

KNOW YOUR CUSTOMER & ANTI-MONEY LAUNDERING POLICY

Spinny Capital Private Limited

(Approved by the Board dated September 14, 2024)

INTRODUCTION:

The Reserve Bank of India (RBI) had issued vide its Master Direction DBR.AML.BC.No.81/14.01.001/2015- 16 dated February 25, 2016 (as amended from time to time) and master circular issued on July 1, 2015 under Prevention of Money-Laundering Act, 2002 and Prevention of Money-laundering (Maintenance of Records) Rules, 2005 advised all NBFCs to revise their KYC policies to incorporated changes suggested in the above Directions/Circulars. Amendment to Prevention of Money-Laundering (Maintenance of Records) Amendment Rules, 2013 dated December 1, 2014, and Obligation of NBFCs under Prevention of Money laundering Act (PMLA), 2002 - Client Due Diligence dated January 2, 2015 advised all NBFCs to revise their KYC policies to incorporate changes suggested in the above circulars.

OBJECTIVES, SCOPE AND APPLICATION OF POLICY:

The objective of KYC guidelines is to prevent the Company from being used, intentionally or unintentionally, by criminal elements for money laundering activities or terrorist financing activities. KYC procedures shall also enable the Company to know and understand its Customers and its financial dealings better, which in turn will help it to manage its risks prudently. Thus, the KYC policy has been framed by the Company for the following purposes:

1. To prevent criminal elements from using Spinny Capital for money laundering activities.
2. To enable the Company to know/ understand its customers and their financial dealings better which, in turn, would help the Company to manage risks prudently.
3. To put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws/laid down procedures.
4. To comply with applicable laws and regulatory guidelines.
5. This policy shall be applicable for all new and existing customer and business partner relationships of Spinny Capital.
6. To ensure that the concerned staff are adequately trained in KYC/AML/CFT procedures.

This KYC Policy is applicable to Spinny Capital and is to be read in conjunction with related operational guidelines issued from time to time. This Policy includes some key elements:

1. Customer Acceptance Policy (CAP)
2. Customer Identification Procedures (CIP)
3. Customer Due- diligence (CDD)
4. Monitoring of Transactions

5. Specified Transactions
6. Risk management
7. Training Programme
8. Internal Control Systems
9. Appointment of Principal Officer
10. Reporting to FIU – India.

Definition of Customer

For the purpose of Spinny Capital KYC policy a 'Customer' means a person as defined under KYC policy of RBI (and any amendment from time to time by RBI) which are at present as under: -

- A person or entity that maintains an account and/or has a business relationship with the Company.
- One on whose behalf the account is maintained (i.e. the beneficial owner)
- Beneficiaries of transactions conducted by professional intermediaries such as Stockbrokers, Chartered Accountants, Solicitors etc. as permitted under the law;
- Any other person or entity connected with a financial transaction which can pose significant reputation or other risks to the Company, say a wire transfer or issue of high value demand draft as a single transaction.

KEY ELEMENTS:

I. CUSTOMER ACCEPTANCE POLICY ("CAP"):

1. The Customer Acceptance policy (CAP) lays down the criteria for acceptance of customers. The guidelines in respect of the customer relationship in the Company broadly includes the following:
 - a) No account is to be opened in anonymous or fictitious/benami name(s)/entity(ies)
 - b) Accept customers only after verifying their identity, as laid down in Customer Identification Procedures. Necessary checks before opening a new account are to be ensured so that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations, etc.
 - c) Segregate customers into different risk categories and, based on risk perception, apply corresponding acceptance criteria. Additionally, generate a profile for each customer based on their risk classification.
 - d) Specify documentation requirements and information to be collected for various customer categories according to perceived risk, ensuring compliance with the Prevention of Money Laundering Act, 2002 (PMLA), and RBI guidelines.
 - e) Refrain from initiating new account openings or closing existing accounts (except as outlined in this Policy) in cases where the identity of the account holder cannot be verified

or required documents/information cannot be obtained/confirmed as per risk categorization, due to customer non-cooperation or unreliable data/information provided to the Company. Incorporate appropriate safeguards to prevent customer harassment.

