SWYOM ADVISORS ALTERNATIVE INVESTMENT TRUST

ANTI-MONEY LAUNDERING AND KNOW YOUR CLIENT POLICY

Anti-Money Laundering and Know Your Client Policy (AML & KYC) 2024-2025

Swyom Advisors Alternative Investment Trust ("Swyom") believes in transparency and it takes the responsibility to ensure and maintain that its assets and resources are not being used for corruption, irregularities, or money laundering. The company has taken it upon itself to detect frauds, irregularities, abuse of position, and institutional gains.

Purpose

The purpose of this policy is to make that the company's financial processes and procedures are according to the Prevention of Money Laundering Act, 2002 read with Prevention of Money Laundering (Maintenance of Records) Rules, 2005 and any other rules and regulations or amendments issued from time to time, and in accordance with the Guidelines/Master Circulars issued by SEBI on Anti-Money Laundering (AML) Standards and Combating the Financing of Terrorism (CFT) /Obligations and Know your Client Norms for Securities Market Intermediaries under the Prevention of Money Laundering Act, 2002.

Scope

This policy applies to every entity related to **Swyom Advisors Alternative Investment Trust** and its employees, directors, officers, contractors, or any third party working on behalf of the company.

The policy is for internal use, and the administration is required to convey it to every concerned person or entity. Failure to comply with the policy will result in appropriate action.

Money Laundering

Money laundering refers to those assets that are money that is acquired in exchange for money or assets gained unlawfully. It also includes money spent for terror purposes, regardless of the means it was obtained.

Under this policy, money earned by using the following means is considered money laundering, and it is prohibited;

a. Money or assets received in exchange for criminal or unlawful acts. Money whose origin is not explicit or earned by assisting any activity in evading lawful means.
b. Property gained after any criminal activity and its origin, location, and disposition are not transparent.
c. Property which is promoting any unlawful activity
d. Terrorism financing

Objective

The objective of this policy is to:

- Create awareness and provide clarity on KYC standards and AML measures.
- Outline the obligations of the Investment Manager i.e. SWYOM Advisors Limited under PMLA.
- SWYOM to align its operations with international standards and practices.
- Establishing mechanisms to identify and report suspicious transactions or activities that may be linked to money laundering or terrorism financing.
- Protecting the integrity and stability of the financial transactions by implementing robust AML controls, procedures, and technologies to prevent misuse of the transactions and company system for illegal purposes.

- Assign specific roles and responsibilities to individuals or departments within the organization for implementing and overseeing AML procedures.
- Outline procedures for conducting risk assessments to identify and evaluate potential AML risks associated with the company's clients, partners, and transactions.
- Define due diligence processes for verifying the identities of customers, assessing their risk profiles, and monitoring their transactions regularly.
- Establish robust KYC procedures for the identification and verification of customers' identities before establishing business relationships.
- Specify measures for ongoing monitoring of customer transactions and behavior to detect any suspicious activities.
- Implement training programs to educate employees about AML regulations, the company's policies, and procedures to recognize and report suspicious activities.
- Outline the process for reporting suspicious transactions or activities internally to the designated compliance authority.
- Establish protocols for maintaining proper records of transactions and customer due diligence information as required by regulations.
- Define internal controls and monitoring mechanisms to assess and mitigate AML risks regularly.
- Encourage a process of continuous improvement by regularly reviewing and updating AML policies and procedures to align with changing regulatory requirements and emerging risks.

Designation and Responsibility

SWYOM shall designate a Designated Director to ensure overall compliance with the obligations of Anti Money Laundering & Principal Officer to act as the focal point for all activity relating to money laundering, to monitor compliance and to provide periodic compliance reports to the Board or Senior Management of SWYOM. “Designated Director" means a person designated by the reporting entity to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules and includes:

(i) the Managing Director or a whole-time Director duly authorized by the Board of Directors if the reporting entity is a company,

(ii) the Managing Partner if the reporting entity is a partnership firm,

(iii) the Proprietor if the reporting entity is a proprietorship concern,

(iv) the Managing Trustee if the reporting entity is a trust,

(v) a person or an individual, as the case may be, who controls and manages the affairs of the reporting entity, if the reporting entity is an unincorporated association or a body of individuals, and

(vi) such other person or class of persons as may be notified by the Government if the reporting entity does not fall in any of the categories above.

The Investment Manager shall designate the Principal Officer who shall report to senior management at the next reporting level or the Board of Directors.

a) The Principal Officer acts as the central point of contact with the law enforcement agencies. He/ She is responsible for implementation of Internal Controls and Procedures for identifying and reporting of any suspicious transactions or activity to the concerned authorities.
b) Unexplained, unusual or abnormal transactions which are not in line with the normal expected trend of transactions in the account including transactions suspected of being linked to criminal conduct should be reported to the Principal Officer, who should then determine whether a report should be made to the appropriate authority.
c) Reporting lines for suspicious transactions should be clear and unambiguous and all reports should reach the Principal Officer without delay.
d) All staff should have access to information about their statutory responsibilities and relevant staff should be made aware of the anti-money laundering policies and procedures developed by Company. Relevant staff

should be provided with Anti Money Laundering training that helps them to understand the money laundering risks involved in Portfolio Management business. Records must be kept regarding persons trained.

As per SEBI circular dated February 03, 2023, records evidencing the identity of its customers and beneficial owners as well as account files and business correspondence should be maintained and persevered for five years following the cessation of the business relationship or the account has been closed, whichever is later.
In situations where the records relate to on-going investigations or transactions which have been the subject of a suspicious transaction reporting, they shall be retained until it is confirmed that the case has been closed.

Registered Intermediaries shall maintain and preserve the records of information related to transactions, whether attempted or executed, which are reported to the Director, FIU – IND, as required under Rules 7 and 8 of the PML Rules, for a period of five years from the date of the transaction between the client and the intermediary.

Registered Intermediaries are required to maintain and preserve the following information in respect of transactions referred to in Rule 3 of PML Rules:

- the nature of the transactions;
- the amount of the transaction and the currency in which it is denominated;
- the date on which the transaction was conducted; and
- the parties to the transaction.

THE STANDARDS

Implementation

This Policy Covers Services offered by Swyom Advisors Alternative Investment Trust.

SWYOM as an intermediary of SEBI, shall put in place a system of maintaining proper record of the nature and maintain proper record of all transactions, the nature and value as has been prescribed in the PMLA and such transactions include:

all suspicious transactions inter-alia, credit or debits into from any non-monetary account such as demat account, security account maintained with registered intermediary of SEBI

For the purpose of suspicious transaction reporting, apart from ‘transaction integrally connected’, ‘transactions remotely connected or related’ should also be considered.

The Suspicious Transaction Report (STR) shall be submitted within 7 days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature. The Principal Officer shall record his reasons for treating any transaction or a series of transactions as suspicious. It shall be ensured that there is no undue delay in arriving at such a conclusion.

These Standards are designed to help business to meet its responsibilities in relation to the prevention of money laundering.

The Standards are based on the Company Policy, the Money Laundering Rules of the Financial Intelligence Unit - India and relevant local guidelines. To implement the anti-money laundering provisions as envisaged under the PMLA, the following four specific parameters which are related to the overall ‘Client Due Diligence Process shall be adopted’:

A. Policy for acceptance of clients
B. Procedure for identifying the clients
C. Risk Management
D. Transaction monitoring and reporting especially suspicious transaction Reporting (STR)

These cover all aspects of our business activities from account relationships, the processing of transactions to the provision of advice to investors. Businesses must also consider the application of these parameters in relation to, for

example, joint venture activities and outsourced services – particularly when cross border issues are involved.

Roles and Responsibilities

The Business Managers

The Company heads have a primary responsibility for prevention of money laundering. They are responsible for the development, implementation, maintenance and monitoring of procedures and controls that meet the requirements of Policy on Money Laundering prevention. Pursuant to Rule 2(1)(f), the Company has appointed the Compliance Officer who has also been designated as the Principal Officer who shall be responsible for reporting suspicious transactions to authorities and would act as a central reference point in facilitating onward reporting of suspicious transactions and play an active role in identification and assessment of potentially suspicious transactions. As per the Rule 2(1)(ba) of PMLA (Maintenance of Records) Rules, 2005,the Board of SWYOM appointed member of the Board as the Designated Director.

Constitution of Anti Money Laundering Committee ("AML Committee"):

The Prevention of Money Laundering Act (PMLA) in India mandates the establishment of a PML Committee within certain entities to oversee and ensure compliance with anti-money laundering measures. The PML Committee typically consists of senior management members and is responsible for implementing and monitoring the organization's adherence to the PMLA and related regulations.

