SADHANA SAHAKARI BANK LTD.

CUSTOMER PROTECTION FROM FRAUDULENT AND FAILED ELECTRONIC TRANSACTIONS POLICY

Customer Liability, Rapid Reporting, Reversal, Compensation and Grievance Redressal Framework

Document Control

Field	Controlled value
Document title	Customer Protection from Fraudulent and Failed Electronic Transactions Policy
Policy code	SSBL-CPFT-001
Version	2.0
Classification	Internal Use Only
Policy owner	CEO / Senior Manager - Payment Channels / Compliance and Customer Service
Approving authority	Board of Directors
Supersedes	Relevant clauses in the Integrated IT, Cyber Security, Digital Banking and Privacy Policy Manual v2.0

Version and Amendment History

Version	Date	Nature of change	Prepared / reviewed by	Approval
2.0	27/08/2026	Comprehensive bank-specific redraft aligned to current RBI directions, ISO standards and the Bank architecture.	IT Head	Pending Board approval
Future	-	All future amendments shall be recorded with rational and affected sections.	IT Head	Board / delegated authority

SADHANA SAHAKARI BANK LTD. HEAD OFFICE

Regulatory and Standards Reference Register

Ref.	Authority / standard	Instrument / edition	Policy relevance
R1	Reserve Bank of India	RBI/2017-18/109; DCBR.BPD.(PCB/RCB).Cir.No.06/12.05.001/2017-18 dated 14 December 2017	Limiting liability of customers of co-operative banks in unauthorised electronic banking transactions.
R2	Reserve Bank of India	RBI/2019-20/67; DPSS.CO.PD No.629/02.01.014/2019-20 dated 20 September 2019	Harmonized TAT and suo motu compensation for failed transactions using authorised payment systems.
R3	Reserve Bank of India	RBI/2020-21/21; DPSS.CO.PD No.116/02.12.004/2020-21 dated 6 August 2020	Online Dispute Resolution system for digital payments.
R4	Reserve Bank of India	Reserve Bank - Integrated Ombudsman Scheme, 2021, as amended	External cost-free redress where the Bank does not satisfactorily resolve/reply within the prescribed period.
R5	Reserve Bank of India	Master Circular on Customer Service - UCBs dated 1 July 2015	Complaint acknowledgement, customer service governance, display, monitoring and audit.
R6	Reserve Bank of India	NEFT / RTGS procedural requirements and FAQs; compensation for delayed credit/return	Penal interest at current RBI LAF Repo Rate plus two percent in applicable delayed NEFT/RTGS situations.
R7	Reserve Bank of India	Master Directions on Fraud Risk Management in Regulated Entities, 2024, and FAQs dated 22 April 2025	Board governance, early warning, transaction monitoring, fraud reporting, investigation and accountability.
R8	Reserve Bank of India	KYC Direction, 2016, as amended	Ongoing due diligence, risk-based transaction monitoring and detection of mule/unusual accounts.
R9	Reserve Bank of India	Comprehensive Cyber Security Framework for Primary UCBs - A Graded Approach	Customer-information protection, transaction monitoring, incident response, logging and channel security.
S1	ISO	ISO 10002:2018 - Quality management - Customer satisfaction - Guidelines for complaints handling	Accessible complaint process, management involvement, analysis, audit and continual improvement.
S2	ISO	ISO 10003:2018 - Customer satisfaction - Guidelines for dispute resolution external to organizations	External dispute-resolution principles.
S3	ISO	ISO 31000:2018 - Risk management - Guidelines	Integrated fraud/customer-protection risk management.
S4	ISO / IEC	ISO/IEC 27001:2022	Information security, event/incident management, logging, evidence, supplier and access controls.
S5	ISO / IEC	ISO/IEC 27701:2025	Privacy management and protection of personal data during complaint investigation and sharing.

1. Executive Policy Statement

Sadhana Sahakari Bank Limited shall protect customers from loss arising from unauthorised electronic banking transactions and failed payment transactions through preventive controls, real-time monitoring, mandatory transaction alerts, simple 24x7 reporting, immediate containment, evidence-based liability determination, prompt shadow reversal, suo motu compensation, fair grievance redressal and Board oversight. Customer liability shall never be presumed merely because valid credentials were used; the burden of proving customer liability lies on the Bank.

CUSTOMER-FIRST PRINCIPLE

The Bank shall apply the most customer-protective outcome that is consistent with the facts, RBI directions and the integrity of the investigation. Where evidence is inconclusive, a Bank/system/third-party weakness is present, transaction alerts or reporting channels failed, or the Bank cannot prove customer negligence, the customer shall not be held liable.

