

American Express Banking Corp. Policy

Policy Reference & Name	:	AEBC 79 Customer Relations Policy
Effective Date	:	August 25, 2026
Policy Sponsor	:	VP CFRO – AEBC, India
Policy Owner	:	Customer Service Head– AEBC, India
Policy Type	:	Operating Policy
Approval Requirement	:	AEBC CEC – Approval AEBC ORMC – Review Sponsor – Approval
Policy Scope	:	American Express Banking Corp. Policy
Next Scheduled Review	:	August 2027
Changes to Previous Policy	:	This is the first iteration of this policy

Table of Contents

1.0. OVERVIEW AND PURPOSE	3
2.0. SCOPE.....	3
3.0. ROLES AND RESPONSIBILITIES.....	3-4
4.0. POLICY REQUIREMENTS.....	4-8
5.0. POLICY EXCEPTION / CONFLICT / INTERPRETATION RESOLUTION.....	8
6.0. POLICY APPROVAL REQUIREMENTS.....	9
7.0. ENFORCEMENT OF ISSUED POLICIES AND PROCEDURES.....	9
8.0. POLICYIMPLEMENTATION.....	10
9.0. RELATED POLICIES, GUIDELINES AND SUPPORTING DOCUMENTS.....	10
10.0. REVISION HISTORY.....	10

1.0 OVERVIEW AND PURPOSE

Taking into account the risks arising out of unauthorised debits to customer accounts owing to customer negligence / bank negligence / banking system frauds / third party breaches, American Express Business Corp., India (“the Bank” / “AEBC”) needs to clearly define the rights and obligations of customers in case of unauthorised transactions in specified scenarios. The Bank needs to ensure that the systems and procedures are designed to make customers feel safe about carrying out electronic banking transactions.

2.0 SCOPE

Policy covers 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 unauthorised electronic banking transactions. The policy must be transparent, non-discriminatory and stipulates the mechanism of compensating the customers for the unauthorised electronic banking transactions and also prescribes the timelines for effecting such compensation keeping in view the below instructions -

- (1) a complaint is resolved and liability of the customer, if any, established within such time, as may be specified in the Bank’s Board approved policy, but not exceeding 90 days from the date of receipt of the complaint, and the customer is compensated as per provisions in section 4.1;
- (2) where it is unable to resolve the complaint or determine the customer liability, if any, within 90 days, the compensation as prescribed in section 4.1 is paid to the customer; and
- (3) in case of credit card, the customer does not bear any additional burden of interest.

The policy should be displayed on the bank’s website along with the details of grievance handling/ escalation procedure. The instructions contained in this section shall be incorporated in the policy.

3.0 ROLES AND RESPONSIBILITIES

Country Executive Committee (“CEC”)	Approve the Policy, and any amendments to the existing Policy at least annually to consider its continuing relevance and applicability.
Operational Risk Management Committee (ORMC)	Review the Policy at least annually and if required suggest any amendments to the existing Policy to ensure its continuing relevance and applicability.
Operations (Fraud)	The Operations (Fraud) Team will be responsible for the below: • On being notified by the customer, credit (shadow reversal) the amount involved in the unauthorised electronic transaction to the customer’s account within 10 working days from the date of such notification by the customer. • Ensure that: (i) a complaint is resolved and liability of the customer, if any, established within such time, as may be specified in the bank’s Board approved policy, but not exceeding 90 days from the date of receipt of the complaint, and the customer is compensated as per provisions of paragraphs (f) to 6 (ii) (i) above; (ii) where it is unable to resolve the complaint or determine the customer liability, if any, within 90 days, the compensation as prescribed in paragraphs (f) to (i) is paid to the customer; and

	(iii) in case of credit card, the customer does not bear any additional burden of interest. The team shall put in place a suitable mechanism and structure for the reporting of the customer liability cases to the Board or Standing Committee on Customer Service. 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, etc.
--	--

