Policy on

Unauthorized Electronic Banking Transactions

November 30, 2023

1. Introduction

1.1 IDBI Bank is one of the leading Banks in the country, which deploys state - of – the - art technology to provide world-class services to customers. The Vision Statement of the Bank is "To be the most preferred and trusted Bank enhancing value for all stakeholders".

1.2 As customers are the biggest stakeholders for the Bank, the Vision Statement truly reflects the commitment of the Bank to enhance value to the customers. The Mission Statement of the Bank, inter alia, incorporates the following:

- ✓ Delighting customers with excellent service and comprehensive suite of best-in-class financial solutions
- ✓ Continuing to act in an ethical, transparent and responsible manner, becoming the role model for corporate governance
- ✓ Deploying world class technology, systems and processes to improve business efficiency and exceed customer's expectations

1.3 The Bank understands that one of the important requirements for customer delight is to have ethical and transparent policy in all its dealings. Thus, the Bank acknowledges that the customer is the core constituent of the Bank and every action of the Bank should be aimed at Customer Delight and the Bank should not allow its operations to lead to any monetary loss to the customer.

1.4 Huge increase in Electronic Banking transactions has resulted in improved efficiencies in providing better service to the users of the system. With the increased thrust on financial inclusion and customer protection and considering the surge in customer grievances relating to unauthorized transactions resulting in debits to their accounts/ cards, Reserve Bank of India (RBI) vides its Circular no. RBI/2017-18/5, DBR.No.Leg.BC.78/09.07.005/2017-18 dated July 6, 2017 on "Customer Protection – Limiting Liability of Customers in Unauthorized Electronic Banking Transactions" has advised that each Bank should have a Board approved Policy to cover aspects of customer protection, including the mechanism of creating customer awareness on the risks and responsibilities involved in electronic banking transactions and customer liability in such cases of unauthorized electronic banking transactions. RBI has further instructed that the Policy must be transparent, non-discriminatory and should stipulate the mechanism of compensating the customers for the unauthorized electronic banking transactions and also prescribe the timelines for effecting such compensation.

This Policy is sequel to these instructions.

2. Objectives of the Policy

2.1 To lay down a Policy Frame work for abiding by RBI guidelines on 'Limiting Liability of Customers in Unauthorized Electronic Banking Transaction"

2.2 To ensure transparent and non – discriminatory treatment of customers in matters relating to unauthorized electronic banking transactions

2.3 To create a system whereby the Bank compensates a customer for any Unauthorized Electronic Banking transactions in line with the instructions of RBI

2.4 To enable the Customer to know before or during a relationship, his and Bank's rights and responsibilities in matters relating to 'Electronic Banking Transactions' so that the customer can take informed decision in this regard.

2.5 To ensure that the staff at all levels in the Bank are aware of the policy of the Bank in this regard, so that dealings with the Customer is uniform across geography and types of customers and is based on transparent standards/procedures.

3. Scope of the Policy

3.1 Electronic banking transactions usually cover transactions through the following modes:

i) **Remote / online payment transactions:** These are the transactions that do not require physical payment instruments to be presented at the point of transactions like internet banking, mobile banking, card not present (CNP) transactions, Pre-paid Payment Instruments (PPI), etc.

ii) **Face-to-face / proximity payment transactions:** These are the transactions that require the physical payment instrument such as a card or mobile phone to be present at the point of transaction e.g. ATM, POS, etc.

iii) Any other electronic modes of credit effected from one entity to another currently being used or adopted from time to time.

3.2 This policy covers transactions only through the above modes. The policy excludes electronic banking transactions effected on account of error by a customer (e.g. NEFT carried out to an incorrect payee or for an incorrect amount), transactions done under duress, claims due to opportunity loss, reputation loss, other incidental costs or collateral damage.

4. Applicability

4.1 This Policy is applicable to Customers who maintain Savings Accounts (including Basic Savings Bank Deposit Accounts – BSBD), Current Accounts, Cash Credit Accounts and Overdraft Accounts. This Policy is also applicable to holders of Credit Cards and Pre-paid cards (including Gift Cards) issued by the Bank.

4.2 This Policy is not applicable to non-customer of the bank who uses bank's infrastructure such as ATMs, POS etc. This Policy is also not applicable to entities that are part of eco system such as interchange organizations, Franchisees, Intermediaries, Agencies, Service Partners, Vendors, Merchants, etc.

5. Definition / Explanation of various terms used in the Policy

5.1 **Bank:** Means IDBI Bank

5.2 **Card Not Present transactions (CNP):** These are transactions made and where payment is effected without the card getting presented. Example of such transaction is purchasing goods and services through Merchant's site.