2. Bank Channel and Operating Context

Channel / dependency	Bank arrangement	Policy implication
CBS	Virtual Galaxy CBS on ESDS cloud with Oracle 19c.	Customer account, balance, audit trail and reversal integrity must be preserved.
UPI / IMPS / NFS / ATM	Sarvatra and sponsor-bank / sub-member arrangements.	Bank remains accountable to the customer while coordinating with switch/sponsor/participant.
NEFT / RTGS	Sub-member through sponsor-bank arrangement.	TAT, return, penal interest, traceability and sponsor escalation must be controlled.
Mobile Banking	Customer-facing applications are integrated with CBS and payment services.	Onboarding, device/authentication, limits, alerts, fraud monitoring and complaint access are critical.
Security monitoring	SECEON SOC, Fortinet, Harmony EDR, Sectona PAM, AD, DLP and dark-web monitoring.	Fraud investigations shall use security and transaction evidence without delaying customer relief.
Branches / customer service	28 branches plus Head Office.	Home branch and all notified reporting channels must accept and promptly register complaints.
Third parties	ESDS, Virtual Galaxy, Sarvatra, sponsor bank, OEMs and support providers.	Contracts and escalation matrices must support evidence, blocking, reversal, reconciliation and TAT compliance.

3. Purpose and Objectives

- Define customer rights and obligations for unauthorised electronic transactions, failed transactions and related digital payment grievances.
- Provide immediate, accessible and auditable reporting and containment across website, phone, SMS, email, IVR/toll-free and branch channels.
- Implement RBI-prescribed zero/limited-liability rules and a clear Board-approved rule for reports received beyond seven working days.
- Ensure shadow reversal within 10 working days and final liability determination within a maximum of 90 days for unauthorised electronic transactions.
- Ensure system-driven TAT and suo motu compensation for failed authorised payment-system transactions.
- Integrate fraud monitoring, KYC/AML vigilance, mule-account detection, cyber incident response, ODR, sponsor/switch coordination and customer communication.
- Provide transparent grievance escalation and access to the RBI Integrated Ombudsman Scheme where applicable.

4. Scope and Applicability

- Remote/online transactions: mobile banking, UPI, IMPS, card-not-present, internet/API-enabled transactions and applicable electronic fund transfers.
- Proximity/face-to-face electronic transactions: ATM, POS, card-present, QR or mobile-based payment where a physical instrument/device is present.
- Failed transactions where an account is debited but the beneficiary/merchant/customer does not receive the intended result within the applicable payment-system rules.
- All savings, BSBD, current, cash-credit, overdraft and other eligible customer accounts and cards covered by RBI directions.
- All Bank departments, branches, channel teams, customer service, grievance officers, IT/SOC, internal audit and third-party providers involved in prevention, investigation, reversal, compensation or reporting.

SADHANA SAHAKARI BANK LTD. HEAD OFFICE

IMPORTANT DISTINCTION

An unauthorised transaction is not the same as a failed transaction. An unauthorised transaction requires liability assessment and customer protection under the 2017 co-operative-bank circular. A failed transaction is one where a genuine attempt did not complete as expected and is governed by the payment-system TAT/compensation framework. Both may arise in the same incident and shall be handled under the stricter applicable requirement.

5. Definitions

Term	Policy definition
Unauthorised electronic transaction	An electronic debit/transaction not authorized by the customer, including a transaction arising from bank deficiency, third-party breach or customer credential compromise.
Bank deficiency / negligence	Control, system, process, employee, vendor-for-bank, alerting, reporting-channel or security failure attributable to the Bank.
Third-party breach	A breach where responsibility lies neither with the Bank nor the customer, but elsewhere in the payment ecosystem.
Customer negligence	A customer act or omission that the Bank proves, on evidence, directly caused or enabled the transaction, such as knowingly sharing a PIN/password/OTP or approving a transaction after clear warning. Use of valid credentials alone is not proof.
Communication of transaction	The SMS, email, app notification, statement or other Bank communication by which the customer is informed of the transaction.
Working day	Working day of the customer's home branch; the date of receiving transaction communication is excluded for liability timelines.
Shadow reversal	Provisional credit of the disputed amount, value-dated to the unauthorised transaction date, without waiting for insurance or inter-party settlement.
Failed transaction	A transaction that did not fully complete due to a reason not attributable to the customer, including debit without receipt of cash, credit or merchant confirmation.
T	Calendar date of the transaction unless the relevant payment-system rule defines otherwise.
ODR	System-driven, rule-based online dispute-resolution mechanism with zero or minimal manual intervention.
Vulnerable customer	A customer requires additional assistance due to age, disability, low digital literacy, language, financial distress or other circumstances.
Customer Protection Review Committee	Bank committee authorized it to make evidence-based liability, waiver and systemic-corrective decisions.

