INDUSIND BANK LTD.

CUSTOMER PROTECTION POLICY

1. INTRODUCTION

1.1 In the present day scenario of increased use of technology for Banking purposes, it will be our endeavor to offer services to our Customers with best possible utilization of our technology infrastructure and branch network. The Bank has undertaken technological initiatives in payment and settlement systems and qualitative changes in operational systems and processes to improve efficiencies in providing better products and services to the Customers. The "Customer" & "Customer's" hereafter will be referred as "You" & "Yours" respectively.

2. OBJECTIVE OF THE POLICY

2.1 This policy is being framed with the ultimate objective of laying down the criteria for determining your liability in different circumstances and increase awareness of your rights and liabilities.

3. SCOPE

3.1 This document covers the following aspects:

a) Strengthening of systems and procedures
b) Definition of unauthorised transactions
c) Reporting of unauthorized transactions by you to banks
d) Limited Liability of a Customer
e) Reversal Timeline for Zero Liability / Limited Liability of customer
f) Compensation
g) Redressal of Complaints And Grievances

4. STRENGTHENING OF SYSTEMS AND PROCEDURES

4.1 We are providing various options of electronic banking facilities:

a) Remote / online payment transactions (transactions that do not require physical payment instruments to be presented at the point of transactions e.g. internet banking, mobile banking, card not present (CNP) transactions), Pre-paid Payment Instruments (PPI), and
b) Face-to-face / proximity payment transactions (transactions which require the physical payment instrument such as a card or mobile phone to be present at the point of transaction e.g. POS, ATM withdrawals, etc.)

4.2 Further, we have implemented various measures for safe electronic banking transactions, as under:

a) appropriate systems and procedures to ensure safety and security of electronic banking transactions carried out by you;
b) robust and dynamic fraud detection and prevention mechanism;
c) mechanism to assess the risks resulting from unauthorised transactions and measure the liabilities arising out of such events;

d) Send SMS and Emails regularly, advising you on how to protect yourself from electronic banking and payments related fraud.

You are also expected to keep your devices free of any malicious files and apps, by installing a reputed anti-virus program/app and periodically running scans. You are strongly discouraged to jail-break or root your mobile devices for any reason, as it may allow malicious apps to by-pass security controls built in the banking app

5. DEFINITION OF AUTHORISED & UNAUTHORISED TRANSACTIONS

5.1 Transactions are differentiated as "Secured" and "Unsecured" transactions basis the usage of second factor authentication which could be an e-secure code /OTP/Verified by Visa (VBV)/Master Secure Code (MSC) which is known to you only. Hence, transactions can be termed as "authorised" or "unauthorised" as follows:

a) Any transaction that is supported by a second factor authentication including an e-secure code or OTP will be considered as "authorised" transaction.
b) Transactions that do not carry the second factor authentication & also not initiated by you can be termed as "unauthrosied transactions" and fall under the purview of this Policy.
c) In cases where the loss is due to negligence by you, such as where you have shared the payment credentials, you will bear the entire loss until you report the unauthorised transaction to us.
The following types of second factor authentication without which secured transactions cannot be completed, are some examples of such authentications which are known to you only.

OTP/e-secure code: Bank sends OTP/e-secure code to your registered mobile number &/or email id for secured transactions.

Verified by Visa (VBV) or Master Secure Code: These passwords are set by you basis Debit/Credit card details & PIN.

ATM, Debit/Credit Card PIN, Card number, CVV, Expiry date & year, Net Banking login id & password, Mobile Banking MPIN & Transaction password should not be shared.

Examples are indicative, not exhaustive.
Your liability in such cases will be established by the virtue of the fact that Bank has sent OTP to your registered mobile number, VBV & such other passwords generated by you.

Any loss occurring after the reporting of the unauthorised transaction shall be borne by us.

6. REPORTING OF UNAUTHORISED TRANSACTIONS BY YOU TO BANK

6.1 For your convenience to notify us of any unauthorised electronic banking transaction at the earliest after the occurrence of such transaction, we have provided you with 24x7 access through multiple channels i.e. a dedicated toll free no, Contact Centre no, grievance redressal mechanism, IVR etc, all details are available on our website www.indusind.com as mentioned in 9.1.

6.2 We will also ensure that immediate response (including auto response) is sent to you once the loss / fraud reporting is received by us and we shall provide registered complaint number. On receipt of report of an unauthorised transaction from you, we would take immediate steps to prevent further unauthorised transactions in the account by blocking your account/card/mobile banking etc.