4.0 POLICY REQUIREMENTS

4.1 Unauthorised Electronic Banking Transaction (UEBTs):

- a) **Definition:** An unauthorised electronic banking transaction refers to any transaction resulting in a debit to a customer's account or payment instrument that is carried out without the explicit consent or knowledge of the customer, including those arising from fraud, third-party breaches, or system deficiencies across remote/online or face-to-face electronic payment channels.
- b) **Zero Liability:** A customer shall have zero liability where the unauthorised transaction occurs due to fraud, negligence, or deficiency on the part of the bank, or in cases of third-party breach where the customer notifies the bank within three working days of receiving the transaction alert.
- c) **Limited Liability:** A customer's liability shall be limited where the unauthorised transaction is due to factors beyond both the bank's and customer's control, and the customer reports the transaction with a delay of four to seven working days; liability is capped as per regulatory thresholds.
- d) **Full Liability:** A customer shall bear the full liability where the loss arises due to the customer's negligence (e.g., sharing of credentials) until such time the unauthorised transaction is reported to the bank; any loss occurring after reporting is borne by the bank.
- e) **Reporting of unauthorised transactions by customers to the Bank:** Bank must ask its customers to mandatorily register for SMS alerts and wherever available register for e-mail alerts, for electronic banking transactions. The SMS alerts shall mandatorily be sent to the customers, while email alerts may be sent, wherever registered. The customers must be advised to notify their bank of any unauthorised electronic banking transaction at the earliest after the occurrence of such transaction, and informed that the longer the time taken to notify the bank, the higher will be the risk of loss to the bank/ customer. To facilitate this, Bank must provide customers with 24x7 access through multiple channels (at a minimum, via website, phone banking, SMS, e-mail, IVR, a dedicated toll-free helpline, reporting to Bank, etc.) for reporting unauthorised transactions that have taken place and/ or loss or theft of payment instrument such as card, etc. Bank shall also enable customers to instantly respond by "Reply" to the SMS and e-mail alerts and the customers should not be required to search for a web page or an e-mail address to notify the objection, if any. Further, a direct link for lodging the complaints, with specific option to report unauthorised electronic transactions shall be provided by Bank on home page of their website. The loss/ fraud reporting system shall also ensure that immediate response (including auto response) is sent to the customers acknowledging the complaint along with the registered complaint number. The communication systems used by Bank to send alerts and receive their responses thereto must record the

time and date of delivery of the message and receipt of customer's response, if any, to them. This shall be important in determining the extent of a customer's liability. The Bank may not offer facility of electronic transactions, other than ATM cash withdrawals, to customers who do not provide mobile numbers to the bank. On receipt of report of an unauthorised transaction from the customer, Bank must take immediate steps to prevent further unauthorised transactions in the account.

f) Limited Liability of a Customer:

1) **Zero Liability of a Customer:** A customer's entitlement to zero liability shall arise where the unauthorised transaction occurs in the following events:

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

2) **Limited Liability of a Customer:** A customer shall be liable for the loss occurring due to unauthorised transactions in the following cases:

- (i) In cases where the loss is due to negligence by a customer, such as where he has shared the payment credentials, the customer will bear the entire loss until he reports the unauthorised transaction to the bank. Any loss occurring after the reporting of the unauthorised transaction shall be borne by the bank.
- (ii) In cases where the responsibility for the unauthorised electronic banking transaction lies neither with the bank nor with the customer, but lies elsewhere in the system and when there is a delay (of four to seven working days after receiving the communication from the bank) on the part of the customer in notifying the bank of such a transaction, the per transaction liability of the customer shall be limited to the transaction value or the amount mentioned in Table under 4.1 (h) , whichever is lower.

g) Maximum Liability of a Customer:

Type of Account	Maximum liability (₹)
Credit cards with limit up to Rs.5 lakh	10,000
Credit cards with limit above Rs.5 lakh	25,000

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

Overall liability of the customer in third party breaches, as detailed in paragraph f (1) and paragraph f (2) above, where the deficiency lies neither with the bank nor with the customer but lies elsewhere in the system, is summarized as below:

h) **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	This is a case of Customer negligence thus full customer liability

The number of working days mentioned in the above table shall be counted as per the working schedule of the Bank excluding the date of receiving the communication.

- i) **Reversal Timeline for Zero Liability/ Limited Liability of customer:** On being notified by the customer, the bank shall credit (shadow reversal) the amount involved in the unauthorised electronic transaction to the customer's account within 10 working days from the date of such notification by the customer. Bank may also at its discretion decide to waive off any customer liability in case of unauthorised electronic banking transactions even in cases of customer negligence. The credit, if any, shall be value dated to be as of the date of the unauthorised transaction.