6. Governance and Accountability

Role / body	Accountability	Minimum evidence
Board of Directors	Approve policy, beyond-seven-day liability rule, compensation framework and risk appetite; review trends and systemic control improvements.	Board resolution and periodic review.
IT / Customer Service / Risk Committee	Review fraud/unauthorised transaction volumes, channel trends, TAT breaches, compensation, root causes and remediation.	Quarterly dashboard and minutes.
CEO	Ensure resources, fair customer outcomes, material escalation, regulatory/sponsor coordination and resolution of systemic issues.	Escalation decisions and action approvals.
Principal Nodal / Grievance Officer	Own customer escalation, reasoned responses, Ombudsman coordination and policy adherence.	Complaint register, responses and escalation.
Senior Manager - Payment Channels	Own channel controls, switch/sponsor escalation, disputes, reversals, reconciliation and scheme TATs.	Channel case records and reconciliation.
Branch Manager / Customer Service	Accept complaints from any notified channel, register immediately, acknowledge, assist vulnerable customers and prevent further loss.	Complaint number, timestamp and customer communication.
IT / SOC / Fraud Monitoring	Preserve evidence, block/contain, monitor transactions, analyses devices/logs and support investigation without delaying provisional customer relief.	SIEM/application logs and investigation note.
CBS / Operations / Finance	Process shadow/final credits, value dating, interest/compensation and account/GL reconciliation.	CBS entries, authorization and ledger reconciliation.
Third parties / sponsor bank / Sarvatra	Provide evidence, trace, blocking, reversal, dispute, settlement and timely escalation under SLA.	Tickets, acknowledgements and partner records.
Internal Audit	Review all unauthorised transaction cases, customer-liability decisions, TAT, compensation and systemic fixes.	Audit report and closure validation.

7. Preventive and Detective Customer-Protection Controls

Control domain	Mandatory requirements
Alerts	SMS transaction alerts are mandatory; email/app alerts shall be sent where registered/available. Alert failures shall be monitored and treated as a possible Bank control deficiency.
Authentication	Strong customer authentication, secure credential lifecycle, device/session controls, risk-based step-up and transaction limits shall be applied according to channel risk.
Fraud monitoring	The Bank shall maintain dynamic fraud detection and prevention using transaction velocity, amount, beneficiary, device, geolocation, account behavior, mule indicators, repeated failures and other risk signals.
KYC/AML monitoring	Risk-based ongoing monitoring shall identify unusual activity, non-KYC risk, rapid pass-through, beneficiary concentration and potential money-mule accounts.
Channel controls	Customer enablement, beneficiary addition, limit change, device binding, credential reset and high-risk transaction changes shall be logged and subject to cooling/step-up controls where applicable.
Cyber controls	SOC, firewall, EDR, PAM, DLP, application and database logs shall support prevention and investigation; cyber incidents shall be linked to customer cases.
Third-party controls	Sponsor/switch/vendor contracts shall define 24x7 escalation, evidence, blocking, reversal, reconciliation, TAT and incident notification.
Customer education	Repeated advice shall cover OTP/PIN/password secrecy, screensharing/remote-access apps, impersonation, phishing, UPI collect requests, QR scams and immediate reporting.
Staff controls	Maker-checker, role-based access, monitoring of staff accounts/transactions and no alteration/suppression of complaint evidence.
Business continuity	Reporting, blocking, reversal and complaint handling shall remain available during channel/system outage through alternate processes.

8. Mandatory 24x7 Reporting Channels

Channel	Bank requirement	Controlled detail to be inserted before issue
Dedicated toll-free / phone	24x7 reporting of unauthorised transaction, card/device loss and fraud; call recording/ticket creation where available.	[Insert verified number]
SMS reply / short code	Customers shall be able to respond directly to transaction alerts where technically supported.	[Insert verified process]
Email	Dedicated monitored mailbox with automatic acknowledgement and ticket number.	[Insert verified email]
Website / online form	Direct prominent link on home page specifically for unauthorised electronic transactions.	[Insert verified URL internally]
Mobile banking / app	In-app report/block/dispute option where available; no complex navigation.	[Insert current function]
IVR / phone banking	Simple menu for immediate card/channel blocking and complaint registration.	[Insert verified route]
Home branch / any notified branch	Branch shall accept complaints, assist customer, issue acknowledgement and immediately alert central team.	All 28 branches
Written complaint	Accepted without prejudice to faster containment; timestamped and registered.	Branch/HO address

NO CHANNEL REFUSAL

A complaint shall not be rejected or delayed because the customer approached a branch other than the home branch, used a different notified channel, lacks a police complaint, has not contacted the merchant/sponsor/switch, or cannot immediately provide every supporting document. Containment and registration shall come first.

9. Complaint Intake, Acknowledgement and Immediate Containment

Time from receipt	Mandatory action	Owner / evidence
Immediate	Register unique complaint/case number; capture receipt channel, date/time, customer/account/channel, disputed transactions and contact details.	Branch/customer service; ticket timestamp.
Immediate	Acknowledge complaint through SMS/email/printed acknowledgement and advise customer of next steps.	Automated/manual acknowledgement.
Immediate / within minutes	Block affected card/channel/device/beneficiary or apply protective restriction as appropriate; prevent further loss.	Channel/CBS block record.
Within 30 minutes for critical/high-risk	Notify payment channel/fraud team and SOC; preserve application, authentication, device, network and transaction logs.	Escalation and evidence hold.

Time from receipt	Mandatory action	Owner / evidence
Within 4 hours	Initial triage: unauthorised, failed, customer-induced/scam, duplicate, merchant dispute, service issue or cyber incident; identify potential widespread exposure.	Triage note.
Same business day	Initiate sponsor/switch/beneficiary-bank trace, fund hold/recall and dispute workflow where feasible.	Partner ticket/reference.
Within 1 business day	Provide customer with case status, provisional classification and additional information request limited to what is necessary.	Customer communication.
Within 10 working days	Complete shadow reversal for eligible zero/limited-liability unauthorised transaction cases.	CBS credit and value date.
Within Board/RBI timeline	Complete reasoned liability decision, final compensation and closure, not exceeding 90 days for 2017-circular cases.	Approved decision and closure letter.

