations, systems and applications. Banks shall also ensure that processing of card details in readable format shall be performed in a secure manner to strictly avoid data leakage of sensitive customer information.
7. Regulatory guidelines related to Debit card and PPI from time to time are to be followed strictly.

12.3 Setting card transaction limits/ validations to mitigate risk in card transactions

1. Card level restriction

- i. There shall be standard limits set for Cash Withdrawal and POS and E-Com card less transactions depending upon Card Types (Basis, Classic, Platinum etc).
- ii. Besides above cash limits, Cardholder shall be allowed to undertake maximum number daily transactions (count) in the cards of 5 (Platinum Variant) & 3 (Classic Variant) within 24 hours cycle (dynamic time).
- iii. As per RBI guidelines, International transactions shall be made available at the request of Customers. Customer will have choice of reducing the per Day Transaction Limits separately for Domestic and International Transaction through Mobile Banking, Net Banking and any other mode like approaching Home Branch by way of Application and through Interactive Voice Response (IVR) as and when such facility is ready.

2. ATM Machine level Limit: Following Machine level Security control Measures for ATM was circulated by RBI /2017-18/206 dated 21.06.2018.

- i. Implementation of security measures such as BIOS password, disabling USB ports, disabling auto-run facility, applying the latest patches of operating system and other software, terminal security solution, time –base admin access, etc.
- ii. Installation of anti-skimming device and whitelisting solution to prevent skimming of card data
- iii. EMV enabled Machine: Card details will be protected from being decrypted and necessary steps shall be taken to install in all ATMs.
- iv. Upgrade all the ATMs with supported versions of Operating System.

3. At Card Network Level

Every Card Network is supposed to have proper Risk Control Measures in place to implement Regulatory guidelines in different geographies. Bank

BANK POLICY ON ISSUANCE AND MANAGEMENT OF DEBIT CARDS

will confirm the same that such measures are in place by all Card Network (MASTER/VISA/NPCI). In view of the varied events to be monitored, a comprehensive Fraud Risk Monitoring Solution is put in place by major players including Card Networks like Visa, Mastercard and NPCI as these entities are the first point of validity check before transaction flow to bank's Switch to CBS and vice-versa.

4. At Card Network / Switch

- i. As mandated in RBI advisory, it is proposed to place appropriate limits at the Card Network level itself in line with RBI Advisory.

The checks suggested to be implemented at Card Networks (Master/ Visa/ Rupay) level or EFRM are as below:

Sr.No	Restrictions	Prudential Limits by Bank	Network Level Controls
1	Bank/Bin wise transaction Restriction on Daily Limit per calendar day	Bin wise transaction Restriction with limit to 150% of average daily on quarterly basis. Separate limit for PMJDY Rupay cards BIN. Separate BIN wise limit for RRB	To set limits at Visa / Master / Rupay Network level. Bank-wise Limit shall be sum total of all Bin limit of all Networks which shall include also of RRB/PMJDY transactions.
2	Velocity Check (Dynamic)	Not more than 3 transactions in 15 minutes of a single card. Not more than 5 transactions in 24 hours	Limits to be set in EFRMS (at present under implementation)
3	International (Present Transaction Limit of Rs 25000 /- Per day)	Minimum 3 hour gap required for same card transaction in different country / Jurisdiction.	Limits to be set in EFRMS (at present under implementation)
4	Domestic	Minimum 1 hour gap required for same card transaction in different cities	Limits to be set in EFRMS (at present under implementation)
5	Merchant group categorization of transaction like Jewelers, Restaurants, Mall/Merchants etc.	To disable / decline during unusual times say 1200 (Mid Night) to 0500 hours for Merchant Establishments	Limits to be set in EFRMS (at present under implementation)
6	Abnormal time limitations	To put restriction up to 2 transaction in odd hours (11.30 PM to 4.30 AM). In case Hospitalization customer may be required during odd times.	Limits to be set in EFRMS (at present under implementation)

BANK POLICY ON ISSUANCE AND MANAGEMENT OF DEBIT CARDS

i. 24/7 monitoring of Transaction Alerts due to breaches of limit from Networks

It is essential to set up a proactive monitoring Cell for 24 x 7 monitoring of alerts which will be provided by Network switches (NPCI, Master card, Visa) through their web based solution as a part of EFRM solution which most entities follow.

