Grievance Redressal Policy of Abhyudaya Bank in respect of Electronic Transactions

I. General

1. Bank has a separate Customer Grievances Redressal Cell (contact number 022-27890636, 022-7890638, email address atmrecon@abhyudayabank.net for quick redressal of customer grievances including those arising from electronic transactions channel. The cell takes utmost care to settle the issues relating to wrong/fraudulent debits and credits through the NPCI Dispute Management Scheme.
2. The customer having a grievance in respect of any of the electronic payments option can approach any branch of Abhyudaya Bank to file a written complaint with details of the matter. The complainant should bring along passbook, and an officially valid ID document, and also a passport-size photograph. The complainant is expected to bring along the debit card with him while lodging the complaint unless it is lost.
3. If in the opinion of the customer, the transaction is suspicious or fraudulent, and he has not already hotlisted the card until then, the card will be immediately hotlisted before the complaint is recorded.
4. In case of a fraudulent debit to or withdrawal from the customer's account, the customer should lodge a police complaint or file FIR. However, filing an FIR by the customer is not a precondition but to lodge police complaint (acknowledgement) is mandatory for any branch of Abhyudaya Bank accepting the complaint.
5. The branch with which the complaint is filed will first assess the issue, record relevant information on complaint letter with signature held and forward the same immediately to the ATM-RECON Dept. Vashi, which at presently working as Customer Grievances Redressal Cell.
6. The Customer Grievances Redressal Cell will be the sole point for further inquiry in respect of status of the complaint.

II. LIABILITY OF A CUSTOMER IN RESPECT OF A PROVEN UNAUTHORISED DEBIT TO HIS ACCOUNT THROUGH ELECTRONIC TRANSACTIONS:

1) Where the customer will have zero liability.

1) Customer will not be liable if the unauthorized transaction occurs in the following events:-
   a) Contributory fraud/ negligence/ deficiency on the part of the bank (irrespective of whether or not the transaction is reported by the customer).
   b) Third party breach where the deficiency lies neither with the bank nor with the customer but lies elsewhere in the system and the customer notifies the bank within **three working days** of receiving the communication from the bank regarding the unauthorized transaction.

2) **Limited liability of a customer-** A customer shall be liable for the loss occurring due to unauthorized transactions in the following cases:-
   a) In cases where the loss is due to negligence by a customer, such as where the customer has shared the payment credentials, the customer will bear the entire loss until he reports the unauthorized transaction to the bank. Any loss occurring after reporting of the unauthorized transaction shall be borne by the bank.

b) In cases where responsibility for the unauthorized electronic banking transaction lies neither with the bank nor with the customer, but lies elsewhere in the system and the customer notifies the bank of such a transaction **within four to seven** working days of receiving a communication of the transaction, the per transaction liability of the customer shall be limited to the transaction value or the amount mentioned in the table below, whichever is lower.

Maximum liability of a customer under "Limited liability of a customer"

TABLE-1

Type of Account	**Maximum Liability (Rs.)**
Basic Saving Bank Deposit Accounts	5000
All other Saving Bank accounts	10000
Current/cash credit/overdraft accounts of MSMEs	
Current Accounts/cash credit/overdraft Accounts of individuals with annual average balance (during 365 days preceding the incidence of fraud) limit upto Rs. 25 lakh	
All other Current/ Cash credit/Overdraft Accounts	25000

c) In case neither the Bank is at fault nor the customer, but the fault lies elsewhere, and the delay in reporting the unauthorized transactions by the customer is more **than seven days** from receiving communication from Bank in respect of the transaction bank's liability will be limited, however bank will extend necessary help in this regard to customer. Abhyudaya Bank will compensate the customer with a maximum of Rs.5,000/- or actual loss whichever is lower, for each such instance. The customer will bear the rest of the loss.

d) **The number of working days mentioned as above,** shall be counted excluding the date of receiving the communication of transaction on customer's registered mobile number/email.

e) **Recognition of deficiency and compensation**

If a card related fraud has been committed in the account of a customer by a member of Bank staff, and the fact thereof has been established, Bank will not only restore the amount; but it will also pay compensation, being interest @ 6%. for the specified period during which the account stood wrongly debited.

f) **Compensation to customer for settlement of disputed ATM transactions:**

Compensation to customer for settlement of disputed ATM transactions will be governed by instructions/guidelines issued by RBI/ NPCI. Accordingly, as per the present RBI/ NPCI instructions, failure to re-credit the customer's account within seven working days of receipt of the complaint shall entail payment of compensation to the customer @ Rs.100/- per day by the issuing bank provided

the claim is lodged with the issuing hank within 30 days of the date of the transaction, and branch has failed to establish the proof of payment/disbursement by ATM.