10. Classification of Customer Cases

Case type	Examples	Primary policy treatment
Bank deficiency	System/process/employee/vendor failure, alert/reporting failure, security control failure.	Zero customer liability; immediate protection and corrective action.
Third-party breach	Payment ecosystem breach with no Bank/customer fault.	Zero or limited liability based on reporting time; shadow reversal.
Customer negligence	Proven knowing disclosure/approval or conduct directly enabling transaction.	Customer bears loss only until reporting; Bank bears post-reporting loss; waiver may be granted.
Social engineering / customer-authorised scam	Customer was deceived into authorizing payment.	Prompt tracing/recall, fraud investigation, empathetic handling and case-specific legal/scheme treatment; do not misclassify as failed transaction.
Failed transaction	Debit occurred but cash/credit/merchant confirmation not received.	Automatic reversal and suo motu compensation under RBI TAT.
Merchant/service dispute	Goods/service/quality dispute where transaction itself was authorized.	Applicable card/UPI dispute or grievance process, not unauthorised-liability process unless fraud exists.
Duplicate / erroneous debit	Technical or processing error.	Immediate correction under payment rules and customer-service obligations.
Account takeover / cyber incident	Credential/device/app compromise, SIM swap, malware or Bank/vendor breach.	Customer protection plus cyber incident response and broader exposure assessment.

11. Customer Liability Framework

11.1 Zero liability

- Where the unauthorised transaction occurred due to contributory fraud, negligence or deficiency on the part of the Bank, irrespective of when the customer reports it.
- Where a third-party breach lies neither with the Bank nor the customer and the customer reports within three working days of receiving transaction communication.
- Where the Bank cannot prove customer liability, transaction alerts/reporting channels failed materially, or evidence was not preserved due to Bank/vendor failure.
- Any post-reporting unauthorised loss after the customer notified the Bank.

11.2 Limited liability - report within four to seven working days

Account type	Maximum customer liability: lower of transaction value or amount shown
BSBD Account	₹5,000
All other Savings Bank accounts	₹10,000
Prepaid payment instruments and gift cards, where applicable	₹10,000
Current / Cash Credit / Overdraft accounts of MSMEs	₹10,000
Individual Current / Cash Credit / Overdraft with annual average balance or limit up to ₹25 lakh	₹10,000
Credit cards with limit up to ₹5 lakh, if applicable	₹10,000
All other Current / Cash Credit / Overdraft accounts	₹25,000

11.3 Board-approved treatment - report beyond seven working days

BANK POLICY FOR REPORTS BEYOND SEVEN WORKING DAYS

Where responsibility lies neither with the Bank nor the customer and the customer reports after seven working days, the Bank shall ordinarily cap the customer's liability at the same account-type limits shown above, and never above the actual loss occurring before notification. The Customer Protection Review Committee may waive the liability fully or partly based on customer vulnerability, alert delivery, clarity of customer communication, fraud sophistication, evidence quality, promptness after actual discovery, system weakness and equitable considerations. Any loss after reporting is borne by the Bank.

11.4 Customer negligence

- Where the Bank proves that loss occurred due to customer negligence, the customer bears actual loss only up to the time of reporting; any loss after reporting is borne by the Bank.
- The Bank may waive customer liability fully or partly even in customer-negligence cases, particularly for vulnerable customers or sophisticated impersonation/fraud.
- The use of a correct PIN, OTP, password, device or biometric is relevant evidence but is not, by itself, conclusive proof of negligence or informed authorization.
- The investigation shall distinguish voluntary informed authorization from deception, coercion, remote-device takeover, SIM swap, malware, spoofed communication or unauthorized account access.

12. Liability Assessment and Burden of Proof

Evidence area	Minimum investigation	Customer-protection rule
Transaction alert	Was SMS/email/app alert generated and delivered? Was reporting method clear?	Alert/reporting failure may constitute Bank deficiency or justify waiver.
Authentication	What factors were used? Any reset, device change, SIM change, new beneficiary, unusual login or step-up failure?	Valid credentials alone do not prove customer fault.
Transaction context	Amount, velocity, time, beneficiary, geolocation/device, normal customer behavior and fraud-rule hits.	Failure of reasonable fraud monitoring shall be considered.
Bank / vendor systems	Application, switch, sponsor, CBS, API, network and security logs; known incident or control gap.	Missing evidence due to Bank/vendor failure shall not prejudice the customer.
Customer conduct	What information/action was knowingly shared/approved and what warnings were shown?	Negligence must be causally connected and proved by the Bank.
Reporting timeline	Date/time of transaction communication and first customer notification; home-branch working days.	Liability window calculated precisely; receipt date excluded.
Post-reporting action	Was the card/channel/account blocked and were further transactions prevented?	Post-reporting loss is borne by Bank.
Third-party response	Sponsor/switch/beneficiary-bank trace, reversal, fund hold and evidence.	Inter-party delay shall not postpone customer relief.