5.3 **Card Present transactions (CP):** These are transactions made and where payment is effected by the card getting presented. Example of such transaction is withdrawal of cash from an ATM, Purchasing goods and service through a POS Machine.

5.4 **Channels of Reporting:** These are Channels available to the customer for reporting unauthorized electronic transactions. The channels are Telephonic, written and using the link provided by the Bank in internet site or elsewhere. Telephonic message can be sent to the Customer Care Centre or any branch of the Bank. Similarly, written reporting can be given to any branch of the Bank.

5.5 **Consent:** Means authorization of a transaction debit either through standing instructions, as per accepted banking practice and regulation, based on account opening process and related matters or based on additional authentication required by the bank such as use of security passwords, input of dynamic password (OTP) or static VBV/ MCSC, challenge questions or use of Card details (CVV/ Expiry date) or any other electronic authentication option provided by the Bank.

5.6 **Customer:** Means an individual or entity that has Savings, Current, Cash Credit and / or Overdraft accounts and also will include holders of Prepaid instruments and cards issued by the Bank.

5.7 **Date and Time of Reporting:** Means Date and Time on which the customer has made his first complaint through any of the channels of Reporting.

5.8 **Electronic Banking Transaction**: Means a transaction done by a customer through Remote / Online or Face to Face / Proximity payment Transaction.

5.9 **Face to Face / Proximity Payment Transactions**: Are transactions which require the physical payment instrument such as a card or mobile phone to be present at the point of transaction e.g. ATM, POS, etc.

5.10 **Loss**: Means the actual financial outgo from customer's account.

5.11 **Negligence of Customer**: Customer shall be found negligent, *inter alia,* if he/she/they has shared payment credentials or account / transaction details viz., Internet banking user ID, PIN, Debit / Credit card PIN/OTP or due to improper protection on customer devices like mobile / laptop / desktop leading to malware / Trojan or Phishing / Vishing Attack. This could also be due to SIM deactivation by the fraudster, also known as SIM Swap/exchange.

5.12 **Number of Days**: is calculated without considering the date of reporting and includes only working days in the Home Branch of the Client.

5.13 **Phishing**: Means the fraudulent practice of sending e mail/message in order to induce a person to reveal personal information such as PIN, OTP, Card Number, and other credentials.

5.14 **Pre-Paid Instruments**: Are documents / cards such as World Currency Cards, Cash Cards, Gift Cards issued by the Bank.

5.15 **Remote / Online Payment Transactions**: Are those which do not require Physical Payment Instruments to be presented at the Point of Transactions. Examples of such transactions are Internet Banking, Mobile Banking, Card Not Present transactions.

5.16 **Reporting**: Means the act of the customer reporting unauthorized electronic banking transaction to the Bank.

5.17 **Shadow Credit**: Means Credit given to the customer but with a lien marked. The customer will not be able to use this amount till the lien is released.

5.18 **Third Party Breach**: Instances such as Application Frauds, Account Takeover, Skimming, Cloning, SIM Swap / exchange, External Frauds, Compromise of

systems such as ATMs, Mail Servers etc., are considered as Third Party Breach where the deficiency lies neither with the Bank nor with Customer.

5.19 **Unauthorized Electronic Transaction**: An Electronic transaction done without the consent of the Customer.

5.20 **Vishing**: Means the fraudulent practice of making phone calls or leaving voice messages purporting in order to induce a person to reveal personal information, such as PIN, OTP, Card number and other credentials.

6. Liability of Customers and Bank under the Policy

Table - I

Third party breach where the deficiency lies neither with the bank nor with the customer but lies elsewhere in the system,			
Reporting by Customer: **Within 3 working days from the date of receipt of communication by the customer intimating the debit**			
S. No	**Type of Account**	**Liability of Customer**	**Shadow Credit to be given**
01	All type of Accounts	Zero	Yes
Reporting by Customer: **between 4 and 7 working days from the date of receipt of communication by the customer intimating the debit**			
02	BSBD Accounts	Rs. 5000/- **Per transaction**. Liability of the customer shall be limited to the Rs. 5000/- or the actual amount of the transaction, whichever is lower	Yes*
03	All other Savings Bank Accounts	Rs. 10000/- **Per transaction.** Liability of the customer shall be limited to Rs. 10000/- or the amount of the transaction, whichever is lower	Yes*
04	Prepaid Instruments and Gift Cards		
05	Current / Cash Credit / Overdraft Accounts of MSME		
06	Current / Cash Credit/ Overdraft Accounts of Individuals with annual average balance (during 365 days preceding the incidence of fraud) / limit up to Rs.25 lakh		
07	Credit cards with limit up to Rs.5 lakh		
08	All Other Current / Cash Credit / Overdraft Accounts	Rs. 25000/-	Yes*