An internal AML Committee has been constituted comprising of Principal Officer and two members of sufficient seniority/experience to ensure unbiased judgement, independency and no internal conflict. The objective of the committee AML Committee is to enable-

- Overview of KYC and Suspicious Transaction Reporting Obligations;
- Develop and implement robust anti-money laundering policies, procedures, and controls within the organization.
- Monitoring the organization's compliance with AML laws and regulations, including reporting obligations and record-keeping requirements.
- Adequate Client Due Diligence /Enhance Due Diligence throughout the Client Relationship;
- greater scrutiny and validation if potentially reportable STRs;
- Identify, assess, and mitigate potential money laundering risks associated with the organization's operations, products, services, and customer base.
- Implement measures to reduce the organization's exposure to such risks.
- consider whether all possible factors are taken into consideration while arriving at a decision to report cases;
- Decide the reporting of Suspicious transactions to FIU-India
- there is no individual prejudice towards a particular investor;
- Monitoring of Clients of Special Categories;
- Reporting of Transactions of Non-Profit Organizations;

The Committee shall comprise of the following members:

- Whole Time Director & Chief Executive Officer;
- SVP – Operations;
- Head- Sales or employee not below the rank of Vice- President from Sales department;
- Risk Officer or employee not below the rank of Vice- President from risk department;
- Principal Officer/ Compliance Officer or employee not below the rank of Vice- President from Compliance department

Quorum of the Committee shall be one-third of the total members or two, whichever is greater/ higher, and that the Committee shall meet at such interval(s), as it may from time to time deem fit.

The Principal Officer is responsible for:

1. receiving suspicious transaction reports and monitoring the same;
2. taking reasonable steps to access any relevant information on concerned parties;
3. Being directly in charge of and responsible for payment or settlement transactions, or overseeing individuals handling these transactions within the organization.
4. To place STR before AML Committee along with recommendation for onwards reporting to FIU- India.
5. Reporting of suspicious transactions as decide by the AML Committee;
6. obtaining and using national and internal finds concerning countries with inadequacies in their approach to money laundering prevention
7. taking reasonable steps to establish and maintain adequate arrangements for awareness creation and staff training.

Compliance, Quality Assurance & Risk Control

The Compliance & Risk team is responsible for general oversight of the operation of the Anti- Money Laundering Policy, the effectiveness and integrity of suspicious transaction reporting procedures, and taking reasonable steps to establish and maintain adequate arrangements for money laundering awareness.

The compliance & Risk team will establish a body responsible for the implementation of this policy.

The compliance & Risk team will carry out the procedure to identify any irregularity on behalf of any stakeholder under this policy. The compliance & Risk team should;

a. Identify all the financers of the company and verify their identity
b. Take special care where stakeholders want anonymity
c. Maintain proper records of the stakeholders

If anyone in the company knows or suspects that a person is involved in money laundering or terror financing, it is their responsibility to report such person to the body established by the company. In such a case, the compliance & Risk team must

a. Take the details of the people involved
b. Verify the type of transactions
c. Reason for suspicion
d. The amount involved

The compliance & Risk team can take help of legal consultants before embarking on business with a third party and carefully screen such interactions.

Combating Money Laundering

“Money Laundering” is the process by which persons attempt to hide and disguise the true origin and ownership of the proceeds of their illegal activities, thereby avoiding prosecution, conviction and confiscation of the funds generated through illegal acts and means. The term “Money Laundering” is also used when the funds are used for terrorist financing though the origin of the funds may be legitimate.

Combating money laundering is a multifaceted endeavor that demands a comprehensive approach encompassing legal frameworks, financial institution vigilance, technological innovation, and international cooperation. Central to this effort are stringent anti-money laundering (AML) laws and regulations, which mandate financial entities to implement

robust measures for detecting, preventing, and reporting suspicious transactions. These measures include Know Your Customer (KYC) procedures to verify client identities, transaction monitoring to identify irregularities, and customer due diligence (CDD) to assess risks associated with different clients. A risk-based approach guides the assessment and management of money laundering risks across various services and customer segments. Additionally, training programs and awareness initiatives ensure that employees are equipped with the necessary knowledge to detect potential illicit activities and comply with regulations. Collaboration among countries and institutions through international cooperation enhances information sharing and enforcement actions, while technological advancements such as AI and data analytics bolster AML processes. This comprehensive strategy, coupled with stringent penalties for non-compliance, underscores the concerted efforts aimed at thwarting money laundering activities and preserving the integrity of the global financial system.

Money laundering process involves three stages:

1. Placement - the physical disposal of cash proceeds derived from illegal activity. The launderer introduces his illegal profits into the financial system, by breaking up large amounts of cash into less conspicuous smaller sums that are then deposited directly into a bank account, or by purchasing a series of monetary instruments that are later collected and deposited into accounts at another location.

2. Layering - separating illicit proceeds from their source by creating complex layers of financial transactions designed to hamper the audit trail, disguise the origin of such funds and provide anonymity to their owners.

3. Integration - placing the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing to be legitimate business funds.

Having identified these stages of the money laundering process, SWYOM has to adopt procedures to guard against and report suspicious transactions that occur at any stage.

The ability to launder the proceeds of criminal activity through the financial systems of the world is vital to the success of criminal operations, and therefore India, as one of the world's emerging financial markets, has a vital role to play in combating money laundering.

Customers themselves are better protected if SWYOM is able to protect itself against criminal activity. Failure to prevent the laundering of the proceeds of crime permits criminals to benefit from their actions, thus making crime an attractive proposition.

Adherence to AML policies and procedures should also enhance the fraud prevention measures that SWYOM takes to protect itself and their genuine customers from losses.

Money Laundering risk assessments

Risk assessment is dependent on the kind of customers the SWYOM deals with. Typically, risks are increased if the money launderer can hide behind corporate structures such as limited companies, offshore trusts, special purpose vehicles and nominee arrangements. SWYOM will consider how their customer base and operational systems impact the capacity of their staff to identify suspicious transactions. The risk assessment shall also take into account any country specific information that is circulated by the Government of India and SEBI from time to time, as well as, the updated list of individuals and entities who are subjected to sanction measures as required under the various United Nations' Security Council Resolutions. The risk assessment carried out shall consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied.

Money laundering risk assessment is a crucial process that enables entities, especially financial institutions, to identify, evaluate, and mitigate the risks associated with potential money laundering activities. This assessment involves a comprehensive analysis of various factors, including customer behaviors, transaction patterns, geographical locations,

and products/services offered. By conducting risk assessments, institutions can categorize their customers based on risk levels, applying enhanced due diligence to higher-risk individuals or entities. Factors such as the complexity of transactions, the presence of politically exposed persons (PEPs), and relationships with high-risk jurisdictions are also considered. The risk assessment process is not static but evolves continuously, adapting to changing regulations, emerging threats, and advancements in money laundering techniques. Regular reviews and updates ensure that risk management strategies remain effective in addressing evolving money laundering risks and maintaining compliance with regulatory requirements, thus safeguarding institutions against potential financial crime activities.

Risk Classification

The level of Money Laundering (ML) risks that the Portfolio Management Services is exposed to through an investor relationship depends on:

- Type of investor (resident individual / non-resident / non-Individual) and nature of business
- Transaction pattern of the client (complexity of transactions, if any)
- Customer's income level
- Portfolio value and manner of making payment for transactions
- PEP status
- Nationality
- whether operating through power of attorney
- Type of product / service availed by the customer
- Country where the Customer is domiciled
- KYC status

Based on the above criteria, investors are classified into three Risk levels – High Risk, Medium Risk and Low Risk. This policy defines certain minimum standards of account documentation for all customer relationships, to enable SWYOM to understand the nature of customer's business, carry evidence of key data regarding the customer and its principal owners/ signatories and understand the type and level of activity that is to be considered as normal in the customer's account.

Investors shall be classified as High Risk if it meets the following risk criteria:

(i) High Risk

Customers or transactions associated with higher risks, such as those involved in complex or high-value transactions, individuals from politically exposed positions, customers from high-risk jurisdictions, or activities that exhibit unusual patterns.

The following investors are classified as high risk, provided their subscription transaction value exceeds Rs. 1 crore.

b) Non-resident clients
c) High Net-worth clients
d) Trust, Charities, NGOs and organizations receiving donations d) Unlisted companies
e) Politically Exposed Persons (PEPs)
f) Clients in high-risk countries**
g) Clients with dubious reputation as per public information available
h) Non-face to face clients

Also, clients with risk rating of more than 2.5 as per the risk rating matrix in **Annexure A** shall be classified as High Risk.

**While dealing with clients from or situate in high-risk countries or geographic areas or when providing delivery of services to clients through high-risk countries or geographic areas i.e. places where existence or effectiveness of action against money laundering or terror financings suspect, registered intermediaries apart from being guided by the FATF statements that inter alia identify such countries or geographic areas that do not or insufficiently apply the FATF

Recommendations, published by the FATF on its website (www.fatf-gafi.org) from time to time, shall also independently access and consider other publicly available information along with any other information which they may have access to. However, this shall not preclude registered intermediaries from entering into legitimate transactions with clients from or situate in such high-risk countries and geographic areas or delivery of services through such high- risk countries or geographic areas.

Non face to face clients means clients who open accounts without visiting the branch/offices of the registered intermediaries or meeting the officials of the registered intermediaries. Video based customer identification process is treated as face-to-face onboarding of clients

The regulations define "Politically Exposed Persons" (PEPs) as individuals who have been entrusted with prominent public functions by a foreign country, including the heads of States or Governments, senior politicians, senior government or judicial or military officers, senior executives of state-owned corporations and important political party officials

ii) Medium Risk

Individuals or transactions falling between the low-risk and high-risk categories based on certain identified risk factors. Enhanced due diligence measures are applied to this category, which may include additional scrutiny of transactions and periodic reviews.