OR

Through Bank’s EFRM (Enterprise Fraud Risk Management) solution, monitor transactions 24*7. (Under implementation at present)

4. **Periodic review mechanism** of such limits needs to be put in place. Revision of limits can be considered on half yearly basis or on major incident in the industry. Any breach in Limits/Validations set at network level will decline the transaction and will be escalated in following Hierarchy\Escalation Matrix.

Level	Threshold %	Designation	Action	Alert to be given by
1	125% of Bin-wise Limit Reached	CM-SWITCH , CM SETTLEMENT	Analyse the detail transaction data and report suitably to AGM (ATM), DGM (ATM)	Concerned network (Master/Visa/NPCI) or EFRM to send 1 st level alert
2	150% of Bin-wise Limit Reached	AGM-IT (Switch), AGM ATM CO	Analyse the detail transaction data and report suitably to GM (TBD), GM (IT), and GM (Data Analytics).	Concerned network (Master/Visa/NPCI) or EFRM to send 2 nd level alert

BANK POLICY ON ISSUANCE AND MANAGEMENT OF DEBIT CARDS

3	200% of Bin-wise Limit or Threshold Breached	DGM-ATM, CISO	Take Decision to continue / decline transaction at switch/card network level. Report incident to GM (TBD), GM(IT), ED(In-charge). Competent authority to decide to continue/decline transaction at Switch/card network level will be MD & CEO and in absence of him, Executive Director of the vertical.	Concerned network (Master/Visa/NPCI) or EFRM to send 3 rd level alert
---	--	---------------	---	--

1st level: cmitswitch@centralbank.co.in & cmatmsettlement@centralbank.co.in

2nd level: agmitdlc@centralbank.co.in & agmatmco@centralbank.co.in

3rd level: dgmcards@centralbank.co.in & CISO@centralbank.co.in

Transaction analysis proposed on alert may be analysed seeking following information from EFRMS/ Network/ Switch:

1. Whether transaction threshold on any particular Card network has been breached and take up with the concerned Card network about the breach
2. Whether transaction on any particular Bin is affected
3. Any specific pattern in Geography/Country for fraudulent transactions
4. Nature of transaction ECOM/POS/ATM
5. Random check whether validation like PIN/CVV/Limits are happening at switch
6. A thorough analysis of incidence to start when 150% of limit breached and monitoring to be more Intense as it crosses 150% and more.
7. On reaching 200% threshold, concerned card network can be advised to decline transactions. The limits suggested are daily limits refreshed on the next calendar day at 00 Hrs/12:00 Midnight (24 hours cycle).

A committee comprising of GM (DP & TB), GM IT, GM (OPR), GM-RMD/CRO and CISO which 'will meet immediately after reaching 200%. Threshold breach to decide post decline course of action and further review of threshold limits'.

For Level 1 and Level 2 Threshold breaches, transaction may be allowed to continue till level 3 is reached, however escalation as per above matrix will be followed.

5. Rationale for Threshold limits proposed:

Bin-wise threshold limit is calculated based on successful transaction Half-year data. Per day limit with threshold Cap at 125%, 150% and 200% is advised at which to be intimated to Card Network for setting Limits.

6. Implementation of CBS level restriction

In addition to card level velocity limits, placing restriction of Maximum Number transaction at account level for Debit card transactions shall also be explored which can be implemented through EFRM Solution when it covers CBS Transactions on Real time Basis.

In order to further reduce the risk, it may be considered to restrict Debit limit on various BGL like (POS-Rupay, POS-Mastercard, POS-VISA) Acquiring BGLs etc. at CBS level as well. Per day Debit/ Credit caps shall be set based on the previous transactions volume observed.