09	Credit Cards with limit above Rs. 5 Lacs	**Per transaction**. Liability of the customer shall be restricted to Rs. 25000/- or the amount of the transaction, whichever is lower	
Reporting by Customer **: Beyond 7 working days to 60 calendar days from the date of receipt of communication by the customer intimating the debit**			
10	All the type of Accounts	Full	No
		However, customer to be compensated up to a limit of Rs. 2,500/- or the transactions value, whichever is lower.	
*Shadow credit shall be restricted to the amount of Bank's Liability			

In cases where the responsibility for the unauthorized electronic banking transaction lies neither with the bank nor with the customer, but lies elsewhere in the system and when there is a delay beyond 60 calendar days in notifying the bank of such a transaction after receiving the communication from the bank, the bank is not liable to compensate the customer.

Table-II

S. No	Unauthorized Transaction occurs in the following events	Liability of Customer	Shadow Credit to be given
01	Contributory fraud/ negligence/ deficiency on the part of the bank (irrespective of whether or not the transaction is reported by the customer).	Zero	Yes
02	If transactions have happened after reporting of unauthorized transaction by the customer through any channels of reporting	Zero	Yes
03	Transactions happened due to negligence of customer, until the customer reports unauthorized transaction.	Full	No

Bank shall not be liable for any liability other than the above amount (such as opportunity loss, loss of reputation, Mental Agony, Incidental expenses) under this Policy.

7. Reversal Timeline for Zero Liability/ Limited Liability of customer

7.1 On being notified by the customer, the bank shall credit (shadow credit) the amount involved in the unauthorized electronic transaction to the customer's account within 10 working days from the date of such notification by the customer. The shadow credit so provided shall be value dated to be as of the date of the unauthorized transaction. Such Shadow credit shall be without waiting for settlement of insurance claim, Police Complaint, if any.

7.2 Further, bank shall ensure that:

- The complaint is resolved and liability of the customer, if any, established within 90 days from the date of receipt of the complaint, and the customer is compensated as per provisions given in the above table

- Where it is unable to resolve the complaint or determine the customer liability, if any, within 90 days, the compensation as prescribed in the above table shall be paid to the customer.
- In case of debit card / bank account, the customer does not suffer loss of interest,

- In case of credit card, the customer does not bear any additional burden of interest.

8. Rights of Customers

8.1 The customer shall have the following rights / entitled to the following services:

i) SMS alerts on valid registered mobile number for all financial electronic debit transactions
ii) Email alerts where applicable and where valid email Id is registered for alerts with the Bank Register complaint through multiple modes
iii) Wherever complaints are lodged online through customer complaints numbers, complaint number and date & time of complaint shall be provided to customers on valid registered email/ mobile number. Written complaint received at Branch shall be acknowledged by the branch in physical form.
iv) Receive compensation in line with this policy document where applicable. This would include getting shadow credit within 10 working days from reporting date and final credit within 90 days of reporting date subject to customer fulfilling obligations detailed herein and limited credit in cases where mentioned in the Policy

9. Responsibilities and obligations of Customers

9.1 Customer shall mandatorily register valid mobile number with the Bank. If there is any change in contact details (mobile/email etc.,), it is the responsibility of the customer to immediately update the same in Bank records. Any unauthorized transaction arising out of delay in updation of contact details by the customer shall be treated as customer liability. Customer should provide all necessary documentation within the stipulated time frame – customer dispute form, proof of transaction success/ failure and copy of police compliant/ FIR and provide copy

of the same to the Bank. Non-submission of documents within stipulated timeframe, due which Bank is unable to conclude the investigation, liability of the unauthorized transactions for such cases shall remain with the customer only.

9.2 Customer shall report the transaction as soon as the unauthorized transaction is observed, so as to avoid any further debits/ financial loss in the account.

9.3 Customer should provide all support, cooperation and documents needed to resolve the complaint within the time frame of 90 days.

9.4 Customer shall co-operate with the Bank's investigating authorities and provide all assistance.

9.5 Customer shall not share sensitive information (such as Debit/Credit Card details & PIN, CVV, Net Banking Id & password, OTP, transaction PIN, challenge questions) with any entity, including bank staff.