Clients with risk rating of 1.5 to 2.5 as per the risk rating matrix in **Annexure A** shall be classified as Medium Risk.

iii) Low Risk

Customers or transactions with lower perceived risks based on various factors such as their business activities, transaction history, geographical locations, and reliability.

These individuals or transactions are subject to standard due diligence procedures.

Clients with risk rating of up to 1.5 as per the risk rating matrix in **Annexure A** shall be classified as Low Risk.

INTERNAL CONTROLS

Policy for acceptance of investors

As part of investor acceptance policy, the following safeguards are being adopted while acceptance of application forms from investors:

1. No account is opened in a fictitious / benami name or on an anonymous basis or account on behalf of other persons whose identity has not been disclosed or cannot be verified.
2. Ensure than an account is not opened where the investor is not able to meet the KYC norms.
3. KYC compliance is mandatory for every client who invests with a Portfolio Fund. Before the Fund decides to do business with a client, it should know who the client is.
4. The investor shall clearly specify regarding operation of the account.
5. Verification of the applicant at the time of onboarding to ensure that the identity of the applicant does not match with any person having known criminal background or is not banned in any other manner by an enforcement agency.

The account is put on hold where SWYOM is unable to apply appropriate CDD measures, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer.

List of Designated Individuals/ Entities

An updated list of individuals and entities which are subject to various sanction measures such as freezing of assets/accounts, denial of financial services etc., as approved by the Security Council Committee established pursuant

to various United Nations' Security Council Resolutions (UNSCRs) can be accessed at its website at http://www.un.org/sc/committees/1267/consolist.shtml. No accounts are to be opened in the name of anyone whose name appears in said list. All existing accounts are continually scanned to ensure that no account is held by or linked to any of the entities or individuals included in the list. Details of accounts bearing resemblance with any of the individuals/entities in the list shall immediately be intimated to SEBI and FIU-IND.

Procedure for freezing of funds, financial assets or economic resources or related services

Section 51A of the Unlawful Activities (Prevention) Act, 1967 (UAPA) and amendments thereto, relating to the purpose of prevention of, and for coping with terrorist activities was brought into effect through UAPA Amendment Act, 2008.The Government has modified the earlier order dated August 27, 2009 by the order dated March 14, 2019 for strict compliance in this regard. Further, the said order stands modified as on February 02, 2021.

In this regard, SWYOM shall be implement the following procedure laid down in the UAPA order dated February 02, 2021:

i) On receipt of updated list of individuals / entities subject to UN sanction measures (hereinafter referred to as 'list of designated individuals / entities) from the Ministry of External affairs which SEBI shall forward to all intermediaries, a check will be run on regular basis to verify whether individuals or entities listed in the order are investors with SWYOM.

ii) SWYOM shall maintain such designated list in electronic form.
- In the event any customers match the particulars of designated individuals / entities shallot later than 24 hours from the time of finding out such customer inform full particulars of such investments the Central (Designated) Nodal Officer for the UAPA at Fax no.011- 23092551 and also convey over telephone on 011-23092548. The particulars apart from being sent on post shall also be sent through email at jsctcr-mha@gov.in.
- SWYOM shall send particulars of the communication stated above in (i) to the UAPANodal Officer of the State/UT where account is held and regulators and FIU-IND, as case may be
- In case the aforementioned details of any of the customers match the particulars of designated individuals / entities beyond doubt, SWYOM shall block such folios and prevent conducting financial transactions under intimation the Central (Designated) Nodal Officer for the UAPA, Ministry of Home affairs at Fax no.011-23092551 and also convey over telephone on 011-23092548. The particulars apart from being sent on post shall also be sent through email at jsctcr-mha@gov.in.
- SWYOM shall also file a Suspicious Transaction Report (STR) with FIU-IND covering all transactions in the accounts.

In case of unfreezing and erroneous freezing of account the procedure laid down in the abovementioned order dated March 14, 2019 shall be followed.

KNOW YOUR CLIENT (KYC)

General

"Know Your Client" (KYC) is a fundamental principle of all anti-money laundering controls. It includes identification of the investor, but it also extends to a full understanding of the nature of the business that underlies a relationship. KYC is an ongoing process - it does not end when account opening procedures are completed. Effective KYC can reduce the risk of accounts being used for money laundering and can help us to identify suspicious transactions.

The more we know about an investor and their business, the better are the chances of identifying changes in their activities that may be grounds for further enquiry, possibly leading to a report to the appropriate authorities. It is therefore essential that adequate information is gathered about the investors or proposed investors, and the nature of their activities, when a relationship begins.

Having sufficient information about our investor and making use of that information is the most effective tool used to counter the efforts of laundering the proceeds of crime. In addition to minimizing the risk of being used for illicit

activities, adequate KYC information provides protection against frauds, enables suspicious activity to be recognized and protects SWYOM from reputation and financial risks.

Where the investor is a new investor, account must be opened only after ensuring that pre- account opening KYC documentation and procedures are conducted. In cases where the investor is an existing investor and no KYC is conducted, the SWYOM shall ensure that the identification of the customer is established within a reasonable time.

A risk-based approach will need to be adopted towards client identification in respect of any additional information that might be required in specific cases.

Application of Commercial Judgment

SWYOM will follow a risk-based approach to the KYC requirements. Consequently, there will be circumstances when it will be both necessary and permissible to apply commercial judgment to the extent of the initial identification requirements. Decisions will need to be taken on the number of verification parameters within a relationship, the identification evidence required, and when additional checks are necessary.

KYC Requirements

The documentation & information requirements and the procedural aspects for completion of the KYC formalities shall be as prescribed by AML Laws/SEBI/KRA from time to time.

The KYC measures would comprise the following:

Every individual will have to fill up a prescribed uniform KYC application form and support it with documents regarding identity i.e. PAN, proof of address, for e.g. Passport and a latest photograph. Further, details such as the investor's occupation, income, tax status, PEP details are required to be obtained by each intermediary. Additional documents to be submitted by non-individual entities which include details of promoters / partners / karta / trustees / whole time directors, asapplicable.

SEBI has issued the SEBI {KYC (Know Your Client) Registration Agency (KRA)} Regulations, 2011. The purpose was to have uniform KYC norms for the securities market. In the KRA regime, a mechanism for centralization of the KYC records in the securities market has been developed. The KYC details of the investor will be shared amongst the KRAs in an interoperable mode. This mechanism currently is in use for all existing investors and also for non-individual investors, alongside the CKYC system.

As per the amendment to PML (Maintenance of Records) Rules dated July 7, 2015 and SEBI circular dated July 21, 2016, the Government of India vide their notification dated November 26, 2015 authorized the Central Registry of Securitization Asset Reconstruction and Security Interest of India (CERSAI), set up under sub-section (1) of Section 20 of the Securitization and Reconstruction of Financial Assets and Enforcement of Security Interest Act, 2002 (54 of 2002), to act as and to perform the functions of the Central KYC Records Registry under the said rules, including receiving, storing, safeguarding and retrieving the KYC records in digital form of a "client", An investor can use the CKYC issued unique number (comprising 14 digits) to transact/deal with all entities governed/regulated by Government of India/Regulator (RBI, SEBI, IRDA AND PFRDA) without the need to complete multiple KYC formalities, which was an inconvenience/hindrance hitherto.

While new investors are currently on-boarded under the provisions of CKYC norms, AMC's must make all efforts to cover existing investors who are KRA KYC compliant, under the CKYC norms.

Further, SEBI vide circular no. SEBI/HO/MIRSD/DOP/CIR/P/2020/73 dated April 24, 2020 ("the Circular") on Clarification on Know Your Client (KYC) Process and Use of Technology for KYC highlighted the below stated points on e-KYC/ Online KYC:

- SEBI registered intermediary shall continue to ensure to obtain the express consent of the investor before undertaking online KYC. Therefore, SWYOM needs to obtain prior consent of investors before undertaking online KYC.

• SEBI has decided to make use of following technological innovations which can facilitate online KYC:

a. eSign: eSign service is an online electronic signature service that can facilitate an Aadhaarholder to forward the document after digitally signing the same provided the eSign signature framework is operated under the provisions of Second schedule of the Information Technology Act and guidelines issued by the controller.

b. e-Document: In terms of PML Rule 2 (1) (cb) "equivalent e-document" means an electronic equivalent of a document, issued by the issuing authority of such document with its valid digital signature, including documents issued to the Digital Locker account of the investor as per Rule 9 of the Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016.

c. Digital Signature: Section 5 of the Information Technology Act, 2000 recognizes electronic signatures (which includes digital signature) and states that where any law provides that information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person then such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of a digital signature affixed in such manner as prescribed by the Central Government. Therefore, the eSign mechanism of Aadhaar shall be accepted in lieu of wet signature on the documents provided by the investor. Even the cropped signature affixed on the online KYC form under eSign shall also be accepted as valid signature.

d. With a view to allow ease of doing business in the securities market, SEBI vide circular dated April 24, 2020, has enabled the Online KYC process for establishing account-based relationship with the RI Investor's KYC can be completed through online / App based KYC, in-person verification through video, online submission of Officially Valid Document (OVD) /other documents under eSign, in the manner specified by SEBI in the circular.