13. Shadow Reversal, Value Dating and Final Resolution

1. On notification, the Bank shall credit the shadow reversal for eligible zero/limited-liability unauthorised transactions within 10 working days, without waiting for insurance, sponsor-bank or beneficiary-bank settlement.
2. The credit shall be value-dated to the date of the unauthorised transaction.
3. For a debit card or bank account, the customer shall not suffer loss of interest. Where a credit-card product is applicable, the customer shall not bear additional interest burden.
4. The complaint shall be resolved, customer liability established and compensation completed within the Board-approved timeline and in no case later than 90 days from receipt.
5. If the Bank cannot resolve or determine liability within 90 days, the prescribed customer protection shall be provided immediately.
6. Any recovery from third parties or insurance after customer credit shall be reconciled separately and shall not delay or reverse legitimate customer relief.
7. A provisional credit may be adjusted only after a reasoned, approved decision, prior customer notice and compliance with RBI directions; no unilateral debit shall be made merely because a third party rejected a claim.

SADHANA SAHAKARI BANK LTD. HEAD OFFICE

14. Failed Transaction TAT and Suo Motu Compensation

The following RBI outer limits shall be automated and monitored. The Bank and its service providers shall endeavor to resolve earlier. Compensation shall be credited suo motu without waiting for a customer claim.

Payment category	Illustrative failure	Auto-reversal / credit outer limit	Compensation after outer limit
ATM	Account debited but cash not dispensed.	T + 5 calendar days	₹100 per day of delay.
Card-to-card transfer	Card debited but beneficiary card not credited.	T + 1 calendar day	₹100 per day of delay.
POS / card-present	Account debited but merchant confirmation not received.	T + 5 calendar days	₹100 per day of delay.
Card-not-present / e-commerce	Account debited but merchant system does not receive confirmation.	T + 5 calendar days	₹100 per day of delay.
IMPS	Account debited but beneficiary account not credited.	T + 1 calendar day	₹100 per day of delay.
UPI fund transfer	Account debited but beneficiary account not credited.	T + 1 calendar day	₹100 per day of delay.
UPI merchant payment	Account debited but merchant confirmation not received.	T + 5 calendar days	₹100 per day of delay.
AePS transfer	Account debited but beneficiary not credited.	T + 1 calendar day	₹100 per day of delay.
AePS cash withdrawal	Account debited but cash not dispensed.	T + 5 calendar days	₹100 per day of delay.
Aadhaar Payment Bridge	Delay in crediting beneficiary account.	T + 1 calendar day	₹100 per day of delay.
NACH	Delay in crediting beneficiary or reversal of debit.	T + 1 calendar day	₹100 per day of delay.
PPI / wallet on-us	Beneficiary PPI not credited / transfer not completed.	T + 1 calendar day	₹100 per day of delay.
PPI merchant transaction	PPI debited but merchant confirmation not received.	T + 5 calendar days	₹100 per day of delay.

SCHEME RULE PREVAILS

The matrix shall be reviewed against the latest RBI/payment-system operating rules. Where a later scheme circular prescribes a shorter TAT or higher compensation, that requirement shall automatically apply.

15. NEFT and RTGS Customer Compensation

- For NEFT, if the transaction is not credited or returned within two hours after the relevant batch settlement, penal interest at the current RBI LAF Repo Rate plus two percent shall be paid for the delay period, without waiting for a claim.
- For RTGS, where a failed payment is not returned within the applicable period, the originating customer is eligible for compensation at the current Repo Rate plus two percent for the delay.
- Sponsor-bank/sub-member dependence does not remove the Bank's obligation to track the transaction, communicate with the customer and ensure applicable compensation.
- Compensation calculation, value date, authorization and GL/account reconciliation shall be independently checked.

16. Online Dispute Resolution and Digital Complaint Access

- The Bank shall provide access to ODR for digital-payment disputes through its own or the relevant payment-system/sponsor arrangement.
- The ODR mechanism shall be transparent, rule-based, user-friendly and require zero or minimal manual intervention for standard failed-transaction cases.
- Customers shall be able to lodge disputes through multiple channels; on-us and off-us transactions shall be covered as applicable.
- Case status, decision, reversal and compensation shall be traceable and available to the customer.
- Manual intervention shall be controlled and recorded with reason; it shall not be used to suppress automatic compensation.
- A customer shall be informed of the next grievance level and RBI Ombudsman route in the closure/rejection response.

17. Fraud Investigation, Fund Recovery and Law-Enforcement Coordination

Activity	Mandatory control
Immediate fund tracing	Initiate beneficiary-bank/sponsor/switch trace, lien/hold/recall or dispute action where legally and operationally available.
Evidence preservation	Preserve CBS, application, channel, authentication, device, IP, alert, call, complaint and CCTV evidence where relevant.
Fraud classification	Apply current RBI fraud-risk directions and internal fraud governance without prejudicing timely customer relief.
Mule-account action	Apply enhanced monitoring, KYC review, debit restriction/hold and reporting in accordance with law and RBI directions.
Cyber incident linkage	Where common compromise is suspected, activate incident response, threat hunting and customer-impact assessment.