9.6 Customer must protect his/her device as per best practices specified on the Bank's website, including updation of latest antivirus software and use of virtual key board etc., on the device (Device includes smart phone, feature phone, laptop, desktop and Tab)

9.7 Customer shall abide by the tips and safeguards mentioned on the Bank's website on Secured Banking available at www.idbi.com >> Customer Care >> Customer Education >> Do's & Don'ts of Banking >> Debit Card and Pin & Internet Banking.

9.8 Customer shall set transaction limits to ensure minimized exposure.

9.9 Customer shall verify transaction details from time to time in his/her bank statement and/or credit card statement and raise query with the bank as soon as possible in case of any mismatch.

9.10 Customer not to click on unknown / unverified links and immediately delete such SMS / email sent by unknown sender to avoid accessing them by mistake in future.

9.11 Unsubscribe to suspicious mails providing links to a bank / e-commerce / search engine website and block the sender's e-mail ID, before deleting such emails.

9.12 Customer shall always go to the official website of your bank / service provider. Carefully verify the website details especially where it requires entering financial credentials. Check for the secure sign (https with a padlock symbol) on the website before entering secure credentials.

9.13 Bank officials / financial institutions / RBI / any genuine entity never ask customers to share confidential information such as username / password / card details / CVV / OTP. Never share these confidential details with anyone, even your own family members, and friends.

9.14 Customer to always remember that there is no need to enter PIN / password anywhere to receive money.

9.15 If UPI or any other app requires you to enter PIN to complete a transaction, it means you will be sending money instead of receiving it.

9.16 Never download an application from any unverified / unknown sources or on being asked/ guided by an unknown person.

9.17 Customer to always obtain the customer care contact details from the official websites of banks / companies.

9.18 Customer shall not call the numbers directly displayed on the search engine results page as these are often camouflaged by fraudsters.

9.19 Customer to also note that customer care numbers are never in the form of mobile numbers.

9.20 Customer shall be cautious while scanning QR code/s using any payment app. QR codes have account details embedded in them to transfer money to a particular account.

9.21 Customer shall never scan any QR code to receive money. Transactions involving receipt of money do not require scanning barcodes / QR codes or entering mobile banking PIN (m-PIN), passwords, etc.

9.22 Customer shall take abundant precaution to prevent his mobile number being swapped with some other SIM by following steps such as (i) Protecting their phone and SIM (ii) Locking phone number with the service provider (iii) Using strong passwords/ security questions (iv) Turn on two-factor-identification (v) Enable biometric authentication of device, etc.

10. Roles and Responsibilities of the Bank

10.1 The Bank shall ensure that the Customer protection policy is available on the Bank's website as well as at Bank's branches for the reference by customers.

10.2 The Bank will regularly educate customers and staff on carrying out safe electronic banking transactions. Information on Safe Banking practices will be made available through campaigns on any or all of the following - website, emails, ATMs, phone banking, net banking, mobile banking. Such information will include rights and obligation of the customers as well as non-disclosure of sensitive information e.g. password, PIN, OTP, date of birth, etc.

10.3 The Bank shall communicate to its customers to register for SMS alerts. The Bank shall send SMS alerts to all valid registered mobile number for all debit electronic banking transactions. The Bank shall also send alert by email where email Id has been registered with the Bank.

10.4 The Bank will enable various modes for reporting of unauthorized transaction by customers. These may include SMS, email, website, toll free number, IVR, Phone Banking or through its branches. The Bank will also enable specific space on its home page where customers can report unauthorized electronic banking transaction.

10.5 The Bank shall respond to customer's notification of unauthorized electronic banking transaction with acknowledgement specifying complaint number, date and time of transaction alert sent and date and time of receipt of customer's notification. On receipt of customer's notification, the Bank will take immediate

steps to prevent further unauthorized electronic banking transactions in the account or card, by blocking all electronic banking channels such as internet banking, mobile banking, UPI payments etc.

10.6 The Bank shall ensure that all such complaints are resolved and liability of customer if any, established within a maximum of 90 days from the date of receipt of complaint.

10.7 During investigation, in case it is detected that the customer has falsely claimed or disputed a valid transaction, the bank reserves its right to take due preventive action of the same including closing the account or blocking card limits, by giving due notice to customer.

10.8 The Bank may restrict customer from conducting electronic banking transaction including ATM transaction in case of non-availability of customer's mobile number.

