Anti-Money Laundering (AML) Policy

Checkpost Capital Private Limited

Checkpost Capital Private Limited ("the Company"), a SEBI-registered Research Analyst under the SEBI (Research Analyst) Regulations, 2014, acknowledges the significance of maintaining robust internal systems and controls to combat money laundering and terrorist financing. In line with the **Prevention of Money Laundering Act, 2002 (PMLA)**, and the applicable rules, guidelines, and circulars issued by SEBI and the **Financial Intelligence Unit - India (FIU-IND)**, this policy is established to ensure the Company fully complies with regulatory expectations and maintains integrity in all its dealings.

The primary goal of this policy is to establish a framework for detecting, preventing, and reporting suspicious transactions or activities that may be linked to money laundering or terrorist financing. This policy also serves to protect the Company from being used, intentionally or unintentionally, by criminal elements for such illicit purposes.

Objectives

The Anti-Money Laundering (AML) Policy of Checkpost Capital Private Limited is developed to:

- Establish and enforce **Customer Due Diligence (CDD)** procedures before onboarding any clients.
- Ensure adherence to SEBI-mandated **KYC (Know Your Client)** norms through KYC Registration Agencies (KRAs).
- Identify and report suspicious transactions to **FIU-IND** in a timely manner.
- Maintain proper documentation and **record-keeping** standards for regulatory audit trails.
- Prevent misuse of the Company's services for **money laundering or terrorist financing**.
- Demonstrate a **risk-based approach** towards client onboarding and ongoing monitoring.

This policy shall be applicable to all personnel involved in client-facing or compliance-related functions.

Definitions

- **Money Laundering**: The process of concealing the origins of illegally obtained money by passing it through a complex sequence of banking transfers or commercial transactions.
- **Suspicious Transaction**: A transaction that gives rise to a reasonable suspicion that it may involve proceeds of crime or be related to terrorist financing or lacks economic or lawful purpose.
- **Beneficial Owner**: The natural person(s) who ultimately owns or controls a client and/or the person on whose behalf a transaction is being conducted.
- **Customer Due Diligence (CDD)**: The process of identifying and verifying the client's identity and assessing their risk level.

Client Onboarding & KYC Compliance

a. Acceptance Policy

Only individuals or entities that are **KYC-compliant as per SEBI regulations** will be eligible for onboarding. This includes:

- Verification of PAN through KRA or CKYC database
- Collection of contact details such as email address and phone number
- Completion of subscription payment using a bank account, UPI, or credit/debit card in the name of the client
- Digital acceptance of Terms of Service and RA Agreement

Clients who are unwilling to cooperate or whose identity cannot be verified satisfactorily shall not be onboarded.

b. Identification and Verification

All clients must undergo a **PAN-based KYC check** through official SEBI-registered KRAs. Where KYC status is confirmed as compliant, the Company may retain verification logs, screenshots, or audit trails rather than full document downloads.

Additional verification shall be performed in case of:

- High-value clients
- Clients from high-risk jurisdictions
- Unusual patterns in payments

c. Risk Categorization

Clients shall be categorized into **low, medium, or high risk** based on the following criteria:

- Occupation and source of funds
- Geography (e.g., high-risk jurisdictions)
- Nature of payment (e.g., third-party payments)

- Past transaction behavior

Higher-risk clients may require enhanced due diligence and periodic review.

Ongoing Monitoring & Due Diligence

a. Periodic Monitoring

All client activity will be periodically reviewed to ensure:

- Consistency with stated investment intent
- No unusual transaction behavior
- Absence of high-risk indicators

Flagged behaviors include but are not limited to:

- Multiple subscriptions from a single IP or payment method
- Rapid subscription and refund requests
- Use of proxies or masked IPs

b. Transactional Red Flags

Examples of suspicious behavior:

- Payment from a name not matching subscriber
- Repeated cancellations
- Attempts to avoid PAN/KYC compliance
- Unusual communication patterns or aggressive resistance to verification

Such cases may be immediately reported if there are grounds for suspicion.

Record Keeping & Retention

Checkpost Capital shall maintain the following documentation for a **minimum of 10 years**:

- KYC verification logs
- Subscription agreements
- Payment records
- Support conversations where applicable
- Screenshots or audit trails of PAN-based KYC status

Records can/shall be maintained in **both hard and soft copy formats**, where necessary.

In case of suspected transactions under investigation, the Company shall retain the records until regulatory closure.

Reporting of Suspicious Transactions

Any client/prospective client who is identified as suspicious, The Principal officer will:

- Assess whether the suspicion is reasonable
- File a **Suspicious Transaction Report (STR)** with **FIU-IND** if warranted
- Maintain confidentiality of the reporting
- Ensure that no tipping-off occurs to the client in question

Examples of transactions that warrant scrutiny include:

- Sudden high-value purchases of multiple portfolios
- Payments from offshore accounts
- Use of shell entities or fictitious names

Principal Officer for AML

The Company has designated the following Principal Officer for AML compliance:

Name: Rithvik Thammareddy
Designation: Principal Officer – AML Compliance
Email: rithvikthammareddy@gmail.com
Phone: 9100046789

Responsibilities include:

- Monitoring implementation of AML Policy
- Maintaining internal reporting and control systems
- Liaising/ if any with FIU-IND and regulatory authorities
- Updating policy in line with regulatory changes

Training and Awareness

All employees involved in customer interaction, compliance, or data handling shall receive training on:

- PMLA obligations
- Recognizing suspicious activity
- Reporting mechanisms

Shall be reviewed periodically with ad-hoc updates for regulatory changes.

Review and Updates

This policy will be reviewed periodically or upon:

- Any change in regulatory framework
- Launch of new services/products/guidlines
- Discovery of any lapses or compliance risk

Any changes shall be documented, approved by management, and communicated to all relevant stakeholders.