Features for online KYC App of the RI - SEBI registered intermediary may implement their own Application (App) for undertaking online KYC of investors. The App shall facilitate taking photograph, scanning, acceptance of OVD through Digi locker, video capturing in live environment, usage of the App only by authorized person of the RI. The App shall also have features of random action initiation for investor response to establish that the interactions not pre-recorded, time stamping, geo-location tagging to ensure physical location in India etc. is also implemented. RI shall ensure that the process is a seamless, real-time, secured, end-to-end encrypted audiovisual interaction with the customer and the quality of the communication is adequate to allow identification of the customer beyond doubt. RI shall carry out the liveliness check in order to guard against spoofing and such other fraudulent manipulations. The RI shall before rolling out and periodically, carry out software and security audit and validation of their App. The RI may have additional safety and security features other than as prescribed above.

• Feature for Video in Person Verification (VIPV) for Individuals – To enable ease of completing IPV of an investor, intermediary may undertake the VIPV of an individual investor through their App. The following process is to be followed.

1. Intermediary through their authorised official, specifically trained for this purpose, may undertake live VIPV of an individual customer, after obtaining his/her informed consent. The activity log along with the credentials of the person performing the VIPV shall be stored for easy retrieval.
2. The VIPV shall be in a live environment.
3. The VIPV shall be clear and still, the investor in the video shall be easily recognizable and shall not be covering their face in any manner.
4. The VIPV process shall include random question and response from the investor including displaying the OVD, KYC form and signature or could also be confirmed by an OTP.
5. The RI shall ensure that photograph of the customer downloaded through the Aadhaar authentication / verification process matches with the investor in the VIPV.
6. The VIPV shall be digitally saved in a safe, secure and tamper-proof, easily retrievable manner and shall bear date and time stamping.
7. The RI may have additional safety and security features other than as prescribed above.

Whereas, as per PML Rule 2 (1) (bba) "digital KYC" means the capturing live photo of the client and OVD or the

proof of possession of Aadhaar, where offline verification cannot be carried out, along with the latitude and longitude of the location where such live photo is being taken by unauthorized officer of the reporting entity as per the provisions contained in the Act.

Exceptions to In-person Verification:

In order to ease the IPV process for KYC, SEBI circular dated April 24, 2022, states as under:

- IPV/ VIPV would not be required when the KYC of the investor is completed using the Aadhaar authentication / verification of UIDAI.
- IPV / VIPV shall not be required by the RI when the KYC form has been submitted online, documents have been provided through dig locker or any other source which could be verified online.

Further also note that SEBI vide circular no. SEBI/HO/MIRSD/DoP/P/CIR/2022/46 dated April06, 2022 on Guidelines in pursuance of amendment to SEBI KYC (Know Your client) Registration Agency (KRA)Regulations, 2011, SEBI shed light on the role on KRA and Registered Intermediaries as follows:

1. KRAs shall continue to act as repository of KYC data in the securities market and shall be responsible for storing, safeguarding and retrieving the KYC documents and submit to the Board or any other statutory authority as and when required.

2. KRAs shall independently validate records of those clients (existing as well as new) whose KYC has been completed using Aadhaar as an OVD. The records of those clients who have completed KYC using non- Aadhaar OVD shall be validated only upon receiving theAadhaar Number.

3. During the process of validation, KRAs shall validate the following details:

a) Aadhaar through Unique Identification Authority of India (UIDAI) authentication/verification mechanism.

b) Mobile number and e-mail ID using OTP validation (only in cases where mobile number and e- mail ID provided by client are not seeded with Aadhaar) PAN using the Income Tax Database.

c) The KRAs shall develop systems/mechanism, in consultation with SEBI and in co- ordination with each other, and shall follow uniform internal guidelines detailing aspects of identification of KYC attributes and procedures for KYC validation

d) The systems of Registered Intermediaries (RIs) and the KRAs shall be integrated to facilitate seamless movement of KYC documents to and from the RIs to the KRAs

e) KRAs shall promptly inform the respective RIs of deficiency/inadequacy in client's KYC documents, if any, that is observed for validation.

f) On successful completion of KYC validation, a unique client identifier called KRA identifier shall be assigned by KRA to the client and such KRA identifier may be used by the client for opening of account with any other intermediary, without repeating the KYC process.

g) The KYC records of new clients (who have used Aadhaar as an OVD) shall be validated within 2 days of receipt of KYC records by KRAs

h) KYC records of all existing clients (who have used Aadhaar as an OVD) shall be validated within a period of 180 days from July 01, 2022.

i) KRA shall intimate the KRA identifier to the client within 2 working days of receipt of KYC records by the KRAs by post or email and maintain the proof of dispatch.

j) Clients whose KYC records are not found to be valid by KRA after the validation process shall be

allowed to transact in securities market only after their KYC is validated.

k) In case of KYC based on non-Aadhaar OVD, the KRA shall only store such records and the same would not be validated by KRAs unless Aadhaar number is provided by the client.

l) The validation of all KYC records (new and existing) as per the timelines provided in circulars issued from time to time

Procedure to be followed fore-KYC:

In order to enable the Online KYC process for establishing account-based relationship with the SWYOM, Investor's KYC can be completed through online / App based KYC, in- person verification through video, online submission of Officially Valid Document (OVD) / other documents under eSign, in the following manner:

i. The investor visits the website/App/digital platform of the SWYOM and fills up the online KYC form and submits requisite documents online.

ii. The name, photograph, address, mobile number, email ID, Bank details of the investor shall be captured online and OVD / PAN / signed cancelled cheque shall be provided as a photo / scan of the original under eSign and the same shall be verified as under:

a. Mobile and email is verified through One Time Password (OTP) or other verifiable mechanism. The mobile number/s of investor accepted as part of KYC should preferably be the one seeded with Aadhaar. (the RI shall ensure to meet the requirements of the mobile number and email as detailed under SEBI circular no. CIR/MIRSD/15/2011 dated August 02, 2011)

b. Aadhaar is verified through UIDAIs authentication / verification mechanism. Further, in terms of PML Rule 9 (16), every RI shall, where the investor submits his Aadhaar number, ensure that such investor to redact or blackout his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required under sub- rule (15).

RI shall not store/ save the Aadhaar number of investors in their system. e-KYC through Aadhaar Authentication service of UIDAI or offline verification through Aadhaar QR Code/ XML file can be undertaken, provided the XML file or Aadhaar Secure QR Code generation date is not older than 3 days from the date of carrying out KYC. In terms of SEBI circular No. CIR/MIRSD/29/2016 dated January 22, 2016 the usage of Aadhaar is optional and purely on a voluntary basis by the investor.

c. PAN is verified online using the Income Tax Database.

d. Bank account details are verified by Penny Drop mechanism or any other mechanism using API of the Bank. (Explanation: based on bank details in the copy of the cancelled cheque provided by the investor, the money is deposited into the bank account of the investors to fetch the bank account details and name.) The name and bank details as obtained shall be verified with the information provided by investor.

e. Any OVD other than Aadhaar shall be submitted through DigiCert / undersign mechanism.

iii. In terms of Rule 2 (d) of Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 (PML Rules) "Officially Valid Documents" means the following:

a. the passport,
b. the driving licence,
c. proof of possession of Aadhaar number,
d. the Voter's Identity Card issued by Election Commission of India,
e. job card issued by NREGA duly signed by an officer of the State Government and
f. the letter issued by the National Population Register containing details of name, address, or any other document as notified by the Central Government in consultation with the Regulator.

iv. Further, Rule 9(18) of PML Rules states that in case OVD furnished by the investor does not contain updated address, the document as prescribed therein in the above stated Rule shall be deemed to be the OVD for the limited purpose of proof of address.

v. PML Rules allows an investor to submit other OVD instead of PAN, however, in terms of SEBI circular No. MRD/DoP/Cir- 05/2007 dated April 27, 2007 the requirement of mandatory submission of PAN by the investors for transaction in the securities market shall continue to apply.

vi. Once all the information as required as per the online KYC form is filled up by the investor, KYC process could be completed as under:

a. The investor would take a print out of the completed KYC form and after affixing their wet signature, send the scanned copy / photograph of the same to the RI under eSign, or
b. Affix online the cropped signature on the filled KYC form and submit the same to the RI under eSig n.

vii. The RI shall forward the KYC completion intimation letter through registered post/ speed post or courier, to the address of the investor in cases where the investor has given address other than as given in the OVD. In such cases of return of the intimation letter for wrong / incorrect address, addressee not available etc., no transactions shall be allowed in such account and intimation shall also sent to the Stock Exchange and Depository.

viii. The original seen and verified requirement under SEBI circular no. MIRSD/SE/Cir- 21/2011 dated October, 5 2011 for OVD would be met where the investor provides the OVD in the following manner:

a. As a clear photograph or scanned copy of the original OVD, through the eSign mechanism, or;
b. as digitally signed document of the OVD, issued to the DigiLocker by the issuing authority.

ix. SEBI vide circular no. MIRSD/Cir- 26 /2011 dated December 23, 2011 had harmonized the IPV requirements for the intermediaries. In order to ease the IPV process for KYC, the said SEBI circular pertaining to IPV stands modified as under:

a. IPV/ VIPV would not be required when the KYC of the investor is completed using the Aadhaar authentication / verification of UIDAI.

b. IPV / VIPV shall not be required by the RI when the KYC form has been submitted online, documents have been provided through digilocker or any other source which could be verified online.