- f) Ensure that the implementation of Customer Acceptance Policy (CAP) does not excessively restrict access to services for the general public, particularly those who are financially or socially disadvantaged.
 - g) Define circumstances under which a customer may act on behalf of another person/entity in accordance with established laws and practices, and strictly adhere to these guidelines to prevent instances where an account is operated by a mandate holder or opened by an intermediary in a fiduciary capacity.
2. The Company will establish a customer profile for each new customer during the credit appraisal process, aligning with the risk categorization outlined in this policy. This profile will encompass details such as the customer's identity, socio-economic status, business activities, as well as information regarding their clients' businesses and locations. The level and nature of due diligence conducted will be contingent upon the perceived risk by Spinny Capital. During the credit appraisal stage, pertinent details will be recorded alongside the customer's profile, acquired through interactions with the applicant by a Company representative, in addition to the collection of relevant documents, adhering to prevailing Credit/products norms. However, in crafting the customer profile, the Company will only request information that is pertinent to the risk category and non-intrusive. Any additional information desired from the customer will be sought separately, with their explicit consent, post-account opening. The customer profile will be treated as confidential, with its contents not disclosed for cross-selling or any other purposes.
3. Perceived risk will be broadly classified into three categories: A, B, and C. Category A encompasses high-risk customers, Category B comprises medium-risk customers, and Category C includes low-risk customers. All entities, regardless of their status or relationship with the Company or promoter, will be subject to the KYC procedure.

The aforementioned requirement may be adjusted based on the perceived risk. Customer risk, in this context, pertains to the money laundering risk associated with a particular customer from the Company's perspective.

High-Risk Customers (Category A):

Characteristics of High-Risk Customers: Customers whose source of funds is unclear or unconvincing will be classified as high-risk customers. Stringent due diligence measures shall be applied to this category of customers.

Medium-Risk Customers (Category B):

Characteristics of Medium-Risk Customers: Customers who are likely to pose a higher-than-average risk to the Company may be categorized as medium-risk customers.

Low-Risk Customers (Category C):

Characteristics of Low-Risk Customers: Individuals and entities whose identities and sources of wealth are easily identifiable, and whose transactions largely align with their known profile, fall under this category. Customers not meeting the criteria for high-risk or medium-risk categories will be categorized as low-risk customers.

II. CUSTOMER IDENTIFICATION PROCEDURES ("CIP"):

1. Customer identification involves identifying and verifying the customer's identity using reliable, independent source documents, data, or information. The Company will gather sufficient information to verify the identity of each new customer, including brief details of its promoters and management where applicable, whether they are regular or occasional, and the purpose of the intended business relationship. This requirement may be adjusted based on risk perception, such as in the case of a publicly listed company where it may not be necessary to identify all shareholders.
2. In addition to risk perception, the type of information/documents required will also depend on the customer type (individual, corporate, etc.). For natural person customers, the Company will collect adequate identification data to verify their identity, address/location, and recent photograph. For legal person or entity customers, the Company will:
 - a) Verify the legal status of the entity through relevant documents.
 - b) Confirm that any individual representing the entity is duly authorized, and verify their identity.
 - c) Understand the ownership and control structure of the customer and identify the natural persons who ultimately control the legal entity. Customer identification requirements will adhere to the provisions of the Prevention of Money Laundering Act and its Rules. An indicative list of documents/information that may be relied upon for customer identification will be established by the Company, which will formulate internal guidelines based on its experience, prudent practices, and legal requirements.
3. The Company will develop and implement a Client Identification Programme to ascertain the true identity of its clients, considering the aforementioned factors. This policy will also outline the identification procedures to be followed at different stages, including establishing a relationship, conducting financial transactions, or in cases where doubts arise regarding the authenticity, veracity, or adequacy of previously obtained customer identification data.

III. MONITORING OF TRANSACTIONS:

The Company typically does not engage in large cash transactions. However, if cash transactions amounting to Rs. 10 lakh or more occur, the Company will maintain comprehensive records of such transactions.

Additionally, the Company will continuously monitor transactions for suspicious activities with the intention of reporting them to the relevant authorities. The level of monitoring undertaken by the Company will be contingent upon the risk sensitivity of the account, with particular emphasis placed on scrutinizing all complex and unusually large transactions lacking apparent economic or lawful purpose.

In adherence to the provisions outlined in the Prevention of Money Laundering Act (PMLA) and its Rules, the Company will promptly notify the appropriate regulatory and investigative bodies of any high-value cash transactions or transactions deemed suspicious in nature.