Activity	Mandatory control
Law enforcement	Assist the customer and report/coordinate as required by applicable law, RBI directions and case facts. Police complaint shall not be a precondition for registration or provisional relief.
Recovery proceeds	Credit/reconcile recovered funds transparently; avoid duplicate benefit while ensuring the customer receives full entitlement.
Systemic remediation	Root cause, affected population, look-back, rule tuning, control correction, staff/vendor accountability and customer notification shall be tracked.

18. Customer Communication and Fair Treatment

- Communication shall be clear, respectful, in an accessible language and shall avoid blaming the customer before investigation.
- Acknowledgement shall state the complaint number, disputed amount, date/time received, immediate protective action, expected next update and escalation contact.
- Requests for information shall be proportionate; the Bank shall not repeatedly seek documents already available in its systems.
- Closure/rejection shall be reasoned, reference the evidence and policy basis, show compensation/liability calculation and provide grievance escalation.
- Vulnerable customers shall receive assisted reporting, branch support and reasonable accommodation.
- No fee shall be charged for reporting fraud, blocking an instrument, lodging a complaint or obtaining the decision.

19. Grievance Escalation Matrix

Level	Authority	When customer may escalate	Bank action
Level 1	Branch / 24x7 channel / Customer Service	Immediately on detection.	Register, acknowledge, contain and route.
Level 2	Central Payment Channel / Fraud and Grievance Team	No meaningful update, disagreement or TAT risk.	Review evidence, reversal, compensation and partner escalation.
Level 3	Principal Nodal / Grievance Officer	Customer dissatisfied with Level 2 or adverse liability decision.	Independent reasoned review and final Bank response.
Level 4	CEO / Customer Protection Review Committee	Material amount, vulnerable customer, systemic issue, exception or waiver.	Final internal policy decision and corrective action.
External	Reserve Bank - Integrated Ombudsman Scheme, where covered	Bank response unsatisfactory/rejected, or no response within 30 days, subject to Scheme conditions.	Provide complete timely records through Principal Nodal Officer.

20. Sponsor Bank, Sarvatra and Third-Party Coordination

Dependency	Bank control requirement
Sarvatra / switch	24x7 escalation, unique ticket, transaction trace, reversal, settlement status, logs and root-cause response.
Sponsor bank	Defined contacts for UPI/IMPS/NFS/NEFT/RTGS; timely dispute, return, compensation, settlement and evidence.
Virtual Galaxy / CBS	Audit trail, account value dating, reversal authorization, no unaudited manual adjustment and incident evidence.
ESDS / infrastructure	System/log availability, outage timeline, evidence preservation and notification of infrastructure/security failure.
Telecom / SMS / email provider	Alert-generation and delivery evidence, outage reporting and alternate customer notification.
Other processors	Contractual obligation to meet RBI TAT and customer-protection requirements, even if the inter-party SLA is longer.
Bank accountability	A third-party dispute or delayed response shall not be cited to postpone RBI-mandated customer credit or compensation.

21. Data Protection, Confidentiality and Record Integrity

- Complaint and investigation data shall be used only for legitimate prevention, investigation, recovery, legal, regulatory and customer-service purposes.
- Access shall be role-based and logged; sensitive authentication data shall not be unnecessarily collected or reproduced.
- Customer data shared with sponsor banks, payment systems, beneficiary banks, vendors or law enforcement shall be limited, authorized and protected.
- Case records, recordings, logs, evidence and decisions shall be retained according to legal/regulatory and Bank retention requirements and placed on hold where investigation/litigation continues.
- Evidence shall be time-synchronized, attributable and protected against alteration or unauthorized deletion.

SADHANA SAHAKARI BANK LTD. HEAD OFFICE

22. Management Information, KPIs and KRIs

Metric / indicator	Target / threshold	Reporting
24x7 complaint-channel availability	≥99.5%; outage immediately escalated	Monthly and quarterly.
Complaint acknowledgement	100% immediate / automated where possible	Monthly.
Immediate protective action	100% without avoidable delay	Case and monthly dashboard.
Shadow reversal within 10 working days	100% eligible cases	Monthly and quarterly Board/committee.
Final resolution within 90 days	100%	Monthly; any breach to CEO.
Failed-transaction auto-reversal within RBI TAT	100%	Daily exception and monthly summary.
Suo motu compensation accuracy	100%	Monthly reconciliation.
Cases where liability imposed	Trend, evidence quality and appeal outcome	Quarterly.
Repeat fraud / mule / beneficiary patterns	Risk-based threshold	Daily monitoring and monthly trend.
Alert delivery failures	Any material failure investigated	Daily/weekly.
Third-party SLA/TAT breaches	Zero unresolved critical breaches	Monthly vendor review.
Ombudsman complaints / awards	Root cause and corrective action	Immediate and quarterly Board review.