6.3 Subsequently, you also need to fill the Customer Dispute Form (CDF) and/or Fraud Reporting Form(s) available at your home branch or on our website www.indusind.com and submit duly filled form along with other applicable document as guided by our officials at your home branch within 5 working days from the date of occurrence of unauthorised transaction/s.

7. LIMITED LIABILITY OF A CUSTOMER

7.1 Zero Liability of a Customer

7.1.1 As instructed by RBI, entitlement to zero liability on you shall arise where the unauthorised transaction occurs in the following events:

a) Contributory fraud / negligence / deficiency on our part once it is established.
b) Third party breach where the deficiency lies neither with us nor with you but lies elsewhere in the system, and you notify us within three working days of receiving the communication from the bank regarding the unauthorised transaction.

7.2 Limited Liability of a Customer

7.2.1 You shall be liable for the loss occurring due to unauthorised transactions in the following cases:

a) In cases where the loss is due to negligence at your end, such as where you have shared the payment credentials like card no, CVV, expiry date, PIN/Password, etc., you will bear the entire loss until you report the unauthorised transaction to us. Any loss occurring after the reporting of the unauthorised transaction shall be borne by us.

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

Table 1

Maximum Liability of a Customer under (paragraph 6.2.1.b)

	Type of Account	**Maximum liability (₹)**
*	Basic Savings Bank Deposit Accounts (BSBD Accounts)	5,000
*	All other Savings Bank accounts	10,000
*	Pre-paid Payment Instruments and Gift Cards	
*	Current / Cash Credit / Overdraft Accounts of MSMEs	
*	Current Accounts / Cash Credit / Overdraft Accounts of Individuals with annual average balance (during 365 days preceding the incidence of fraud) / limit up to Rs.25 lakh	

*	Credit cards with limit up to Rs.5 lakh	
*	All other Current / Cash Credit / Overdraft Accounts	25,000
*	Credit cards with limit above Rs.5 lakh	

7.2.2 Further, if the delay in reporting is beyond seven working days, you shall be responsible for the entire liability.

7.2.3 Your Overall liability in third party breaches, as detailed in paragraph 6.1.1.b and 6.2.1.b, where the deficiency lies neither with us nor with you but lies elsewhere in the system, is summarized in the Table 2:

Table 2	
Summary of Customer's Liability	
Time taken to report the fraudulent transaction from the date of receiving the communication	**Customer's liability (₹)**
Within 3 working days	Zero liability
Within 4 to 7 working days	The transaction value or the amount mentioned in Table 1, whichever is lower
Beyond 7 working days	100%

7.2.4 The number of working days mentioned in Table 2 shall be counted as per the working schedule of your home branch where you maintain your account excluding the date of receiving the communication.

8. REVERSAL TIMELINE FOR ZERO LIABILITY / LIMITED LIABILITY OF CUSTOMER

8.1 Once you have notified us of the unauthorised electronic transaction as per the liability structure discussed at Table 1 and Table 2 above, we shall credit (shadow reversal) the amount involved in the unauthorised electronic transaction to your account within 10 working days from the date of such notification & submission of documents as listed in 8.4 below. A shadow credit is the credit given in your account by us with a restriction on usage of the funds. You will not be able to utilize this fund till we convert it from shadow credit to clear credit. The credit shall be value dated to be as of the date of the unauthorised transaction.

8.2 Further, we shall ensure that:

a) complaint is resolved and your liability, if any, established within 90 days from the date of receipt of the complaint.
b) where we are unable to resolve the complaint or determine your liability, if any, within 90 days, the shadow credit will be converted to clear credit.
c) in case of debit card / bank account, you do not suffer loss of interest, and in case of credit card, you do not bear any additional burden of interest.

8.3 If, after the shadow credit, your liability is established the Bank shall reverse the credit by debit to your account within 90 days from the date of your complaint.

8.4 Shadow credit will be accorded only after you submit below documents at our branch. You need to visit our branch and submit below listed documents to enable us to claim the amount from our insurance company:

Sr. no	Document Required
1	Claim form duly filled & signed by you (form available with branch)
2	FIR at loss location with stamp & attestation of concerned police station
4	Dispute letter given by you to us
5	Physical scan copy of Debit Card (front/back)
6	Complete passport copy (all pages of passport) – in case fraudulent transaction occurred overseas
7	If claim amount is > 1lakh, attested copy of Pan Card , Address Proof & 2 latest Passport colour photos
8	Cancelled cheque copy or NEFT mandate form duly filled in by you to enable Insurance company to credit your account directly.