Feature for Video in Person Verification (VIPV) for Individuals – To enable ease of completing IPV of an investor, intermediary may undertake the VIPV of an individual investor through their App. The following process shall be adopted in this regard:

i. Intermediary through their authorised official, specifically trained for this purpose, may undertake live VIPV of an individual customer, after obtaining his/her informed consent. The activity log along with the credentials of the person performing the VIPV shall be stored for easy retrieval.

ii. The VIPV shall be in a live environment.

iii. The VIPV shall be clear and still, the investor in the video shall be easily recognizable and shall not be covering their face in any manner.

iv. The VIPV process shall include random question and response from the investor including displaying the OVD, KYC form and signature or could also be confirmed by an OTP.

v. The RI shall ensure that photograph of the customer downloaded through the Aadhaar authentication / verification process matches with the investor in the VIPV. The VIPV shall be digitally saved in a safe, secure and tamper-proof, easilyretrievable manner and shall bear date and time stamping.

vi. The RI may have additional safety and security features other than as prescribed above

Ultimate Beneficial Owner(s):

SEBI Master circular no. SEBI/HO/MIRSD/MIRSD-SEC-5/P/CIR/2023/022 dated February 03,2023 elaborates on Client Due Diligence process/ measures as follows:

i. Obtaining sufficient information in order to identify persons who beneficially own or control the securities account. Whenever it is apparent that the securities acquired or maintained through an account are beneficially owned by a party other than the client, that party shall be identified using client identification and verification procedures. The beneficial owner is the natural person or persons who ultimately own, control or influence a client and/or persons on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement;

ii. Verify the client's identity using reliable, independent source documents, data or information;

iii. Identify beneficial ownership and control, i.e., determine which individual(s) ultimately own(s) or control(s) the client and/or the person on whose behalf a transaction is being conducted.

iv. Verify the identity of the beneficial owner of the client and/or the person on whose behalf a transaction is being conducted, corroborating the information provided in relation to (iii);

v. Understand the ownership and control structure of the client;

vi. Conduct ongoing due diligence and scrutiny, i.e., Perform ongoing scrutiny of the transactions and account throughout the course of the business relationship to ensure that the transactions being conducted are consistent with the registered intermediary's knowledge of the client, its business and risk profile, taking into account, where necessary, the client's source of funds;

vii. Registered intermediaries shall review the due diligence measures including verifying again the identity of the client and obtaining information on the purpose and intended nature of the business relationship, as the case may be, when there are suspicions of money laundering or financing of the activities relating to terrorism or where there are doubts about the adequacy orveracity of previously obtained client identification data; and

viii. Registered intermediaries shall periodically update all documents, data or information of all clients

and beneficial owners collected under the CDD process.

In order to comply with the above Act/Rules/Regulations & Guidelines, the following CDD process is being implemented:

I. Identification Process:

(A) For Investors other than Individuals or Trusts:

Where the client is a person other than an individual or trust, viz., company, partnership or unincorporated association/body of individuals, the intermediary shall identify the beneficial owners of the client and take reasonable measures to verify the identity of such persons, through the following information:

aa) The identity of the natural person, who, whether acting alone or together, or through one or more juridical person, exercises control through ownership or who ultimately has a controlling ownership interest;

Explanation: Controlling ownership interest means owner-ship of/ entitlement to:
i. more than 10% of shares or capital or profits of the juridical person, where the juridical person is a company;

ii. more than 15% of the capital or profits of the juridical person, where the juridical person is a partnership; or

iii. more than 15% of the property or capital or profits of the juridical person, where the juridical person is an unincorporated association or body of individuals.

bb) In cases where there exists doubt under clause (aa) above as to whether the person with the controlling ownership interest is the beneficial owner or where no natural person exerts control through ownership interests, the identity of the natural person exercising control over the juridical person through other means;

Explanation: Control through other means can be exercised through voting rights, agreement, arrangements or in any other manner.

cc) Where no natural person is identified under clauses (aa) or (bb) above, the identity of the relevant natural person who holds the position of senior managing official.

(B) For Investor which is a Trust:

Where the client is a trust, the intermediary shall identify the beneficial owners of the client and take reasonable measures to verify the identity of such persons, through the identity of the author of the trust, the trustee, the protector, the beneficiaries with 10%or more interest in the trust or any other natural person exercising ultimate effective control over the trust through a chain of control or ownership shall be considered as beneficial owner.

(C) Exemption in case of listed companies:

Where the client or the owner of the controlling interest is a company listed on a stock exchange or is a majority owned subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.

In case a person has beneficial ownership or control of the investments then the Company would obtain sufficient information in order to verify the identity of such persons. Wherever it is apparent that the units acquired or maintained through an account are beneficially owned by a person other than the investor, the principal i.e. the beneficial owner would be identified using Investor identification and verification procedures. The identity of the beneficial owner would be identified using reliable, independent source documents, data or information. The names of the relevant persons holding senior management position; and the registered office and the principal place of its business, if it is different

(D) Applicability for foreign investors:

Intermediaries dealing with foreign investors' viz., Foreign Portfolio Investors and Qualified Foreign Investors, may be guided by SEBI Master Circular SEBI/HO/AFD-2/CIR/P/2022/175 dated December 19,2022 and amendments thereto, for the purpose of identification of beneficial ownership of the client.

Note: Compliance of the same shall be monitored by their Board of Directors.

9A) Every Banking Company or Financial Institution or intermediary, as the case may be, shall register the details of a client, in case of client being a non-profit organization, on the DARPAN Portal of NITI Aayog, if not already registered, and maintain such registration records for a period of five years after the business relationship between a client and a reporting entity has ended or the account has been closed, whichever is later.

(9B) Where the client has submitted any documents for the purpose of sub-rule (1), it shall submit to the reporting entity any update of such documents, for the purpose of updating the records mentioned under sub-rules (4),(5),(6),(7),(8) or (9), as the case may be, within 30 days of such updating

"Non-profit organization" means any entity or organization, constituted for religious or charitablepurposes referred to in clause (15) of section 2 of the Income-tax Act, 1961 (43 of 1961), that is registered as a trust or a society under the Societies Registration Act, 1860 (21 of 1860) or any similar State legislation or a Company registered under the section 8 of the Companies Act, 2013 (18 of 2013);

Aadhaar based e-KYC:

SEBI circular dated October 8, 2013, enables Aadhaar based e-KYC service offered by UIDAI for KYC verification on authorization by the client to the intermediary on a voluntary basis. e-KYC isdone with the help of an investor's Aadhaar number. While completing the e-KYC, the authentication of the investor's identity can be done as follows:

Via Biometrics (No limit on the investment amount here unless those specifically imposed by the scheme/Fund house). SWYOM shall take all reasonable steps to ensure that KYC information is collected and kept up-to- date, and that identification information is updated when changes occur with respect to the investor. Further the data is required to be maintained for 5 years.

Investment Manager shall implement accepting of Aadhaar and implementation of Central KYC requirements as notified by the regulators from time to time.

SEBI vide circular No. CIR/MIRSD/29/2016 dated January 22, 2016, had clarified that the usage of Aadhaar as issued by the UIDAI is optional and on a voluntary basis.

Whereas, The Department of Revenue (DoR), Ministry of Finance vide its circular dated May 09,2019 stated that if the Central Government (CG) is satisfied that a reporting entity other than banking company, complies with such standards of privacy and security under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, and it is necessary and expedient to do so, it may by notification, permit such entity to carry out authentication of the Aadhaar number of clients using e-KYC authentication facility. However, CG shall not issue any notification in this behalf without consultation of the appropriate Regulator and Unique Identification Authority of India ("UIDAI").

In line with the above decision, Government of India, DoR, vide Gazette Notification No. G.S.R. 261(E) dated April 22, 2020 has notified nine reporting entities as per the recommendation by UIDAI and SEBI to undertake Aadhaar authentication service of the UIDAI under section 11A of the Prevention of Money-laundering Act, 2002. In view of the same, 9 entities have been authorised to undertake Aadhaar Authentication service of UIDAI subject to compliance of the conditions as laid down.

These entities shall get registered with UIDAI as KYC user agency ("KUA"). Thereafter, the SEBI registered intermediaries, who want to undertake Aadhaar authentication services through KUAs, shall enter into an agreement with KUA and get themselves registered with UIDAI as sub-KUAs.

Establishing business relationship with Politically Exposed Persons:

SEBI circular SEBI/HO/MIRSD/MIRSD-SEC-5/P/CIR/2023/022 dated February 03,2023 defines Politically Exposed Persons (PEPs) as individuals who are or have been entrusted with prominent public functions in a foreign country, e.g. Heads of States or of Governments, senior politicians, senior government / judicial / military officers, senior executives of state-owned corporations, important political party officials etc. Family members or close relatives of such individuals are also considered as PEPs.