10.9 This policy should be read in conjunction with Grievance Redressal Policy of the Bank. Clauses from the Bank's Grievance Redressal Policy shall form a part of this policy where not specifically addressed in this policy. The policy is available on the following link:
www.idbibank.in >> Customer Care >> Customer Education >> Regulatory Disclosures >> Policies and Codes.

11. Notifying the Bank / Police Authorities for unauthorized transaction

11.1 Customer to visit 'Customer Care' section on IDBI Bank website and report the unauthorized transaction:

11.2 Customer shall report unauthorized transaction to the Bank at the earliest through any one of the above channels, with basic details such as Customer ID / Credit / Debit Card Number / Account Details, date and time of transaction and amount of transaction, last successful transaction.

11.3 Customer shall Lodge police complaint and maintain copy of the same and furnish police complaint/FIR when sought by bank's authorized personnel.

11.4 Customer shall authorize the bank to block the credit/ debit card/ net banking/ account(s) to reduce likelihood of additional loss.

11.5 Customer shall clearly specify the facilities to be blocked failing which the Bank reserves the right to block all electronic transactions of the customer to protect the customer's interest. Also, revoking these blocks would require explicit consent from customer for each facility.

11.6 Customer shall share relevant documents as needed for investigation or insurance claim viz. cardholder dispute form, copy of passport in case of international transactions and police complaint.

11.7 Customer shall fully co-operate and comply with Bank's reasonable requirements towards investigation and provide details of transaction, customer presence, etc.

11.8 In case, customer does not receive shadow credit or written communication to his / her satisfaction, customer can contact Grievance Redressal Officers (GRO), details of GRO for Banking complaints and Credit Card complaints are available on banks internet web page at Customer Care>> Grievance Redressal>>Banking Complaints & Credit card.

12. Proof of customer liability

12.1 The Bank has a process of second factor authentication for certain electronic transactions, as regulated by the Reserve Bank of India. Bank has onus to prove that all logs / proofs / reports for confirming two factor authentication is available. Any unauthorized electronic banking transaction which has been processed post second factor authentication known only to the customer would be considered as sufficient proof of customer's involvement / consent in effecting the transaction.

13. Force Majeure

13.1 The bank shall not be liable to compensate customers for delaying shadow /actual credit if some unforeseen event (including but not limited to civil commotion, sabotage, lockout, strike or other labour disturbances, accident, fires, natural disasters or other "Acts of God", war, damage to the bank's facilities or of its correspondent bank(s), absence of the usual means of communication or all types of transportation, etc. beyond the control of the bank prevents it from performing its obligations within the specified service delivery parameters.

14. Burden of Proof

14.1 The burden of proving customer liability in case of unauthorized electronic banking transactions shall lie on the bank.

15. Internal Ombudsman

15.1 All customer complaint cases of Unauthorized Electronic Banking Transactions, where real / actual credit is rejected to customer shall be referred to Internal Ombudsman, for further examination before sending/providing the final response to the complainant.

16. Reporting and Monitoring Requirements

16.1 Bank shall report the customer liability cases to the Customer Service Committee of the Board as at the end of every quarter. The reporting shall, *inter alia*, include volume/ number of cases and the aggregate value involved and distribution across various categories of cases viz., card present transactions, card not present transactions, internet banking, mobile banking, ATM transactions, UPI, etc. and also the grievance redressal Mechanism

16.2 The standing Committee on Customer Service shall periodically review the following aspects of Electronic Banking Transactions:

a. appropriate systems and procedures to ensure safety and security of electronic banking transactions carried out by customers;
b. robust and dynamic fraud detection and prevention mechanism;
c. mechanism to assess the risks (for example, gaps in the bank's existing systems) resulting from unauthorized transactions and measure the liabilities arising out of such events;
d. appropriate measures to mitigate the risks and protect themselves against the liabilities arising there from; and
e. a system of continually and repeatedly advising customers on how to protect themselves from electronic banking and payments related fraud.

16.3 All such transactions shall be reviewed by the Internal Audit Department of the Bank.

******

Explanations for the abbreviations used in the Policy

ATM	Automated Teller Machine
CNP	Card Not Present
CP	Card Present
CVV	Card Verification Value (Number printed on the back of the card)
GRO	Grievance Redressal Officer
IVR	Interactive Voice Response
MCSC	Master Card Secure Code
MSME	Marginal, Small and Medium Enterprises
NEFT	National Electronic Funds Transfer
OTP	One Time Password
PIN	Personal Identification Number
POS	Point of Sales
SIM	Subscriber Identity Module
SMS	Short Message Service
VBV	Verified BY Visa

****