



Mobile Number
President : 8002771182
General Secretary: 9835452010

स्टेट बैंक ऑफ इंडिया ऑफिसर्स एसोशिएशन
State Bank of India Officers' Association
(Patna Circle)
Regd No. 1872 of 1972
REGISTERED UNDER TRADE UNION ACT – 1926

All letters to be addressed
to the General Secretary

State Bank Building
2nd Floor, Local Head Office
West Gandhi Maidan,
Patna-800001

CIRCULAR NO.07 /2026

DATE : 09.01.2026

TO,
ALL MEMBERS

**SUBJECT: MONEY MULE ACCOUNTS – IMPLEMENTATION SAFEGUARDS,
CSP/BC CHANNEL CONTROLS, AND FAIR OFFICER-PROTECTION
FRAMEWORK (IN LIGHT OF BANK SOP/EDD INSTRUCTIONS AND
RBI DIRECTIONS)**

We reproduce hereunder the text of the AISBOF Circular No. 07 dated 09.01.2026, the contents of which are self-explicit.

With warm greetings,

(Amaresh Vikramaditya)
General Secretary

OUR UNITY : ZINDABAD-ZINDABAD
S.B.I.O.A. : ZINDABAD-ZINDABAD

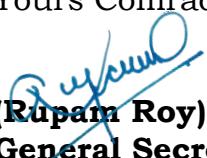
TEXT

**SUBJECT: MONEY MULE ACCOUNTS – IMPLEMENTATION SAFEGUARDS,
CSP/BC CHANNEL CONTROLS, AND FAIR OFFICER-PROTECTION
FRAMEWORK (IN LIGHT OF BANK SOP/EDD INSTRUCTIONS AND
RBI DIRECTIONS)**

We have sent a communication to the Deputy Managing Director (HR) & Corporate Development Officer, State Bank of India, Corporate Centre, Mumbai, on the captioned subject.

The content of the communication is reproduced below.

With Greetings,
Yours Comradely,


(Rupam Roy)
General Secretary

To,

The Deputy Managing Director (HR) & CDO
State Bank of India
Corporate Centre,
Madame Cama Road
Mumbai-400021.

Dear Sir,

**SUBJECT: MONEY MULE ACCOUNTS – IMPLEMENTATION SAFEGUARDS,
CSP/BC CHANNEL CONTROLS, AND FAIR OFFICER-PROTECTION
FRAMEWORK (IN LIGHT OF BANK SOP/EDD INSTRUCTIONS AND
RBI DIRECTIONS)**

We write to place on record our continuing and serious concern regarding the operational, reputational and personal-risk exposure being faced by branch functionaries in matters relating to “suspected money mule” accounts, particularly those sourced/opened through CSP/BC channels and subsequently observed to be used for cyber-enabled frauds and laundering of proceeds.

The Federation is fully aligned with the Bank’s statutory and regulatory obligations on KYC/AML/CFT, fraud risk management, and timely reporting to FIU-IND/LEAs. We also note and welcome that the Bank has already issued an internal Policy/SOP on prevention, identification and restriction of money mules, along with a reiteration circular emphasising that EDD must be conducted meaningfully (not perfunctorily) and that customer profiling (purpose/occupation/income) and due diligence must be correctly recorded, failing which deviations will be viewed seriously.

In parallel, RBI directions emphasise (i) strengthening of early warning signals and monitoring for money mule accounts, (ii) robust KYC/ongoing due diligence and FIU-IND reporting governance, and (iii) the need for structured, system-led detection and response rather than ad-hoc, officer-centric determinations.

Notwithstanding the above frameworks, the implementation reality at field level is that branch officers, often not the owners of end-to-end controls (channel onboarding, CSP supervision, device controls, transaction monitoring thresholds, and system intelligence), are being put under pressure to “certify / label / confirm” mule status and to take restrictive actions without a uniformly documented authority matrix, maker-checker assurance, and recorded rationale.

This results in a practical paradox for the operating officer:

- service disruption, complaints, legal notices, and allegations of arbitrariness, frequently directed personally at the signing officer.
- post-incident scrutiny, “why not detected” allegations and retrospective disciplinary framing, again disproportionately focused on branch staff.
- where the branch is made accountable for outcomes while the decisive controls are dispersed across channel teams, analytics/monitoring, and central AML governance.