CHAPTER-13

13 CUSTOMER PROTECTION –LIMITED LIABILITY IN UNAUTHORISED ELECTRONIC BANKING TRANSACTIONS

Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions by use of Debit Card/Stolen Card/ Lost Card

Bank’s Board approved Policy on “**Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions**” shall be applicable for electronic banking transactions involving face-to-face/ proximity payment transactions (transactions which require the physical payment instrument such as Debit Card to be present at the point of transaction e.g. ATM, POS, Online E-Com etc.)

CHAPTER-14

14. FAILED TRANSACTION (CUSTOMER DISPUTES)

Management of Failed Transaction and Harmonization of Turn Around Time (TAT) for Failed Transactions

1. Large number of Customer Complaints emanates on account of unsuccessful or failed transactions. The failure could be on account of various factors not directly attributable to the customers such as disruptions of communication links, non-availability of Cash in ATMs, Time-Out Sessions, Non-credit to beneficiary account due to various causes.
2. A ‘Failed Transaction’ is a transaction which has not been fully completed due to any reason, not attributable to the customer such as failure in communication links, Non-availability of Cash in an ATM, Time-out of Sessions. Failed Transactions shall also include the credits which could not be effected to the beneficiary account on account of

BANK POLICY ON ISSUANCE AND MANAGEMENT OF DEBIT CARDS

lack of full information or lack of proper information and delay in initiating a reversal transaction.

3. Branch can generate request of Failed ATM/POS terminal transaction using Branch Helpdesk Menu-ATM Reversal-CBI (Card used in our Bank for cash) and Non-CBI ATMs (Our Card used in other Bank ATM and All POS E-Com transactions). Branch shall check the failed E-Com transaction (Transaction routed through ATM Branch code-5002 or Immediate Payment Service Branch code 4982) in CBS. For transactions routed through branch code 4982, mail shall be sent at smtbk2@centralbank.co.in with complete details of the dispute transaction.
4. To have uniform Rectification Actions and Compensation payment to Customers for these failed transactions, Reserve Bank of India has prescribed Turn Around Time (TAT) which shall be as under:
 - i. It may be noted that:
 - The stipulated TAT is the outer limit for resolution of failed transactions; and
 - The bank and other operators/system participants in the process shall endeavor towards quicker resolution of such failed transactions
 - ii. Wherever financial compensation is involved, the same shall be effected to the customer's Account suomotu, without waiting for a complaint or claim from the customer.
 - iii. Customers who do not get the benefit of redress of failure as defined in the TAT, can Register a complaint to the Banking Ombudsman of Reserve Bank of India or Bank's Internal Ombudsman.
 - iv. The TAT and Customer compensation for failed Transactions shall be as under:

Sr. No.	Description of the Incident	Framework for Auto-Reversal and Compensation	
		Timeline for Auto-Reversal	Compensation Payable
1	Automated Teller Machines (ATMs) including Micro-ATMs		
a	Customer's Account is debited but cash not dispensed.	Pro-active reversal (R) of failed transaction within a maximum of T+5 days	Rs.100/- per day if delay is beyond T+5 days, to the credit of account holder.
2	Card Transaction		
a	<u>Card to Card Transfer:</u> Card Account debited but the beneficiary card account not credited.	Transaction to be reversed (R) latest within T+1 day, if credit is not effected to the beneficiary account.	Rs.100/- per day beyond T+1 day.
b	<u>Point of Sale (PoS) (Card Present) including Cash at PoS:</u> Account debited but confirmation not received at merchant location i.e; charge-slip not generated.	Auto-reversal within T+5 days.	Rs.100/- per day of delay beyond T+5 days

BANK POLICY ON ISSUANCE AND MANAGEMENT OF DEBIT CARDS

c	Card Not Present (CNP) (E-Commerce) Account debited but confirmation not received at merchant's system.	Auto-reversal within T+5 days.	Rs.100/- per day of delay beyond T+5 days
3	Prepaid Payment Instruments (PPIs) – Cards/Wallets		
a	<u>On-Us Transaction</u> Beneficiary's PPI not credited. PPI debited but transaction confirmation not received at merchant location.	Reversal effected in Remitter's account within T+1 day.	Rs.100/- per day if delay is beyond T+1 day.
b	<u>Off-Us Transaction</u> The Transaction will ride on UPI, card Network, IMPS etc. as the case may be. The TAT and compensation rule of respective system shall apply.		