9. REDRESSAL OF COMPLAINTS AND GRIEVANCES

9.1 You can use any one of the below channels & contact points for reporting unauthorised transactions and lodging complaint:

Mode	Contact details
Home Branch	Please visit your home branch where you maintain your account and report the incident
Contact Centre nos with IVR facility available (24*7) for you.	General Banking - (In India) : 1860 500 5004 / 1800 209 0061 / 022 44066666 General Banking - (Outside India) : 1860 500 5004 / 022 44066666 Exclusive Banking and Credit card customer - (India and Outside India) : 1860 267 7777 / 022 4220 7777
Website	You can also access the Complaint form available on our Bank's website and use it for reporting unauthorized transactions.
Email	You can write to us at reachus@indusind.com for lodging any grievance or reporting unauthorized transactions. You can also write to us at premium.care@indusind.com for lodging any grievance or reporting unauthorized transactions related to your Credit card.

Simultaneously, you can use the following channels / options for blocking your cards instantly:

SMS: If you hold only one Debit Card, you can send a SMS to 9223512966 from the registered mobile number with the Keyword **LOST** followed by your Date of Birth to block the lost debit card. If you holds Credit card, you can send a SMS to 5676757 from the registered mobile number with the keyword **BLOCK** followed by the last four digit of your credit card number, to block the credit card.

You can also hotlist your credit and debit card on IndusMobile and IndusNet instantly.

9.2 In case, you do not receive the shadow credit or written communication to your satisfaction, within 10 working days from the date of reporting unauthorised transactions, you can write to our bank officials as under

Particulars	Write to
In case, shadow credit is not received within 10 working days of reporting of the unauthorised transactions, **Banking Customers** may write **to Head - Customer Care** and **Credit Card Customers** may write to **Head - Cards Services**	**Mr. Vishal Anand** Head - Customer Care OPUS Center, 47, Central Road, Opp. Tunga Paradise Hotel, MIDC, Andheri (East), Mumbai 400093 **Ms. Tuesy Chhatwal** Head - Cards Services IndusInd Bank Ltd. Datamatics, Bldg No 3 (Ground Floor), Plot No – B-5, Part B Cross lane, MIDC, Andheri (East), Mumbai – 400093
In case, you do not receive a response from Head – Card Services or Head Customer Care within **7 working days,** you may call/ write to the **Nodal Officer** at the address/email/contact number provided herewith.	**Ms. Anita Verghese** **Executive Vice President & Principal Nodal Officer** IndusInd Bank Ltd. 701/801 Solitaire Corporate Park, 167, Guru Hargovindji Marg, Andheri-Ghatkopar Link Road, Chakala, Andheri (East), Mumbai - 400 093 E-mail: nodal.officer@indusind.com Tel. No.: (022) 6641 2200, 6641 2319 Fax: (022) 6641 2318

9.3 Nodal Officer

9.3.1 Our Nodal Officer will endeavor to resolve the issue to the Complainant's satisfaction within 7 working days. In case, the complaint needs more time to examine, the complaint shall be acknowledged by explaining the need for more time to respond.

9.3.2 All unresolved cases will be referred to Internal Ombudsman for further examination before sending the final response to the complainant.

9.4 Internal Ombudsman (IO)

9.4.1 IO will examine such complaints for independent review.

9.4.2 The final response to you for such cases will be sent by the Bank only after examination by IO and the fact that the response has IO concurrence will be mentioned in the response to you.

9.4.3 If the complaint is not resolved within 30 days from the lodgment of the complaint or if the complainant is not satisfied with the response, he/she can approach the office of the Banking Ombudsman.

9.4.4 We have displayed on our website and in all our branches a Notice explaining that we are covered under the Banking Ombudsman Scheme 2006 as amended upto July 01, 2017 of the Reserve Bank of India. The contact details of Regional Manager, Bank's Nodal Officer and Banking Ombudsman are prominently displayed on the notice board at branch. A copy of the Scheme is available at the Branches and availability of the Scheme is also displayed at the Branch Notice Board. The Scheme is also displayed on Bank's website. If a complainant

has any matter that he/she would like to report to the Banking Ombudsman, he / she may contact the Branch Head for details.

Please mention your full name, address and other contact particulars in the complaint letter.

Anonymous complaints will not be entertained.

****