IV. SPECIFIED TRANSACTIONS:

Specified Transactions to include any withdrawals or deposits in cash, transactions in foreign exchange, transactions in high value imports and remittances, exceeding the value as agreed upon by the Board of Directors, and other transactions that may have a high risk or any instances of Money laundering or Terrorist financing.

Before commencement of any transaction of a specified nature, the Company shall ensure the below mentioned points:

1. Verify the identity of the clients undertaking such specified transaction by authentication under the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016.
2. Take additional steps to examine the ownership and the financial position, including sources of funds of the Client and any such additional checks as may be decided by the Board of Directors.
3. Record the purpose behind conducting the specified transaction and the intended nature of the relationship between the transaction parties as decided by the Board of Directors.

V. RISK MANAGEMENT:

The Management, under the supervision of the Board of Directors of the Company shall ensure that an effective KYC process is put in place by establishing appropriate procedures and ensuring their effective implementation. It will cover proper management oversight, systems and controls, segregation of duties, training and other related matters. Responsibility will be explicitly allocated within the Company for ensuring that the policies and procedures applicable to the Company are implemented effectively. The Company shall devise procedures for creating Risk Profiles of their existing and new customers and apply various Anti Money Laundering measures keeping in view the risks involved in a transaction, account or business relationship.

VI. TRAINING PROGRAMME:

The Company shall have an ongoing employee training programs so that the members of the staff are adequately trained in KYC/ AML/ CFT procedures. Training requirements shall have different focuses for front line staff, compliance staff and officer/ staff dealing with new customers so that all those concerned fully understand the rationale behind the KYC policies and implement them consistently.

VII. INTERNAL CONTROL SYSTEM:

The Company's Internal Audit and Compliance functions will evaluate and ensure adherence to the KYC policies and procedures. As a general rule, the compliance function will provide an independent evaluation of the Company's own policies and procedures, including legal and regulatory requirements. The Management under the supervision of the Board shall ensure that the audit function is staffed adequately with skilled individuals. Internal Auditors will specifically check and verify the application of KYC procedures and comment on the lapses observed in this regard.

Compliance in this regard shall be put before the Board or any Committee of the Board along with their normal reporting frequency. Further, the Company shall have an adequate screening mechanism in place as an integral part of their recruitment/ hiring process of personnel to ensure that person of criminal nature/ background do not get an access, to misuse the financial channel.

VIII. APPOINTMENT OF PRINCIPAL OFFICER:

The Company shall designate a senior employee as 'Principal Officer' (PO) who shall be located at the Head Office and shall be responsible for monitoring and reporting of all transactions and sharing of information as required under the law. PO shall maintain close liaison with enforcement agencies, NBFCs and any other institution which are involved in the fight against money laundering and combating financing of terrorism.

IX. REPORTING TO FINANCIAL INTELLIGENCE UNIT - INDIA:

The PO shall report information relating to cash and suspicious transactions, if detected, to the Director, Financial Intelligence Unit India (FIUIND) as advised in terms of the PML Rules, in the prescribed formats as designed and circulated by RBI at the following address:

Director,
Financial Intelligence Unit India, 6th Floor, Hotel Samrat, Chanakyapuri, New Delhi - 110021

AML PROCESS

Transaction Monitoring: Continuous monitoring is a vital component of robust KYC procedures. Effective risk control and mitigation can only be achieved through a comprehensive understanding of a customer's normal and reasonable activity, enabling Spinny Capital to identify transactions deviating from regular patterns. However, the level of monitoring will be contingent upon the risk sensitivity of the account. The following types of transactions warrant close monitoring:

1. Cash transactions exceeding ten lakh rupees or its equivalent in foreign currency.
2. Series of cash transactions interconnected and individually valued below ten lakh rupees or its equivalent in foreign currency, where the monthly aggregate exceeds ten lakh rupees or its equivalent in foreign currency, within a month.
3. Cash transactions involving counterfeit currency notes or banknotes passed off as genuine, or instances of valuable security forgery.
4. Suspicious transactions, irrespective of being cash or non-cash, as specified in the Rules framed by the Government of India under the Prevention of Money Laundering Act, 2002.