Refer to [AEBC 59 Customer Compensation Policy](#)

Further, Bank shall ensure that:

- (iv) a complaint is resolved and liability of the customer, if any, established within such time, as may be specified in the bank's Board approved policy, but not exceeding 90 days from the date of receipt of the complaint, and the customer is compensated as per provisions of paragraphs (f) to 6 (ii) (i) above;
 - (v) where it is unable to resolve the complaint or determine the customer liability, if any, within 90 days, the compensation as prescribed in paragraphs (f) to (i) is paid to the customer; and
 - (vi) in case of credit card, the customer does not bear any additional burden of interest.
- j) **Burden of Proof:** The burden of proving customer liability in case of unauthorised electronic banking transactions shall lie on the Bank.
- k) **Reporting and Monitoring Requirements:** The bank shall put in place a suitable mechanism and structure for the reporting of the customer liability cases to the Board or Standing Committee on Customer Service. 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, etc. The Board in the bank shall periodically review the unauthorised electronic banking transactions reported by customers or otherwise, as also the action taken thereon, the functioning of the grievance redressal mechanism and take appropriate measures to improve the systems and procedures. Such transactions shall be reviewed by the bank's internal auditors.

4.2 Educates customers about their responsibilities:

Bank to engage in creating an environment of customer awareness on the risks and responsibilities involved in electronic banking transactions and customer liability in such cases of unauthorised electronic banking transactions through various electronic channels such as SMS, emails, notifications on website, etc. For the purpose, Bank should conduct periodic fraud awareness campaigns, reporting guidance and customer education on safe electronic banking practices.

4.3 Grievance and escalation process:

Grievances Redressal Escalation – The various channels through which our customers can contact us for any assistance or redressal of their grievances are listed below:

Level 1: American Express Helpline

Should you require any assistance, you can contact us below:

Call Us: Call us 24x7 (toll-free) at 1800 419 3646 (number also available at the back of your Card).

Chat with us: via Mobile Messaging (24x7 support) by clicking on the Chat icon on the Amex App.

Connect at Branch: You can file a complaint in the complaint register available at our branch.

Connect Online: Complaint form available on our website

Level 2: Manager - Executive Correspondence Unit

If you are not satisfied with the response received at our helpline, you can escalate your grievance at the below-mentioned address.

Please note that the contact information below is purely for grievance redressal escalation. For general inquiries, customers may reach out to us through our customer service channels (Contact Us)

Call Us: +91 124 6702523 (Monday to Friday 8:30 am to 5:00 pm)

Email Us: Manager-Customerservicesindia@aexp.com

Write to Us: American Express Banking Corp.

Cyber City, Tower C, DLF Bldg. No. 8

Sector 25, DLF City Phase II

Gurgaon – 122002 (Haryana)

Level 3: Head of Customer Service

For further escalation of grievances:

Call Us: +91 124 6702527 (Monday to Friday, 8:30 am to 5:00 pm)

Email Us: Head-Customerservicesindia@aexp.com

Write to Us: Ms. Priyameet Kaur

American Express Banking Corp.
Cyber City, Tower C, DLF Bldg. No. 8
Sector 25, DLF City Phase II
Gurgaon – 122002 (Haryana)

Level 4: Nodal Officer

Call Us: +91 124 6702386 (Monday to Friday, 8:30 am to 5:00 pm)

Email Us: AEBCNodalOfficer@aexp.com

Write to Us: Ms. Garima Chandel

American Express Banking Corp.
Cyber City, Tower "C", DLF Bldg. No. 8
Sector 25, DLF City Phase II
Gurgaon – 122002 (Haryana)

Level 5: Principal Nodal Officer

Call Us: +91 124 6702638 (Monday to Friday, 8:30 am to 5:00 pm)

Email Us: pnoindia@aexp.com

Write to Us: Mr. Ashish Pandey

American Express Banking Corp.
Cyber City, Tower "C", DLF Bldg. No. 8
Sector 25, DLF City Phase II
Gurgaon – 122002 (Haryana)

Level 6: Banking Ombudsman Scheme

If you are not satisfied with redressal of the complaint provided by the Bank or if you have not received a response from the Bank within one month (i.e., 30 days) of logging a complaint with us, you may approach the Office of the RBI Ombudsman for grievance redressal. The complaint can be made to the Office of the Banking Ombudsman with the complete transaction and other requisite details. (The 30-day period will be reckoned after all the necessary information sought from the customer has been received) [Click here](#) for salient features / details on the Integrated Banking Ombudsman Scheme.