Note: T is the day of the transaction and refers to the calendar date.

- If the reversal of Transaction is not completed within TAT and bank is required to pay penalty, it is necessary to examine the reason for delay in reversal within TAT and penalty amount be recovered from responsible party which includes the Agency involved in Reconciliation of ATM/Debit Card Transaction.
- Bank being part of National Financial Switch (NFS) ATM Network, Bank will Abide/follow Dispute Management System as prescribed by NPCI (National Payments Corporation of India) but within RBI prescribed rules in the matter.

CHAPTER-15

15. UNSOLICITED COMMUNICATION

Unsolicited commercial communication

It must be ensured that telemarketers who comply with directions/ regulations 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.

CHAPTER-16

16. LOYALTY PROGRAM-ANMOL REWARDS

Any discounts, cash back, reward points, loyalty points or any other benefits offered by bank shall be provided in a transparent manner including source of such benefit. The accounting process for the same shall be verifiable in the books of the banks. Detailed information regarding these benefits shall be displayed on the website of the Bank and a copy of the same shall also be provided to the card holder.

Cent Rewardz Loyalty Programme for Debit Card holders.

Today's consumers crave instant gratification. An effective loyalty program not only just encourages increased utilization of products, but also it can drive sales of additional products and services. As per independent market research, more than half of all

BANK POLICY ON ISSUANCE AND MANAGEMENT OF DEBIT CARDS

consumers want their Banks to identify discounts for them—ways they can save with their banking provider and with their favorite merchants/retailers. Loyalty Rewardz is an instrument to encourage customers to pay using their bank Debit Card, Digital Banking modes for their favorite merchandise to earn more points and remain loyal with the Bank.

The bank has rolled out the Anmol Rewardz Programme for its Debit Card customers with effect from Aug 2011.

Cent Rewardz is a unique and highly rewarding bank Loyalty Program through which, Bank rewards Bank customer whenever they choose to buy a product or pay for a service using Bank Debit Card. When customer chooses bank's product/service, customer reposes its trust and faith in bank. Cent Rewardz is Central Bank of India's Loyalty Program for its Debit Card customers. Cent Rewardz rewards a customer whenever he/she chooses to buy a product or pay for a service using your Central Bank of India Debit Card.

The objective of "Anmol Rewardz Programme" is to increase usage of our card products for POS/E-Com transactions and thereby improve interchange income and digital transaction by customers. Issuing bank receives interchange income 0.50% to 0.90% (in case of Debit Cards) on usage at POS / E-Com. Another objective is also to encourage our customer's to use our debit cards at our own banks

1. The vendor for management of Royalty Programs shall be selected through proper procedure by following CVC and Bank's internal Policy/Guidelines.
2. At present, a vendor is selected through RFP Process and due approval of Board. The SLA with M/s Loyal Rewardz Management Pvt Ltd is valid up to 31/10/2022.
3. All Central Bank of India Debit Card holders are pre-enrolled into Cent Rewardz, on an individual basis. Each member has only a single membership (CIF based) with Cent Rewardz, irrespective of the number or types of accounts held with the Central Bank of India. However, card holders need to activate the Cent Rewardz account by visiting <https://debit.centrewardz.com/> or via the Cent Rewardz app.
4. Every card holders of Cent Rewardz is eligible to accrue CBOI Points. Customer will earn & accumulate CBOI Points for all spends at Point of Sale (POS) and online purchases using your Central Bank of India Debit Card.