g) Bank will not be responsible for the loss to the customers due to customer's carelessness in keeping the cards, or, in keeping information of PIN or other security information secret, or, if any information is disclosed by the customer to anyone regarding ATM /DEBIT card. Bank will also not be responsible for the loss to the customer, if the customer acts fraudulently and/or acts without reasonable care which has resulted into loss to him/her. Bank will also not be responsible for the losses arising out of misusing of lost PIN, compromise of passwords or confidential information, suffered by the customer until the time the Bank has been notified and Bank has taken steps to prevent misuse which will be done within 24 hours.

h) **Maximum time for resolution of any complaint to be 90 days from its lodging.**

Notwithstanding anything contained herein above, the Bank shall not pay any compensation in the following cases:-

a) Delays on account of non-functioning of business due to factors beyond the control of the bank: The period covered by such events shall be omitted for calculation of delay etc.
b) Where the issues are sub judice and pending before Courts, Ombudsman, arbitrator, Government.

i) **Force Majeure**

The **Bank shall not be liable** to compensate customers under this Policy if some unforeseen event including but not limited to civil commotion, sabotage, lockout, strike or other labour disturbances, accident, fire, natural disasters or other "Acts of God", war, damage to the Bank's or its correspondent bank(s)' systems, communication channels etc. beyond the control of the Bank, prevents it from performing its obligations within the specified service delivery parameters.

j) **Amendment/Modification of the Policy**

The Bank reserves the right to amend/modify this Policy, as and when deemed fit and proper, at its sole discretion. Bank shall also endeavor, to review the Policy at annual intervals.

Annexure-I

Precautions Advised for Prevention of E-channel Related Frauds

I. Various Electronic channels defined

1) ATM

This is an electronic channel through which the customers can withdraw money 24 hours across the country (under NFS Network). As of now, this is one of the largest networks of Bank ATMs having approximately 2,38,000 ATMs installed. Customers are allowed to withdraw money through ATM of any bank using their ATM card & PIN. Risks under this system come from customers negligently sharing their payment credentials, skimming through which card details are compromised without knowledge of customer, use of ATM card by family members misusing knowledge of PIN, etc. Under these circumstances, customers lose their money. To control this, Bank informs customers from time to time through SMS not to share any payment credentials like card number, PIN and mobile number. Bank also clearly informs customers at the time of issue of card not to keep the PIN along with the card so that no third party can have access to the account for withdrawal. **Bank has provided 24 hours' guards for all its ATMs to avoid possibility of skimming.** Bank has installed CCTV cameras in all ATM cubicles.

2) Rupay Debit Card

This is an indigenous debit card floated by NPCI. Bank has issued only ATM cum Rupay Debit cards to its customers. The risks involved in it and measures for their mitigation are almost same as those mentioned above for ATM, as ATM has to be operated through use of a card. However, a fraudster can also make payment for purchases and pay bills online & at merchant sites through Rupay Debit Cards. To reduce the risk, Bank has put the daily limit for payments through classic cards at Rs. 50,000/- and through platinum cards at Rs.1,00,000/-, so that the customer can come to know (through Bank's SMS for debit) and hotlist the card before a major amount is siphoned off by the fraudster. NPCI also proactively monitors the Rupay card usage and informs the Bank about the compromised cards so that Bank hotlists such cards in time to eliminate or reduce further loss to the customer.

3) Internet Banking

Bank offers facilities only like statement-view and fund-transfer between the customer's own accounts through our Internet Banking. Payment outside our Bank, and outside the customer's own accounts are thus not possible at present.

4) UPI

Unified Payment Interface (UPI) is an initiative by NPCI through which a customer can remit and receive money without exchanging the account details. It also allows the customer to call for a payment by the counter party and on the consent of the latter, money is received by the customer (Pull Transaction). It is an extension of the IMPS.

5) Mobile Banking

Under the Bank's Mobile Banking facility, financial transactions are possible only through a combination of MPIN and TPIN. Bank offers payment options through NPCI driven platform IMPS where the transaction can take place 24x7. At the same time, a customer can opt to use the NEFT route to have a payment transaction within the Bank's NEFT stipulated time. Bank also provides Bill Payments option for most of the utility and telecom billers.

II. SMS Alerts

1. If a customer wants to use Rupay Debit Card for Point of Sale transactions, he/she will have to mention Mobile Number in the Application for Rupay Debit Card. This disclosure is not same as registration for SMS alerts which is a paid service; such registration being in respect of credit/debit transactions in the account other than ATM transactions and PoS transactions.
2. Customer will receive free SMS Alerts on the mobile number disclosed & recorded in respect of the ATM or PoS Transactions.
3. A customer who avoids or declines to mention mobile number in the application for Rupay Debit Card will be able to use the card only for transactions at ATM and not at PoS.
4. While the position in respect of furnishing mobile number is as above, the customers are requested, in their own interest, to furnish mobile number even if they wish to avail themselves of ATM transactions only, as otherwise, Bank will not be able to send them alerts in respect of suspicious transactions, and thus customers' own safety will be compromised.