INFORMATION PRESERVATION:

The following information pertaining to the above transactions must be retained:

1. Nature of transactions.
2. Transaction amount and currency denomination.
3. Transaction date.
4. Transaction parties.

CENTRAL KYC RECORDS REGISTRY:

The Spinny Capital Operations Department will take necessary measures to adhere to the CKYCR norms within stipulated timelines. The Government of India has authorized the Central Registry of Securitization Asset Reconstruction and Security Interest of India (CERSAI) to function as the CKYCR, responsible for receiving, storing, safeguarding, and retrieving customers' KYC records in digital format.

TRANSACTION REPORTING:

Under the PMLA and its associated Rules, the Principal Officer is obligated to report all cash transactions and suspicious transactions to the Financial Intelligence Unit (FIU-IND). Accounts subject to Suspicious Transaction Reports (STRs) will face no operational restrictions. It is imperative to avoid tipping off customers at any level. Additionally, all attempted transactions abandoned or aborted by customers upon request for details or documentation must be reported in STRs by Spinny Capital, regardless of transaction amount.

The types of transactions to be reported and the reporting procedures are detailed as follows:

1. REPORTING OF CASH TRANSACTIONS:

The following transactions shall be reported to the FIU-IND as applicable to Spinny Capital:

- i. Cash transactions amounting to Rs. 10 lakhs and above, or its equivalent in foreign currency.
- ii. Series of cash transactions interconnected, individually valued below Rs. 10 lakhs or its equivalent in foreign currency, where the aggregate monthly value exceeds Rs. 10 lakhs or its equivalent in foreign currency. Reporting of Cash Transaction Report (CTR) shall comply with the provisions of the Prevention of Anti Money Laundering Act, 2002 and rules made thereunder.

2. REPORTING OF SUSPICIOUS TRANSACTIONS:

In addition to reporting cash transactions, the Principal Officer is obligated to report all suspicious transactions to the Director, FIU-IND. Suspicious Transaction Reports (STRs) shall be filed if there are grounds to believe the transaction involves proceeds of crime, irrespective of the transaction amount or threshold limit for predicate offences under the PMLA, 2002. Any delay in furnishing information to the Director FIU-IND, even for one day, will be considered as non-compliance.

The following activities warrant attention:

1. Large cash transactions exceeding usual thresholds.
2. Transactions lacking economic rationale, such as immediate withdrawal of deposited assets without valid justification.
3. Business accounts with significant credit volume inconsistent with their nature.
4. Attempts to evade reporting or record-keeping obligations, including reluctance to provide required information.
5. Unusual activities involving funds from known money laundering sources.
6. Customers providing insufficient or suspicious information regarding business activities or financial status.
7. Employees exhibiting suspicious behavior, such as lifestyle beyond means or repeated negligence.
8. Examples of suspicious transactions include large cash transactions, multiple accounts under the same name, placing funds in term deposits to secure additional loans, sudden activity surges, and repeated movement of funds among accounts.

Reporting of Suspicious Transaction Report (STR) shall comply with the provisions of the Prevention of Anti Money Laundering Act, 2002 and rules made thereunder.

3. RECORD KEEPING:

Central Operations (COPS) is responsible for record-keeping and retention as per the PMLA, 2002 Rules. Transaction records must be maintained for five years from the cessation date of the customer's transaction with Spinny Capital. Documents should be preserved in hard copy or digitized format to enable reconstruction of transactions and provide evidence if required for prosecution.

Records pertaining to customer identification and address verification obtained during account opening or business relationship must be preserved for at least five years after the relationship ends.

All other requirements under FATCA/CRS/PML/FIU-Ind, including the appointment of designated officers/directors, principal officers, and reporting obligations (STR, CTR, CCR, and other

applicable reports), shall be complied with as directed by RBI or other authorities, to the extent applicable to Spinny Capital.

List of Documents

Individual Applicants	Documentation
Identity Proof	<ul style="list-style-type: none"> • PAN card
Address Proof	<ul style="list-style-type: none"> • Passport copy • Driving licence • Proof of possession of Aadhaar number • Voter ID Card • Utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill) • Property / Municipal Tax receipt • Pension or family Pension Payment Orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address • Letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and licence agreements with such employers allotting official accommodation

Non-Individual Applicants	Documentation for identity proof
Companies	<ul style="list-style-type: none"> • Certificate of Incorporation • Memorandum of Association / Articles of Association • Board resolution & Authorization for signing of Loan agreement and Cheques • KYC of beneficial owner • Income Tax PAN card • Address Proof as specified in the document
Partnership Firms	<ul style="list-style-type: none"> • Registered Partnership Deed • Service Tax / Sales Tax /Vat /GST Registration Certificate in name of Firm • Firms Registration Certificate