Type	Point(s) for every Rs.100 spent
International Shopping cum Debit Card (MasterCard)	1
Next gen Debit Card (MasterCard)	1
Platinum Debit Card (MasterCard)	1.5
International Shopping cum Debit Card (Maestro)	1.5
International Shopping cum Debit Card (VISA)	1
Platinum Debit Card (VISA)	2
Wonder Debit Card (VISA)	1
Platinum Debit Card (RuPay)	1.5
Shopping cum Debit Card (RuPay)	1

Customers can check Cent Rewardz account balance by visiting- <https://debit.centrewardz.com/> or logging into their account on the Cent Rewardz app.

- Value of 1 Anmol rewardz Point is 25 paise.
Customer can redeem their Rewardz Points for exciting products and services on redemption platform provided by Vendor, such as:
 1. Flight Tickets

BANK POLICY ON ISSUANCE AND MANAGEMENT OF DEBIT CARDS

2. Hotel Bookings
3. Bus Tickets
4. Movie tickets
5. Mobile/DTH Recharge
6. Merchandise (electronics, home and decor, jewelry, sports and lots more)

Debit Card members will need to achieve a threshold of 100 Rewardz Points to be eligible to redeem. Rewardz Points need to be redeemed within three years (36 months excluding the month of accrual) of earning them. Unredeemed points will expire at the end of three years. Additional points earned at Partner Stores are valid for a period of 12 months or 1 year excluding the month of accrual.

CHAPTER-17

17. INSURANCE TO CARD HOLDER

Offer of Free /Chargeable Accident / Health Insurance to Card holders

- a. Bank may consider offering Accident Insurance Cover to its Debit Card Holder (Both Classic and Premium) for promotion of frequent use of Debit Cards at Merchant Establishments/ATM/E-Commerce/Micro ATMs/ Business Correspondences of the Bank at locations within a certain period of usage against accidental injuries caused by all kind of Accidents, for Accidental Death and Permanent Total Disability.
- b. Bank shall extend the Accident Insurance Cover made available by different Card Network with terms and conditions as stipulated by Card Network.
- c. If any Card Network has tie up for any Health Insurance at concessional rates, Bank may offer the same to such Cardholders without any liability on the Bank.
- d. Any offer of Accident Insurance/Air Accident Insurance to Customers shall be implemented after due approval of the Board.
- e. The selection of Vendor for Accident Insurance Cover by the Bank shall be by strictly following CVC and Bank's Procurement Policy.
- f. In case of an insurance cover provided with a card, bank shall ensure that the relevant nomination details are recorded by the Insurance Company and the availability of insurance is included, along with other information. The information shall also include the details regarding the insurance cover, name/address and telephonenumber of the Insurance Company which will handle the claims relating to the insurance cover.

CHAPTER-18

18. CO-BRANDING

RBI has issued guidelines that all persons authorized / approved to issue pre-paid payment instruments are permitted to co-brand such instruments with the name / logos of corporate, financial institution, Government Organizations etc. for whose customers / beneficiaries such instruments are issued. The name of the issuer shall be visible prominently on the payment instrument

18.1 Co-branding arrangement

BANK POLICY ON ISSUANCE AND MANAGEMENT OF DEBIT CARDS

Co-branded debit cards issued by banks will be subject to the following terms and conditions, in addition to the common feature of a Debit Card:

a. Board approved policy

The co-branding arrangement, if any shall be done after obtaining approval of the Board. The policy may specifically address issues pertaining to the various risks associated with such an arrangement including reputation risk and put in place suitable risk mitigation measures. Further, the information relating to revenue sharing between the card-issuer and the co-branding partner entity shall be indicated to the cardholder and also displayed on the website of the card-issuer.