23. Board and Internal Audit Reporting

- Quarterly reporting shall include case count and value by ATM, card-present, card-not-present, mobile banking, UPI, IMPS, NFS, NEFT, RTGS and other channels.
- Reports shall show zero/limited/customer-negligence classifications, reports within 3 days/4-7 days/beyond 7 days, shadow reversals, final outcomes, compensation, TAT breaches and recoveries.
- Systemic failures, repeat fraud patterns, alert failures, reporting-channel outages, vendor delays and policy exceptions shall be highlighted.
- Internal Audit shall review all unauthorised electronic transaction cases on a risk-based basis, with full coverage of liability-imposed, TAT-breached, high-value, vulnerable-customer and repeat/systemic cases.
- The Board/Committee shall direct improvements to systems, procedures, customer awareness and vendor controls and track them to closure.

24. RACI Matrix

Activity	Board / Committee	CEO / Nodal Officer	Payment / Fraud Team	Branch / Customer Service	IT / SOC / CBS	Vendor / Sponsor	Internal Audit
Approve policy and beyond-7-day rule	A	R	C	I	C	I	C
Register and acknowledge complaint	I	A	C	R	I	I	I
Immediate block / containment	I	A	R	R/C	R	C	I
Preserve / analyse evidence	I	C	R	C	R	C	I
Shadow reversal / compensation	I	A	R	C	R/C	C	C
Liability decision	I	A/R	R	C	C	C	C
Partner dispute / recovery	I	C	A/R	I	C	R/C	I
Customer response / escalation	I	A/R	R	R	C	I	I
Regulatory / Ombudsman response	I	A/R	C	C	C	C	I
Independent review	I	I	C	C	C	C	A/R