III. Precautions to be taken by Card holders to Prevent Frauds

The most important aspect for reducing ATM / RuPay debit card related fraud is the customer awareness. Here are a few guidelines to help our customers for not becoming an ATM / RuPay debit card fraud victim:

1. Do not note down the PIN anywhere.
2. Sign the signature panel on your RuPay debit card as soon as you receive.
3. Ensure that PIN changes and cash withdrawal messages are received on your registered mobile. If you have not registered your mobile number, please do the same immediately.
4. If your card is lost / stolen or if you suspect that your card has been duplicated and used fraudulently, you are advised to hotlist the cards immediately. To hotlist cards you can follow any one of the steps mentioned below:
   a) Dial "**9223110011"** from the MOBILE NUMBER registered with our Bank. After 2-3 rings call will be disconnected, the system will **HOTLIST** the card & you will get SMS confirmation for the same.
   b) Customer can directly call 1800223131/ 022-68778900 and register a request to hotlist the card by providing necessary credentials asked by the staff member manning the desk.
   c) If the card holder has availed our mobile banking services, he can hotlist the card by selecting card hotlist option.
   d) Customer can also email to hotlist@abhyudayabank.net for necessary action.

5. Look for suspicious attachments. Criminals often capture information through ATM skimming, using devices that steal information recorded in magnetic strip. At a glance, the skimmer looks just like a regular ATM slot, but it's an attachment that captures ATM card information. To spot a skimmer, look for any attachment which slightly protrudes from the machine and may not he parallel with the inherent grooves. Sometimes, the equipment will even cut off the printed labels on the ATM. The skimmer however cannot obtain PIN number; however, to get that, fraudsters place hidden cameras facing the ATM screen; there may also a bystander (actually the criminal), who may be standing by to inform you that the machine has problems and may offer to help you. In such cases, be cautious. If you do not feel safe, do not use ATM machine.
6. Minimize your time at the ATM. The more time you spend at the ATM, the more vulnerable you are. After the transaction, if you think you are being followed, go to an area with a lot of people and call the police.
7. If possible, avoid using ATMs at night. While robberies are less prevalent than fraud at ATMs; there's still risk, especially at night,
8. Be aware of your surroundings. Before you slide your card into the machine, look around if the area appears safe or if there is anybody who can see the PIN pad. Having the card ready before entering in ATM premises is better than searching for it though the purse at the machine. While you are fumbling with a wallet or purse, you are an easy prey for a thief.
9. If your card is stuck inside an ATM, be suspicious of anyone offering help. Immediately report the incident to the bank.
10. Collect your receipts and card before leaving the place. Ensure you leave the ATM only after completion of your transaction & display of Home Page (Welcome screen).
11. Register your mobile no. with base branch if not done so far for receiving transactional SMS. Further check the transactional SMS from time to time.
12. Never disclose your PIN/CVV to anyone not even to bank officials. Bank officials never enquire an ATM PIN/CVV - whether to process an issue involving ATMs, or to remove a card stuck in the machine.
13. Always change the PIN as soon as you receive it. Preferably, change it frequently. This habit will also help remind you of changing the PIN if you find a suspicious activity.
14. Never provide information via e-mail/phone. Most ATM and Point-of-Sale (PoS) debit frauds originate from `phishing' e-mails. Phishers attempt to obtain information about your bank account by asking for your PIN, account number and personal information. Much like ATM skimming equipment, these e-mails appear legitimate. If you click on a link, you will be sent to a Web site that looks exactly like the one the phishers are imitating. Your Bank does not ask for information through e-mail/phone. If you receive one of these e-mails/calls, inform the Bank.
15. Check your passbook/statements to verify that they properly reflect the amounts you have withdrawn. Report any unauthorized transactions immediately to the bank. Once you have reconciled your statements tear off all receipts. Customer can use toll free no. **18003135235 from your registered mobile no. for latest balance enquiry.**
16. Keep the list of all your card account numbers in a safe and secure place. Include therein telephone numbers of Banks to call if your cards are ever lost or stolen or duplicated.
17. Use ATMs with surveillance cameras and be aware of people and your surroundings. When you enter or exit an ATM in an enclosed area, be sure you close the entry door completely. Do not open locked ATM vestibule doors for others

or allow any unknown persons to enter the ATM area while you are making your transaction. Shield the ATM keypad with your hand or body while entering your PIN. Secure your card and cash after completing your transaction and before exit the ATM area. Count your cash immediately. Your ATM/DEBIT card is like cash, so keep it in a safe place.

18. Lodge a written complaint with the Base Branch in respect of the unauthorized electronic transaction.