The co-branded debit card shall explicitly indicate that the card has been issued under a co-branding arrangement. The Bank shall not advertise/market the co-branded card as its own product. In all marketing/advertising material, the name of the card-issuer shall be clearly shown. The co-branded card shall prominently bear the branding of the card-issuer.

b. Due diligence

Due Diligence shall be carried out in respect of the non-banking entity with which Bank intend to enter into tie-up for issue of such cards to protect the Bank against the reputation risk, Bank is exposed to in such an arrangement. It will be ensured that in cases where the proposed co-branding partner is a financial entity, it has obtained necessary approvals from its regulator for entering into the co-branding agreement.

c. Outsourcing of activities

The card issuing bank would be liable for all acts of the co-branding partner. The bank will ensure adherence to the guidelines of the Regulator on “Managing Risks and Code of Conduct in outsourcing of financial services by banks” as contained in the circular DBOD.No.BP.40/21.04.158/2006-07 dated November 3, 2006 as amended from time to time.

Card-issuers shall ensure that cash backs, discounts and other offers advertised by a co-branding partner are delivered to the cardholder on time. Card-issuers shall be liable for any delay or non-delivery of the same to the cardholders.

d. Role of non-bank entity

The role of the non-bank entity under the tie-up arrangement shall be limited to marketing/distribution of the cards or providing access to the cardholder for the goods/services that are offered.

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.

CHAPTER-19

19. TOKENIZATION

Tokenization – Card transactions

- i. Continuing the efforts to improve safety and security of card transactions, Reserve Bank of India had permitted card networks for tokenization in card transactions for a specific use case.
- ii. RBI has permitted authorized card payment networks to offer card tokenization services to any token requestor (i.e., third party app provider), subject to the conditions. This permission extends to all use cases / channels [e.g., Near Field Communication (NFC) / Magnetic Secure Transmission (MST) based contactless transactions, in-app payments, QR code-based payments, etc.] or token storage mechanisms (cloud, secure element, trusted execution environment, etc.). Presently, this facility shall be offered through mobile phones / tablets only. Its extension to other devices will be done later based on experience gained.
- iii. All extant instructions of Reserve Bank on safety and security of card transactions, including the mandate for Additional Factor of Authentication (AFA) / PIN entry shall be applicable for tokenized card transactions also.
- iv. All other instructions related to card transactions shall be applicable for tokenized card transactions as well. The ultimate responsibility for the card tokenization services rendered rests with the authorized card networks.
- v. No charges shall be recovered from the customer for availing this service.
- vi. SMS will be sent to the customers on their registered mobile no. for implementation of the Tokenization.

CHAPTER-20

21. E-Mandate on Debit Card:

As per RBI Guidelines, Banks are advised to provide E-Mandate facility to Debit Cardholder to undertake a onetime registration process for repetitive transactions. Bank shall provide such facility with following Terms & Conditions.

A. Applicability

The e-mandate arrangement on cards shall be only for recurring transactions and not for a 'once-only' payment.

B. Registration of card details for e-mandate based recurring transactions

1. A cardholder desirous of opting for e-mandate facility on card shall undertake a one-time registration process, with Additional Factor Authentication (AFA) validation by the issuer. An e-mandate on card for recurring transactions shall be registered only after successful AFA validation, in addition to the normal process required by the issuer.
2. Registration shall be completed only after all requisite information is obtained by the issuer, including the validity period of the e-mandate and other audit trail related requirements. The facility to modify the validity period of the e-mandate at a later stage, if required, shall also be provided for.
3. During the registration process, the cardholder shall be given an option to provide the e-mandate for either a pre-specified fixed value of recurring transaction or for a variable value of the recurring transaction; in the case of the latter, the cardholder shall clearly specify the maximum value of recurring transactions, subject to the overall cap fixed by the RBI (currently ` 2,000/- per transaction).
4. Any modification in existing e-mandate shall entail AFA validation by the issuer.