SEBI Master Circular dated December 19, 2008 on Anti Money Laundering (AML) and Combating Financing of Terrorism (CFT) - Obligations of Intermediaries under Prevention of Money Laundering Act, 2002 necessitates Portfolio Management Services to obtain senior management approval for establishing business relationship with PEPs and their close relatives / accounts of family members. Where a customer has been accepted and is subsequently found to be, or subsequently becomes a PEP, Investment Manager must obtain AML Committee approval having representation from senior management to continue the business relationship. Reasonable measures to verify the sources of funds as well as the wealth of clients and beneficial owners identified as PEP shall be taken.

Further, the client shall be identified by the intermediary by using reliable sources including documents / information. The intermediary shall obtain adequate information to satisfactorily establish the identity of each new client and the purpose of the intended nature of the relationship. The information must be adequate enough to satisfy competent authorities (regulatory / enforcement authorities) in future that due diligence was observed by the intermediary in compliance with the directives. Lastly, failure by prospective client to provide satisfactory evidence of identity shall be noted and reported to the higher authority within the intermediary.

Establishing Identity

What is identity?

Identity generally means a set of attributes which together uniquely identify a natural or legal person. For example, an individual's identity comprises his/her name including all other names used, the residential address at which he/she can be located and his/her photograph.

Date of birth is also important as an identifier in support of the name and is essential to law enforcement agencies in an investigation.

Whose Identity Should Be Verified?

Identification evidence should usually be verified for:

- the named account holder(s)/the person in whose name an investment is registered;
- any principal beneficial owner of funds being invested who is not the account holder or named investor;

The failure or refusal by an applicant to provide satisfactory identification evidence within a reasonable time scale and without adequate explanation may lead to a suspicion that the depositor or investor is engaged in money laundering. In such circumstances, SWYOM would consider making a suspicious activity report.

Identification Procedures: General Principles:

SWYOM shall establish to its satisfaction that they are dealing with an individual or an entity and obtain identification evidence sufficient to establish that the applicant is that individual or entity. When reliance is being placed on any third party to identify or confirm the identity of any applicant, the overall legal responsibility to ensure that the procedures and evidence obtained are satisfactory rests with the SWYOM. Further, as per SEBI master circular dated February 03, 2023, reliance shall be subject to the conditions that are specified in Rule 9 (2) of the PML Rules and SEBI Regulations issued from time to time.

Accordingly, in terms of Rule 9(2) of PML Rules:

a. The registered intermediary shall immediately obtain necessary information of such client due diligence carried out by the third party;
b. The registered intermediary shall take adequate steps to satisfy itself that copies of identification

c. data and other relevant documentation relating to the client due diligence requirements will be made available from the third party upon request without delay;

d. The registered intermediary shall be satisfied that such third party is regulated, supervised or monitored for, and has measures in place for compliance with client due diligence and record- keeping requirements in line with the requirements and obligations under the Act;

e. The third party is not based in a country or jurisdiction assessed as high risk;

SWYOM shall further add a clause in the Service Level Agreement (SLA) with the RTA to cover the adherence of PMLA Rules relating to verification of the client's identity and address.

It is important that the procedures adopted to verify identity are sufficiently robust whether the procedures are being undertaken face-to-face or remotely. Reasonable steps should be taken to avoid single or multiple fictitious applications or substitution (impersonation) fraud for the purpose of money laundering.

Identification - General

Establishing and retaining documentary evidence of the true identity (and address) of investor is a critical part of the KYC regime. It is essential that we are satisfied that investors are who they claim to be and that they are not conducting business in fictitious names, possibly to disguise their involvement in illicit activity.

Reasonable steps must therefore be taken, by obtaining and verifying sufficient evidence of identity, to be able to show that an investor, or potential investor, is who they claim to be. Where the investor is, or appears to be, acting on behalf of another, sufficient identification evidence must be obtained in respect of both parties. These steps must be taken as soon as possible after contact with an investor or potential investor is made with a view to carrying out a transaction or reaching an understanding to carry out a transaction.

Identification - Exceptions

a) Under exceptional circumstances, where it is essential to conduct business before full documentary evidence of identity has been obtained, the reasons for the exception must be recorded in the investor's file and the exception resolved as a matter of urgency.

b) Business must not be continued with investors who fail to produce satisfactory evidence of their identity. This applies to one-off transactions as well as proposed new account relationships.

c) An undue delay by an investor in providing satisfactory proof of identity, without adequate explanation, might be viewed as grounds for suspicion that the person concerned is involved in money laundering and consideration should be reported.

d) Note that the exceptions do not apply if there is any knowledge or suspicion that the investor or potential investor may be involved in money laundering.

KYC for Specific Investor Categories

The following sections summaries KYC and identification standards for the most common investor categories. For any other (specialized) investor category, not specified below, KYC and identification procedures adopted must be in line with the Company Policy and local law and regulation.

Individual investors

1. Identification evidence (including evidence of addresses) must be obtained and retained on file, for all parties to an account, including any beneficial owner of funds who may not be a signatory to the account. Identification evidence must also be retained for any intermediate parties where an account is managed or owned by an intermediary.
2. Clear, legible copies of all relevant pages of identification documents must be retained on investor files.
3. For Clients with a higher risk profile such as proprietorships, partnerships, NRIs, trusts and private limited companies, mandatory documents have been specified in addition to the introduction/ identification requirement.

4. Whenever possible, identification evidence should be provided by the investor at a face-to-face meeting before an account is opened. Where verification of identity cannot be completed face to face, copy of passports or identity cards suitably certified by another correspondent bank, or diplomatic mission, may be acceptable.

Individual Investors - Evidence and Verification of Addresses

As per the PMLA (Maintenance of Records) Rules, 2005, copies of documents and a record of the manner in which address verification was achieved must be retained in Investor files. Only 'officially valid document or OVD' as prescribed under PMLA (Maintenance of Records) Rules 2005, shall be accepted by SWYOM. OVD in this regard shall mean the following:

(a) Passport

(b) Driving Licence

(c) Voters Identity card issued by Election commission of India

(d) Job card issued by NREGA duly signed by an officer of the state government of name, addressor any other document as notified by the Central Government.

(e) proof of possession of Aadhaar number

(f) the letter issued by the National Population Register containing details of name, address or any other document as notified by the Central Government in consultation with the Regulator,

the Permanent Account Number (PAN) Card (mandatory as per SEBI Circular dated April 24, 2020 for transacting in the securities market.

Provided that where simplified measures are applied for verifying the identity of the clients the following documents shall also be deemed to be 'officially valid documents':

(a) identity card with applicant's Photograph issued by Central/State Government Departments, Statutory/Regulatory Authorities, Public Sector Undertakings, Scheduled Commercial Banks, and Public Financial Institutions;

(b) letter issued by a gazette officer, with a duly attested photograph of the person;

In case of officially valid document furnished by the client does not contain updated address, or where simplified measures are applied for verifying the limited purpose of proof of address of the clients or where a prospective customer is unable to produce any proof of address, then the following documents or their equivalent e-documents thereof shall be deemed to be officially valid documents for the limited purpose of proof of address:

(a) utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);

(b) property or Municipal tax receipt;

(c)pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;

(d) 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:

Provided that the client shall submit updated officially valid document or their equivalent e- documents thereof with current address within a period of three months of submitting the above documents.

Where a client has provided his Aadhaar number for identification under clause (a) of above and wants to provide a current address, different from the address as per the identity information available in the Central Identities Data Repository, he may give a self-declaration tothat effect to the reporting entity.

Provided also that in case the OVD presented by a foreign national does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address.

Provided also that where the client submits his proof of possession of Aadhaar number containing Aadhaar Number as an officially valid document, it shall be ensured that such client redacts or blacks out his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required.

[Explanation. - For the purpose of this clause, a document shall be deemed to an *"officially valid document"* 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.

Individual Investors - Minors and Students

1.In some circumstances, accounts for minors are opened by adult family members. In these circumstances, identity evidence for the guardian, or anyone else operating the account, should be obtained together with a copy of the birth certificate or passport of the minor.
2.For students, evidence of identity and address verification should be obtained in the normal way as far as is possible. Where this proves impractical however, verification can be obtained through a parent or the prospective Investor's college or university.
3.On no account must numbered or alternate name accounts be used even where the identity of the underlying Investor has been established and recorded. To offer such facilities runs contrary to international initiatives to promote transparent banking designed to assist the prevention of money laundering.