Integrated Banking Ombudsman Contact Details

Toll Free Number : 14448 (9:30 am to 5:15 pm)

Link to log a complaint : <https://cms.rbi.org.in>

Address : Centralised receipt and Processing Centre (CRPC), Reserve Bank of India, 4th Floor, Sector 17, Chandigarh 160017

You can also file a complaint in the complaint register available at our branch or the Complaint Form available on our website.

For any complaints related to mis-selling or harassment by the representative of the Bank, customer can raise a complaint through:

Email: Manager-Customerservicesindia@aexp.com

Telephone No. 0124-6702523 (Monday to Friday 8:30 to 5:00 pm)

If you are not satisfied with redressal of the complaint provided by Bank or if you have not received a response from Bank within prescribed timeline, you may also join the Customer Meeting and/or you can also meet us in person or join online to express your grievance on the monthly “Grievance Redressal Day”.

For more details, you can click here - https://www.americanexpress.com/in/company/voice-of-customer.html?inav=en_in_footer_company_information_customer_service_comittee

5.0 Policy Exception/Conflict /Interpretation Resolution

It is the responsibility of American Express Banking Corp. colleagues subject to this policy to escalate to the Sponsor, interpretation issues, or policy gaps/inadequacies associated with AEBC Policies. The Owner may provide policy interpretation and guidance as needed; but when potential issues have contradictory interpretations for existing practices the Owner should facilitate a discussion with the Sponsor to develop appropriate resolution plans.

All requests for exceptions to policies, or the related procedures, must be formally approved by the Policy Approvers, as outlined in Section 6 of this Policy. Exception requests must include an Action Plan and Rationale and must carry either an Expiration or Review Date. Any identified exception to a policy that has not yet been approved must be escalated to the respective Sponsor immediately. Approved policy exceptions do not constitute policy non-compliance.

It is the responsibility of the Owner to define their Policy’s Exception / Conflict / Interpretation Resolution Requirements and will maintain documentation of all exceptions and will regularly review these exceptions to assess whether a policy change is required and to ensure ongoing policy compliance.

The General Counsel's Organization is responsible for resolving questions about the alignment of this policy with laws and regulations.

The AEBC CRO retains the authority to resolve conflicts surrounding policy framework related matters only, with appropriate senior leadership, should they arise.

6.0 Policy Approval Requirements

This policy must be reviewed and approved by the AEBC CEC at least annually. Additional reviews could be triggered by major changes in corporate strategy, the regulatory environment or financial market conditions. Prior to each review by the AEBC CEC this policy, and any proposed changes in this policy, should be reviewed by:

Approval Level

AEBC CEC – Approval

AEBC ORMC – Review

Sponsor – Approval

7.0 Enforcement Of Issued Policies And Procedures

All employees, agents, representatives, advisers, contractors, affiliates and third party vendors of AEBC are responsible for complying with applicable official policy, procedure, or a standard/program. AEBC Senior Management and Officers are ultimately responsible for ensuring adherence to policy within AEBC. Internal auditors and control groups, as applicable, will review compliance with policy and procedure. Noncompliance with issued policies or procedures is a breach of the terms of employment and may lead to disciplinary actions which may include termination of employment, or third-party agreement.

Noncompliance with issued policies or procedures is a breach of the terms of employment and may lead to disciplinary actions which may include termination of employment, or third-party agreement.

AEBC Policies do not take precedence over local law, yet still must be aligned to management policy requirements.

8.0 Policy Implementation

This Policy is expected to operate in conjunction with other associated Risk and Operating policies which are listed in Related policies, Regulatory Guidelines & Supporting Documents – Section 10. In the case of changes to referenced risk policies and frameworks, subsequent updates of this Policy will harmonize requirements across associated policies and evaluate policy ownership across the relevant associated policies.

9.0 Related Policies, Guidelines And Supporting Documents

This policy is intended to work in conjunction with the below mentioned regulatory guidelines. This policy does not supplement the below and/or any regulatory guidelines. In case of any conflict between existing and/or any future RBI circulars/guidelines, the RBI circulars/guidelines shall supersede this policy.

- a) Reserve Bank of India (Commercial Banks - Responsible Business Conduct) Directions, 2025

b) Reserve Bank – Integrated Ombudsman Scheme, 2026

10.0 Policy Revision History

Previous Approval Date – This is the first iteration of this policy

Current Approval Date – August 25th, 2026

11.0 Policy Appendices

NA