5. SMS will be sent to the customers on their registered mobile no. for implementation of the E-mandate.

C. Processing of first transaction and subsequent recurring transactions

- i. While processing the first transaction in e-mandate based recurring transaction series, AFA validation shall be performed. If the first transaction is being performed along with the registration of e-mandate, then AFA validation may be combined. All such AFA validation shall be as per extant instructions of the RBI.
- ii. Subsequent recurring transactions shall be performed only for those cards which have been successfully registered and for which the first transaction was successfully authenticated and authorized. These subsequent transactions may be performed without AFA.

D. Pre-transaction notification

- i. As a risk mitigation and customer facilitation measure, the Bank will send a pre-transaction notification to the cardholder, at least 24 hours prior to the actual charge / debit to the card. While registering e-mandate on the card, the cardholder shall be given facility to choose a mode among available options (SMS, email, etc.) for receiving the pre-transaction notification from the issuer in a clear, unambiguous manner and in an understandable language. The facility for changing this mode of receiving pre-transaction notification, shall also be provided to the cardholder.
- ii. The pre-transaction notification shall, at the minimum, inform the cardholder about the name of the merchant, transaction amount, date / time of debit, reference number of transaction/ e-mandate, reason for debit, i.e., e-mandate registered by the cardholder.
- iii. On receipt of the pre-transaction notification, the cardholder shall have the facility to opt-out of that particular transaction or the e-mandate. Any such opt-out shall entail AFA validation by the issuer. On receipt of intimation of such an opt-out, the issuer shall ensure that the particular transaction is not effected / further recurring transactions are not effected (as the case may be). A confirmation intimation to this effect shall be sent to the cardholder.

E. Post-transaction notification

In line with the extant instructions, the Bank shall send post-transaction alert / notification to the cardholder. This notification shall, at the minimum, inform the cardholder about the name of the merchant, transaction amount, date / time of debit, reference number of transaction / e-mandate, reason for debit, i.e., e-mandate registered by the cardholder.

F. Transaction limit and velocity check

1. The cap / limit for e-mandate based recurring transactions without Additional Factor Authentication (AFA) will be Rs. 2,000/- per transaction. The limit specified Rs.2000/- shall be reviewed on the basis of regulatory guidelines. Transactions above this cap shall be subject to AFA as hitherto.
2. The limit of ` 2,000/- per transaction is applicable for all categories of merchants who accept repetitive payments based on such e-mandates.
3. Suitable velocity checks and other risk mitigation procedures shall be put in place.

G. Withdrawal of e-mandate

1. The cardholder shall be provided an online facility to withdraw any e-mandate at any point of time following which no further recurring transactions shall be allowed for

BANK POLICY ON ISSUANCE AND MANAGEMENT OF DEBIT CARDS

the withdrawn e-mandate. (Note: The exception to this will be a pipeline transaction for which pre-transaction notification has already been sent to the cardholder, but the debit has not been communicated to or received by the cardholder, and the e-mandate withdrawal happens during the interregnum.) Information about this facility to withdraw e-mandate at any point of time, shall be clearly communicated to the cardholder at the time of registration and later on whenever felt necessary.

2. The withdrawal of any e-mandate by the cardholder shall entail AFA validation.
3. In respect of withdrawn e-mandate/s, it will be ensured that the merchants on-boarded, delete all details, including payment instrument information.

H. Dispute resolution and grievance redressal

1. An appropriate redress system shall be put in place by the Bank to facilitate the cardholder to lodge grievance/s. Card networks shall also put in place dispute resolution mechanism for resolving these disputes with clear Turn Around Time (TAT).
2. The card networks shall make suitable arrangements to separately identify chargeback/dispute requests in respect of e-mandate based recurring transactions.
3. RBI instructions on limiting liability of customers in unauthorised transactions shall be applicable for such transactions as well.

I. Miscellaneous

It shall be the responsibility of acquirers to ensure compliance by merchants on-boarded by them in respect of all aspects of these instructions.