	<ul style="list-style-type: none"> • Authority Letter from all the Partners for loan and authorization to specific partners to sign loan documents. • KYC of Beneficial owner • Income Tax PAN card • Residence Proof as specified in the document
--	--

Note:

- Validity of Documents should be valid and not expired
- For the purpose of this clause, a document shall be deemed to be an OVD even if there is a change in the name subsequent to its issuance provided it is supported by a marriage certificate issued by the State Government or Gazette notification, indicating such a change of name.

Methods to collect and verify KYC details of the customers:

Different methods prescribed by RBI are as follows:

Different Methods	Description
Paper-based KYC	This is an in-person form of verification where customers share physical, self-attested copies of their documents — Proof of Address (POA) and Proof of Identity (POI)
Aadhaar-based eKYC	Aadhaar-based eKYC makes use of the verified data to authenticate customers remotely. There are two ways in which an identity can be verified through Aadhaar — Online Mode: OTP-Based and Online Mode: Biometric-based.
Offline KYC	Offline KYC uses an offline form of Aadhaar without connecting to the UIDAI database. In this form of KYC, an Aadhaar XML/PDF-based or QR-code-based demographic authentication— Name, Address, Gender, DOB, Photograph — can be conducted without the use of biometrics. The XML-based authentication carries a high-resolution photo, but the zipped file can get complicated to download and share with agencies apart from possibility of misuse during transfer. The QR-code mode supports a low-resolution image, and details can be digitally verified through e-Aadhaar on hand-held scanner/mobile apps, making it secure and tamper-proof.

Digital KYC	Digital KYC involves capturing a live photo of the customer and Officially Valid Documents (OVDs) to be geo-tagged by an authorized officer. An individual can share digital copies of PAN, Aadhaar, or Driving Licence for KYC directly on the institution's portal or other digital mediums. The Digital KYC process will then only verify the submitted details against the geo-tagged OVDs and not the document's authenticity.
Central KYC (CKYC)	CKYC is a process that relies on a central repository of customer KYC records in the BFSI sector. This repository allows for inter-usability of KYC records across the financial services sector so that both businesses and customers don't have to go through the entire process of KYC verification every time they engage with each other. Customers or a financial institution submit a signed CKYC form along with POA and POI. If all checks are in place, the form is processed, and a 14-digit KIN is issued for future transactions.
Video KYC	Video KYC refers to assisted/non-assisted KYC via video. It involves an agent and an auditor for verification and audit. Available as Video-based Customer Identification Process (VCIP), Video-based In-Person Verification (VIPV), and Video-based identification Process (VBIP), Video KYC is an entirely paperless and presence-less KYC process for a compliant and fraud-free authentication. The customer onboarding process is initiated by submitting the POI and POA and recording a video via an app or a web portal provided by the service provider, which then is manually viewed and verified by an agent.

Based on the merits of each step mentioned above, Spinny Capital will be using following methods:

- **Physical KYC:** This is the fall back for customers who are either not able to do online KYC or are willing to directly proceed with physical KYC.
- **Video KYC:** A third party panel tool to process Video KYC will be integrated. Option to perform video KYC will come in user journey, but if the customer has logged out of the journey, then a provision to send/share link with customer to continue the KYC journey will be provisioned on LOS. Here the workflow will be managed on the third-party tool and LOS will only carry the status of the case representing cases and their states basis action taken
- **Digital KYC:** Similarly, for Spinny Stores, a third-party panel tool to process Digital KYC will be integrated. Option to perform digital KYC will come in user journey, but if the customer

has logged out of the journey, then a provision to send/share link with customer to continue the KYC journey will be provisioned on LOS. Here the workflow will be managed on the third-party tool and LOS will only carry the status of the case representing cases and their states basis action taken.

List of Acronyms used in this document.

KYC	Know Your Customer
ITR	Income Tax Return
CPV	Contact Point Verification
TVR	Tele- Verification Report
AML	Anti Money Laundering
PAN	Permanent Account Number
CRO	Chief Risk Officer
POI	Proof of Identity
POA	Proof of Address
LOS	Lending Operating System