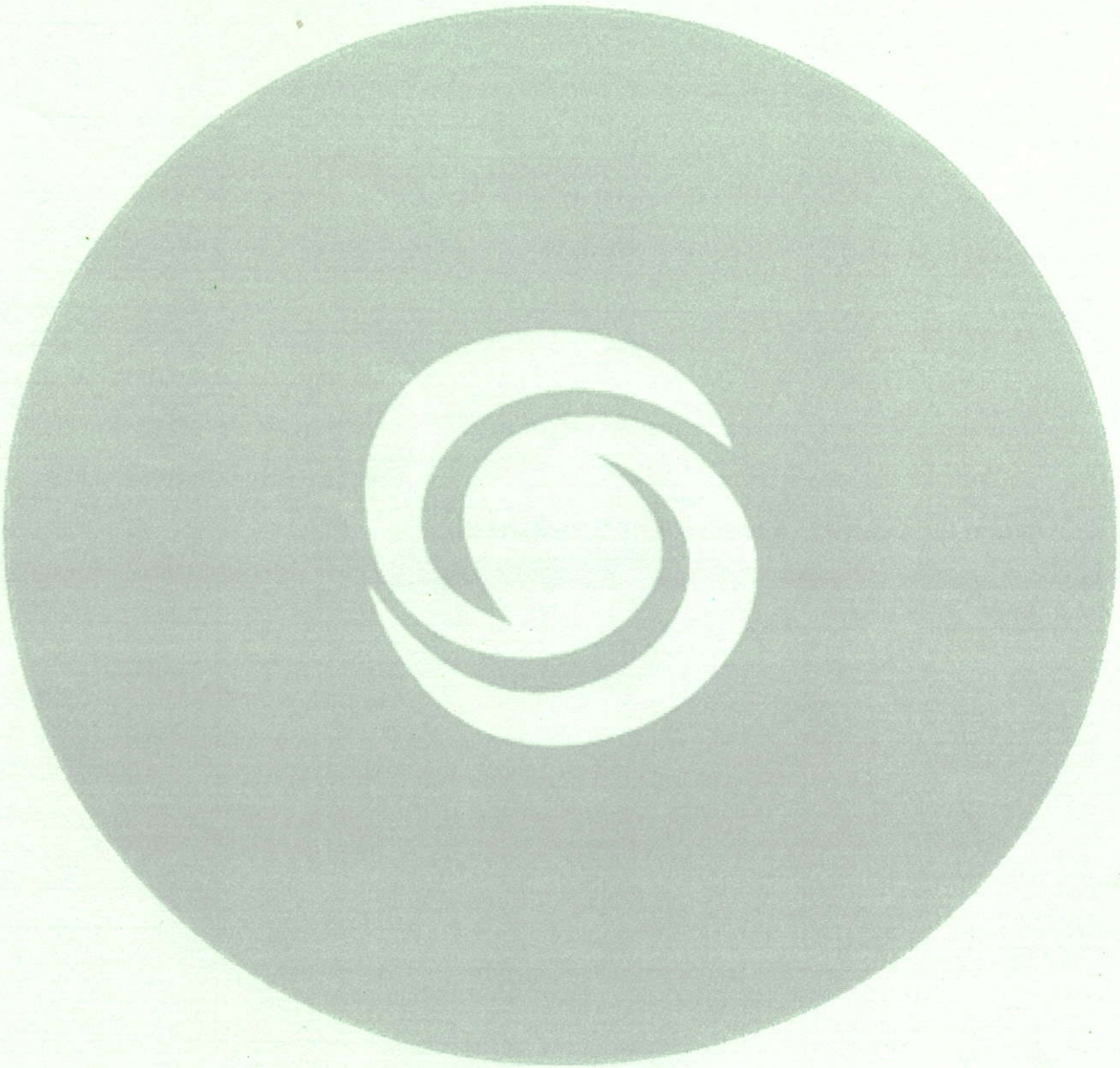
25. Exceptions and non-compliance

No exception may reduce a customer entitlement mandated by RBI or law. Any system inability to provide alerts, 24x7 reporting, automatic reversal, compensation, audit evidence or required TAT shall be treated as a control deficiency, risk-assessed, immediately remediated and reported to management. Vendor limitations do not constitute an acceptable customer-protection exception.

26. Training, Awareness and Policy Review

- Branch, call-centre/customer-service, payment-channel, CBS, SOC, grievance and audit personnel shall receive role-based training at least annually.

- Staff should be trained not to blame customers, demand unnecessary police reports, defer to third parties or close cases without reasoned evidence.
- Customer education shall be repeated through branches, website, app, SMS/email and awareness campaigns.
- This policy shall be reviewed annually and whenever RBI/payment-system rules, channels, sponsor arrangements, fraud patterns, Ombudsman decisions or Bank systems materially change.



Annexure A - Customer Complaint and Immediate Action Form

Field	Required entry
Complaint / case number	
Date and exact time received	
Reporting channel and receiving employee/system	
Customer name / account / contact	
Transaction channel, reference, date/time and amount	
Date/time customer received transaction communication	
Date/time customer first discovered the transaction	
Customer statement and suspected method	
Instrument/channel blocked and time	
Further transaction prevention action	
SOC/fraud/payment escalation time	
Sponsor/switch/beneficiary-bank ticket	
Shadow reversal eligibility and due date	
Failed-transaction TAT/compensation applicability	
Evidence preservation reference	
Next customer update and escalation level	

Annexure B - Liability Assessment Worksheet

Assessment point	Finding / evidence	Decision impact
Bank/system/vendor deficiency present?		
Alert generated and delivered?		
24x7 reporting channel available?		
Third-party breach with no customer fault?		
Customer reporting window: ≤3 / 4-7 / >7 working days?		
Specific proven customer negligence and causal link?		
Any post-reporting loss?		
Account type and applicable cap?		
Vulnerable-customer/equitable waiver factor?		
Shadow reversal date/value date?		
Failed-transaction TAT/compensation separately applicable?		
Final reasoned decision and approver?		

Annexure C - Customer Communication Minimum Content

- Acknowledgement: case number, receipt time, disputed transaction(s), protective action and expected update.
- Shadow reversal notice: amount, value date, provisional nature and no impact on final rights.
- Information request: only necessary items, secure submission channel and due date.
- Closure: findings, liability category, evidence relied upon, credit/compensation calculation, date credited and escalation rights.
- Adverse decision: clear reasons, policy/RBI basis, internal appeal contact and RBI Ombudsman information where applicable.

- Outage/systemic incident: safe alternatives, fraud-reporting route, expected next update and caution against impostor communications.

Annexure D - Regulatory Alignment Matrix

Policy area	RBI requirement / source	ISO alignment
Fraud prevention / alerts / 24x7 reporting	Co-operative-bank customer liability circular, 14 Dec 2017	ISO 10002; ISO/IEC 27001 incident and communications controls
Zero / limited liability and burden of proof	RBI/2017-18/109	ISO 10002 fairness and complaint handling
10-day shadow reversal / 90-day resolution	RBI/2017-18/109	ISO 10002 timeliness and effectiveness
Failed transaction TAT / compensation	DPSS.CO.PD No.629/02.01.014/2019-20	ISO 10002; ISO 31000
ODR	DPSS.CO.PD No.116/02.12.004/2020-21	ISO 10003
Ombudsman / external redress	RB-IOS 2021, as amended	ISO 10003
Fraud monitoring / mule detection	Fraud Risk Management Directions; KYC Direction	ISO 31000; ISO/IEC 27001
Evidence / cyber linkage / privacy	UCB cyber framework; CERT-In / applicable privacy requirements	ISO/IEC 27001; ISO/IEC 27701

This Policy supersedes all earlier instructions, circulars and policy provisions of the Bank on the same subject matter to the extent of any inconsistency. The Policy shall remain in force until it is superseded by a subsequent version approved by the Board of Directors.

Mr.Pritam Dhavale
IT Head

Mr. Sanjay Haribhau Shevkar
Chief Executive Officer

This Customer Protection from Fraudulent and Failed Transactions Policy was placed before the Board of Directors of Sadhana Sahakari Bank Ltd. and was approved by the Board of Directors of the Bank vide its Meeting dated 27/08/2026 and Resolution No. 7(10) . The Policy shall be effective from date 01/04/2026.

Mr. Rajesh Ramchandra Kawade

Chairman

SADHANA SAHAKARI BANK LTD. HEAD OFFICE