Trusts, Nominee Companies and Fiduciaries

1. Money launderers may view the anonymity and complex structures associated with some types of Trust arrangement as providing an opportunity to avoid identification procedures and conceal the origin of funds.
2. It is therefore essential to verify the identity of the settlor of the Trust (i.e. the person supplying the funds), those who have control over the funds, beneficiaries, and any person who has authority to remove the Trustees. Exceptionally, identification requirements may be waived for any Trustee who does not operate an account or give instructions relating to fund transfers. Whenever a Trustee is replaced, the identity of the new Trustee should be verified before they are allowed to exercise control over the funds.
3. Whenever funds are received on behalf of a Trust the source of the funds must be properly identified, and the nature of the transaction understood (reasonable exceptions may be allowed in the case of regular receipts from the same, previously identified source).
4. For discretionary and offshore Trusts, the nature and purpose of the Trust as well as the original source of funding must be ascertained.
5. Particular care must be taken when Trusts are set up in offshore locations where strict banking secrecy prevails. Trusts set up in jurisdictions where no money laundering legislation or regulation exists will also warrant additional enquiries and measures. Steps should be taken to obtain written confirmation from the trustees or managers of the Trust that there are no anonymous principals. The original source of the funding should also be established.
6. Any application to open an account or undertake a transaction on behalf of another without the applicant identifying their Trust or nominee capacity should be regarded as suspicious and treated accordingly.

Corporate Investor

1. Companies can be established with the sole purpose of laundering money, or illicit money can be passed through the accounts of otherwise legitimate companies. The KYC process must ensure the company is not merely a 'brass plate' company set up to facilitate money laundering.
2. For corporate Investors (and subsidiaries of such Investors) quoted on a nationally approved and regulated stock exchange there is no need to verify the identity of individual shareholders or directors beyond what might form part of normal commercial due diligence. Evidence of this special "exchange listed" status must be recorded

on file.

For private, unquoted, companies, in addition to verifying the legal existence of the business, including its registered address, it is essential to identify those who have control over the company and its assets. Therefore, the identity of all beneficial owners, directors and any other persons with control over the company's assets should be verified in line with the requirements for individual Investors (above).

3. The identity of all signatories to a business relationship must also be verified in line with individual
4. Investor standards where they have a mandate to provide instructions involving any transaction.

Powers of Attorney and Third-Party Mandates

1. The authority to deal with assets under a Power of Attorney or Third-Party Mandate constitutes a business relationship and therefore any person fulfilling that role must also be identified in the same manner as the primary Investor. A copy of such Power of Attorney must be obtained and verified with the original
2. New powers of attorney for corporate or Trust businesses should always be verified, and it is important that the reason for granting the power of attorney is understood and recorded.

Unincorporated Businesses/Partnerships

1. Where they do not already hold personal Bank accounts, identification evidence must be obtained for the principal beneficial owners or controllers of these types of business. This may include identifying signatories to whom significant control has been delegated. Whereas formal partnership arrangement exists, a mandate authorising the opening of the account and the issuing of instructions for transactions should be obtained.

2. Evidence of the trading address must be obtained. It must also be established that the business or partnership has a legitimate purpose by, for example, a visit to the trading address to confirm the true nature of the business activities. For established businesses, a copy of the latest report and accounts should be obtained.

Financial Institutions

1. It is essential to determine that a financial institution with which a relationship is proposed, is properly constituted, is supervised and regulated by an acceptable regulatory authority and in addition to normal business considerations, is an institution with which we would wish to be associated from a reputational perspective.
2. Discretion should be exercised as to whether these documents should be notarized. Consideration should also be given as to whether it is necessary to check the institution with the relevant regulator, a known correspondent in a suitably regulated country.
3. Relationships must not be established with “Shell Banks” that have no physical presence in any country, or with correspondents that allow their accounts to be used by such institutions.

Financial Institutions Acting as Agents

Where a Client of the Bank, “A”, acts as an agent for an underlying Client “B”, the identity of both “A” and “B” must be verified in accordance with these Standards. However, a copy of the legal mandate for the Bank to act on behalf of its client for investment should be obtained for our records and the same must be verified with the original.

The KYC requirement for non-individual investor shall be as prescribed by SEBI / Prevention of Money Laundering (Maintenance of Records) Rules, 2005 as amended from time to time.

Monitoring Conduct of the account

In line with KYC guidelines, SWYOM will continuously develop and implement appropriate methods of monitoring so that throughout the Investor relationship, suspicious Investor activity can be detected, appropriate action can be taken, and reports made to the regulatory authorities in accordance with laid down procedures.

Treatment of Financial and Non-Financial transactions in respect of persons/ entities debarred by SEBI for

accessing securities market

SEBI from time-to-time issues orders debarring certain entities/ persons from accessing the capital markets or dealing in securities for a specific period in accordance with provisions of SEBI (Procedure for Holding Inquiry by an Enquiry Officer and Imposing Penalty) Regulations, 2002,

SWYOM shall process financial and non-financial transactions in respect of persons/entities debarred by SEBI, as per the orders issued by SEBI in this regard.

Record Retention

Under the Act and Guidelines, all intermediaries have an obligation of maintaining and preserving client and transactions related records. All necessary records on transactions, client documentation and business correspondence etc., should be maintained at least for the minimum period prescribed under the relevant Act and Rules (PMLA and rules framed there under as well SEBI Act) and other applicable legislations, Regulations or exchange bye-laws or circulars. Records must be made available at all times for inspection by auditors and regulators. Further, registered intermediaries shall maintain such records as are sufficient to permit reconstruction of individual transactions (including the amounts and types of currencies involved, if any) so as to provide, if necessary, evidence for prosecution of criminal behavior. In case of any suspicious transaction, the competent investigating authorities would need to trace through the audit trail for reconstructing a financial profile of such transaction. Hence proper record keeping, and retention should be adopted. Records confirming the identity of customers and beneficial owners as well as account files and business correspondence shall be maintained and preserved for a period of five years after the business relationship between a client and the AMC has ended or the account has been closed, whichever is later.

1. the beneficial owner of the account
2. volume of the funds flowing through the account and
3. For selected transaction:

- origin of funds
- form in which the funds were offered or withdrawn i.e. cheques, wire transfer, drafts.
- identity of person undertaking the transaction
- destination of the funds
- form of instruction and authority, etc.

Records may be retained in hard copy, on microchip or computer, or another electronic format. The documents should be kept updated and should be readily and quickly made available to the investigating authorities.

Care should be taken to ensure that transactional records are not lost before the year retention period expires as a direct consequence of automatic data retention constraints.

Documentary evidence of any action taken in response to internal and external reports of suspicious transactions must also be retained for at least 5 years. Where it is known that an investigation is ongoing, the relevant records should be retained until the authorities inform the SWYOM otherwise.

Where business is refused because of a failure to meet these Standards or other local anti-money laundering requirements, a record of the refusal should be retained for years (no record is required where business is refused on purely commercial grounds)

Wire Transfers/Electronic Fund Transfers

Particular attention must be paid to the adequacy of information contained in records relating to electronic fund transfer instructions. These offer money launderers the opportunity to speedily disperse funds to different jurisdictions making subsequent tracing and investigation difficult. To assist investigating authorities, all electronic payment messages, both domestic and international should, subject to any technical limitations, contain the full name, account number and address of the ordering Investor and beneficiary in the respective message fields. Where this information

is not contained in electronic payment messages, full records must be retained by the originating office (this does not apply to inter-bank transfers). These records must be retained as stated above

Cash transactions

As per the policy, SWYOM does not entertain cash transactions.

Investor Education

SWYOM may be required to seek documents under KYC and additional documents post due diligence, hence it essential that client understands the AML obligation casted upon financial intermediaries. Information providing AML requirements shall be hosted on website.

Any additional information for understanding AML requirements shall be provided upon request from Investor.

Recognising and Reporting Suspicious Transaction/Activity

What is meant by "suspicion"?

The Rules notified under the PMLA defines a "suspicious transaction" as a transaction whether or not made in cash which, to a person acting in good faith -

a) gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or
b) appears to be made in circumstances of unusual or unjustified complexity; or
c) appears to have no economic rationale or Bonafede purpose; or
d) gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism".
e) Any other criteria as decided by the Principal Officer for generating STR alerts. Explanation. - Transaction involving financing of the activities relating to terrorism includes transaction involving funds suspected to be linked or related to, or to be used for terrorism,
f) terrorist acts or by a terrorist, terrorist organization or those who finance or are attempting to finance terrorism.

Additionally, SEBI circular dated February 03, 2023 provides a list of circumstances which may be in the nature of suspicious transactions. This list is only illustrative and whether a particular transaction is suspicious or not will depend upon the background, details of the transactions and other facts and circumstances:

g) Clients whose identity verification seems difficult or clients that appear not to cooperate
h) Asset management services for clients where the source of the funds is not clear or not in keeping with clients' apparent standing /business activity;
i) Clients based in high-risk jurisdictions;
j) Substantial increases in business without apparent cause;
k) Clients transferring large sums of money to or from overseas locations with instructions for payment in cash;
l) Attempted transfer of investment proceeds to apparently unrelated third parties;
m) Unusual transactions by CSCs and businesses Undertaken by offshore banks/financial services.

Accordingly, Investment Manager may conduct Enhance Due Diligence (EDD) in the following circumstances:

1. Clients of high-risk countries, including countries where existence and effectiveness of money laundering controls is suspect or which do not or insufficiently apply FATF standards shall be subject to appropriate counter measures and such clients to be categorized as 'CSC'.
2. EDD may be conducted in addition to other disciplinary actions in case where an individual or

entity's name is getting tagged in 'Debarred list of entities/ individuals' released by BSE &NSE from time to time.