CHAPTER-21

21. EMI ON DEBIT CARDS.

The EMI on Debit Cards solution provides selected Debit Card holders an option to convert their purchase into a loan repayable in 6/9/12/18 months as per their choice. The loan account is created immediately and confirmation provided to the merchant instantly. The Bank gains in the process by easy building up of loan book (unsecured loan to pre-approved customers), the customer gains by being able to purchase a product which otherwise he would not have been able to purchase, the seller gains by being able to sell high value products.

Product Types/Features

- a. Online EMI on Debit Cards: It will provide EMI facility to pre-approved customers, for purchasing consumer durables online from on-line Retailers (Example: Flipkart, Amazon, any other such retailers of repute).
- b. Offline - Debit Card EMI: This will provide EMI facility to pre-approved customers, for purchasing consumer durables from merchant stores by swiping their Debit Cards. The Offline Debit card EMI facility offered through the POS terminals, the facility shall be extended to the selected Debit Card customers of Bank identified based on regular credits in their account, credit score, etc. 2 types of EMI facilities to be offered as under:
 - i. NO Cost EMI: Here the Brand will pay the Interest to Bank. This will come from those Brands which have high inventory and less demand. These Brands gain by attracting customers and increasing their demand.
 - ii. Bank EMI: Here Bank will charge interest to the customer.

- c. Bank shall explore to provide EMI in Debit Card after proper study of market, risk mitigation and comprehensive policy before introduction. It is being a Retail Loan product, the Ownership and Management shall be vested with Retail Banking Department.

CHAPTER-22

22. SECOND FACTOR AUTHENTICATION /ONE TIME PASSWORD (OTP) FOR CASH WITHDRAWAL

OTP beyond a threshold limit or Transactions for ATM withdrawal

- a) Bank is providing the 2nd factor authentication as OTP (One Time Password) in case of E-Com transaction on the transaction initiated through Net banking/ Mobile banking along with transaction password.
- b) Due to increase of fraud in the ATM card present transactions by cloning of Cards, some major banks have introduced third factor authentication for security of Card Transaction for Onus ATM withdrawal. Bank also introduced such facility to provide the OTP for the Onus ATM withdrawal transaction.
- c) Bank had introduced 2nd Factor Authentication as OTP for Onus cash withdrawal transaction from ATM beyond a threshold limit.
- d) **MD & CEO shall be competent authority for Threshold limit amendment and changes/modification of operational matters, rate of service availed from vendor, service charges levied to customer Subject to Regulatory/Government guidelines, if any.**

CHAPTER-23

23. PERIODIC REVIEW OF DEBIT CARD POLICY & OPERATION

23.1 Annual Review of Policy:

The bank will review the policy on operations/ issue of debit cards/ **card usage**/ on annual basis and same will be placed before Board.

23.2 Half yearly Review of ATM related Complaints

Reserve Bank of India has advised all Scheduled Commercial Banks to submit the quarterly review of Customer Complaints pertaining to ATM failed transactions and resolution thereof within a period of T+5 days (T being the date of transaction). Simultaneously, a review on ATM Transactions, indicating inter alia, the denial of services to the customers at ATM sites, reasons thereof and the action taken to avoid recurrence of such instances has to be submitted to the Board and/or any Sub-Committee of the Board if Board desires so and on its approval, the same shall be submitted to RBI

23.3 Half yearly Review of Performance of ATM Department

ATM Department shall place Review Note on Performance of ATM Department Functioning to Board or any Sub-Committee of the Board as directed by the Board on following areas of performance:

- i. ATM Rollout/Replacement/Closure
- ii. ATM Cash Replenishment by Bank staff/CRA
- iii. ATM Monitoring
- iv. Accounting and Transaction Reconciliation
- v. Fraud Risk Management

23.4 Half yearly Review of Debit Card Business

Debit Card reduces branch workload by migrating customers from Branch to ATMs. It generates Interchange Income through POS & E-com and income through issuance fee / annual fee etc.

The Department shall place Review of the performance of the debit Card business vis-à-vis Targets and Status of execution of business strategy to achieve desired result/ target before the Board and/or to any Sub-Committee of the Board at the direction of the Board.

END OF DOCUMENT