Accounts sourced through CSP/BC ecosystems require special handling because mule operators frequently exploit early-life high velocity transactions, sometimes before traditional branch behaviour patterns become observable. While RBI permits use of BCs for prescribed customer interactions, the responsibility for KYC compliance and risk decisioning remains with the Bank, and compliance decision-making cannot be outsourced.

Accordingly, where the Bank's governance places the onus of "mule" labelling or restrictive actions on field level officers without central/system-led risk intelligence and protected approvals, it creates inconsistent outcomes and unfair post-facto attribution of blame.

We request the Bank to issue an implementation clarification that money mule identification/tagging shall be system-led and AML-led, with branches providing EDD/verification inputs only, and not owning the "labelling" decision. Accordingly, any "Suspected Money Mule" status and consequential actions (freeze/stop/hold/partial restrictions) must be invoked only through a defined authority framework (AML/KYC/FCC/PRM, as designated) with maker-checker, recorded reasons/reason-codes, and a retrievable audit trail. To ensure uniformity across Circles and audit units, the Bank should mandate a standard documentation checklist and reason-code matrix for every tagging/de-tagging and restriction decision.

Equally, since the Bank's policy framework already imposes accountability and training expectations, it must also provide formal protection to bona fide staff acting in good faith. We therefore seek a written circular clarifying that no disciplinary/vigilance action will be initiated merely because an account later turns out to be a mule, unless mala fide intent, proven collusion, or gross negligence is established through due process and that once suspicion is escalated through the prescribed AML route (including One-Page STR/escalation protocols), all regulatory reporting and external coordination must follow the designated governance chain (Principal Officer/AML-CFT), without forcing branch staff into informal disclosures. Further, where officers are summoned in LEA enquiries for actions performed in official capacity and in compliance with approved SOP, the Bank must provide panel legal support and institutional representation. Finally, for CSP/BC-sourced accounts, we request immediate channel hardening through whitelisting/geo-fencing, device binding, agent analytics and exception reporting to branches/AML, with central triggers for red flags (spikes in openings, common contact details, abnormal early-life velocity, failed contactability, etc.); while making it explicit that CSP may source/assist, but risk decisions (EDD conclusion, restrictions, mule-tagging) consistent with the non-outsourcing principle must be under maker-checker concept and not shifting the entire burden to the individual branch functionaries.

Since RBI guidance also emphasises technology-enabled monitoring, we request confirmation of time-bound implementation and evidence-ready audit trails for the Bank's system linkages and dashboards (including use of telecom/DIP inputs like revoked mobile indicators, analytics-driven identification, and other ecosystem alerts integrated into Bank workflows). Branches must receive clear, actionable dashboards and standardized scripts rather than discretionary instructions.

We also seek that the Bank institutionalise:

1. Refresher training/certification for CSP supervisors and account-opening officials on mule typologies, EDD documentation discipline, and escalation etiquette.
2. Non-punitive post-incident reviews that examine root causes (channel controls, monitoring thresholds, contactability failures, ignored alerts, supervisory gaps) rather than default blame on the certifying officer.

In view of the above, we request your intervention to ensure that, within a defined and communicated timeline, the Bank issues:

- an implementation circular clearly demarcating (i) CSP/BC sourcing responsibility, (ii) branch verification/EDD responsibility, and (iii) AML/FCC decision responsibility with maker-checker;
- a good-faith officer-protection instruction and bank-funded legal support protocol for actions taken under approved SOP; and
- measurable CSP/BC channel hardening controls supported by technology and audit-backed monitoring.

Money mule accounts are a real and growing risk to the Bank, and we reiterate that a centrally governed, documented and system-led approach is essential, both to ensure regulatory compliance and to prevent bonafide branch officials from being made victims of systemic/channel-control gaps. We therefore reiterate our request for a practicable framework be made operational so as to protect the bank, to ensure regulatory compliance, and at the same time safeguard bonafide officers who act in good faith under approved processes.

Yours faithfully,

Sd/-
(Rupam Roy)
General Secretary