3. EDD may be conducted in case of Disqualified Companies and that of directors on the board of such companies.

4. EDD may be conducted in case the Ultimate Beneficial Owner (UBO) is a PEP.

Note that the above is not an exhaustive list, and Investment Manager may at its discretion conducted on case-to-case basis. Therefore, Investment Manager may include a further enhanced scrutiny of transactions, enhance relevant reporting mechanisms or systematic reporting of financial transactions, and applying enhanced due diligence while expanding business relationships with the identified country or persons in that country etc.

Further, while undertaking EDD a Investment Manager shall ensure the following:

1. EDD shall be conducted at client level only within the same Investment Manager,
2. In case of Individual, EDD once conducted shall be valid for a period of 2 years, and
3. In case of non-individual, EDD once conducted shall be valid for a period of 2 years or until the authorized signatory has changed (in case of joint account and non-individual investor investing), which is earlier.

The provisions of the PMLA place an obligation on Fund and Investment Manager to furnish information in respect of suspicious transactions. The Registrar and Transfer Agent(s) of the Fund, will provide the transactions which fall under the criteria of suspicious transactions, as specified under PMLA regulations or as per the criteria's provided by the Principal Officer and report the same to Principal Officer, on periodical basis.

The Principal Officer shall review the said reported transactions and place the same before AML Committee along with recommendation for final decision with regard to report any transaction as suspicious to FIU within 7 working days of decision of AML Committee.

Suspicion is personal and subjective and falls far short of proof based on firm evidence. Suspicion may be defined as being beyond mere speculation and based on some foundation i.e. "A degree of satisfaction and not necessarily amounting to belief but at least extending beyond speculation as to whether an event has occurred or not"; and "Although the creation of suspicion requires a lesser factual basis than the creation of a belief, it must nonetheless be built upon some foundation."

Refer to **Annexure B** for the criteria for determining Suspicious Transactions.

Any suspicious transaction shall be immediately notified to the Designated/Principal Officer within the intermediary. The notification may be done in the form of a detailed report with specific reference to the clients, transactions and the nature /reason of suspicion. However, it shall be ensured that there is continuity in dealing with the client as normal until told otherwise and the client shall not be told of the report/ suspicion. In exceptional circumstances, consent may not be given to continue to operate the account, and transactions may be suspended, in one or more jurisdictions concerned in the transaction, or other action taken. The Designated/ Principal Officer and other appropriate compliance, risk management and related staff members shall have timely access to client identification data and CDD information, transaction records and other relevant information.

Accordingly, for SWYOM, such reporting to be done before the AML committee, which is constituted as stated above.

Internal Reporting of Suspicious Transactions

There is a statutory obligation on all staff to report to the Principal Officer transactions where they have knowledge, suspicion or reasonable grounds for knowledge or suspicion of money laundering.

1. SWYOM must take reasonable steps to ensure that any member of staff who handles or is responsible for handling transactions which may involve money laundering, makes a report promptly to the Principal Officer if he knows or suspects or has reasonable grounds to know or suspect that a client or the person on whose behalf the client is acting, is engaged in money laundering.
2. The steps to be taken under (1) include arrangements for disciplining any member of staff who fails, without adequate reason, to make a report of the kind envisaged in this section.

Tipping off

An important element to the success of the AML process is that the investor should not be informed (i.e. tipped off) that his/her accounts are under monitoring for suspicious activities and/or that a disclosure has been made to the designated authority namely Financial Intelligence Unit, India. (FIU-IND).

SWYOM can however make normal enquiries to learn more about the transaction or instruction to determine whether the activities of the customer arouse suspicion.

Where it is known or suspected that a suspicion report has already been made internally or externally, and it then becomes necessary to make further enquiries, care must be taken to ensure that the suspicion is not disclosed either to the investor or to any other third party. Subject to internal procedures, such enquiries should normally/only be made as directed by the Principal Officer.

REPORTING SUSPICIOUS TRANSACTIONS

SWYOM will:
"Make prompt reports of suspicious transactions, or proposed transactions, through the appropriate internal channels and, were, to the relevant authorities".
"co-operate with any lawful request for information made by government agencies during their investigations into money laundering.

Internal Reports
As an internal policy all employees of SWYOM should report suspicions, where it is considered necessary for a report to be passed first to his immediate supervisor or manager and in turn would be passed promptly, without delay, to the Principal Officer. In case of exigencies, such employee can directly report the same to the Principal Officer. The AML committee must in its judgment decide on the merit of the reporting of such cases found to be suspicious. Once an employee has reported his/her suspicion to the Principal Officer he/she has satisfied the obligation. All reports should be documented. However, the employees should ensure that the above are not used to prevent reports reaching the Principal Officer whenever staff have stated that they have knowledge or suspicion that a transaction may involve money laundering.

In case an employee fails, without reasonable excuse, to make a report or who blocks, or attempts to block, a report by another member of staff, then necessary disciplinary action would be taken against them.

The Principal Officer has been entrusted with the responsibility of collating and reporting transactions prescribed under the Rules notified. All internal reports of suspicious transactions should be considered by the AML Committee, and these should be reported externally if he has reasonable grounds to suspect, as specified in the Rules notified.

For the purpose of determining whether an individual or transaction is suspicious and reportable to FIU-IND, review and assessment can also be done based on client data available at a group- level.

In reaching a decision concerning a suspicion report, the AML Committee should take reasonable steps to consider all relevant KYC information available within the SWYOM concerning the person or business to which the initial report relates. This may include, as part of reviewing they information/ investor profile:

- Transaction pattern of the client (complexity of transactions if any)
- Status of client (resident individual / non-resident / non-Individual)
- Value of investment
- Type of product / service availed by the client
- Location of the client's domicile
- Client's business or profession
- Manner of remittance of funds
- Dubious background of clients (based on publicly available information)

As part of the review, the Principal Officer may choose to relate the transaction to other connected accounts or relationships. However, any need to search for information concerning connected accounts or relationships should not delay the making of a report.

If after completing this review, the Principal Officer decides that there are grounds for knowledge, suspicion or reasonable grounds to suspect money laundering, then the Principal Officer must disclose the information to AML Committee as soon as practicable after the disclosure was received in order to avoid committing an offence of failure to disclose. Nevertheless, care should be taken to guard against a report being submitted as a matter of routine without undertaking reasonable internal enquiries to determine that all available information has been taken into account. The officer will be expected to act honestly and reasonably and to make his/her decisions in good faith. The decision whether or not to report must not be subject to the consent or approval of any person other than the Principal Officer.

The Principal Officer shall within seven working days to the Financial Intelligence Unit, India (FIU-IND) from the date of decision of AML Committee that such transaction was suspicious.

Accounts where suspicious transactions have been reported to the FIU-IND may be reclassified as High Risk / Monitored closely. Following the reporting of a suspicious transaction, SWYOM should continue to be vigilant in monitoring further transactions in such accounts. However, the PO may, after a period of time, based on further developments in the account, remove such accounts from a high-risk classification**.**

Transaction Monitoring / Review

On an ongoing basis, the SWYOM may carry out scrutiny of clients especially clients in special categories / high risk categories, throughout the course of its business relationship in terms of AMFI criteria to ensure that the transactions being conducted are consistent with the Investment Manager knowledge of the client, its business and risk profile and also the source of funds. Anything unusual about clients/ transaction pattern based on a set of internal parameters and various combinations of information will be closely monitored. If required, additional information for enhanced KYC purposes should be sought within a reasonable timeframe. All investigations for ascertaining suspicious transactions are dependent on the reasons for the STR alert and other factors mentioned elsewhere in this document. Multiplicity and complexity along with the value of the transactions may generally form the basis of reporting, other than adverse publicly available information. Alerts should not be sent to FIU-IND without appropriate scrutiny and affirmation that the transaction is suspicious in nature, backed by reasons.

Reporting for receipts from Non-Profit Organization

- SWYOM is required to furnish NTRs in respect of transactions involving receipts of value more than Rs. 10 lakhs or its equivalent in foreign currency by their clients who are non- profit organizations to FIU-IND by the 15th day of the succeeding month.
- NTRs must contain details of legal persons since, as per definition under Rule 2(1) (ca) of the Money Laundering (Maintenance of Records) Rules, 2005, a non-profit organization means any entity or organization that is registered as a Trust or a society under the Societies Registration Act, 1860 or any similar State legislation or a company registered under section 25 of the Companies Act, 1956. Keeping in view this definition, list of customers is reviewed at the time of on-boarding clients to identify and tag NPO accounts.
- Transactions of a single account should be given in report along with details of the legal entity, individuals, account and transaction on lines similar to those for CTRs.
- Separate NTR is required to be filed for each NPO account. Transactions of unrelated clients should not be clubbed in one report.

NOTE: No nil reporting needs to be made to FIU-IND in case there are no cash/suspicious/non- profit organization transactions to be reported.

AWARENESS AND TRAINING

The Company will raise awareness on money laundering prevention and train our staff about what money laundering is, the recognition of suspicious transactions, the requirements of local regulation and legislation, the Company's

Policy and Standards on the prevention of money laundering, and the procedures and controls in each jurisdiction".

General

1. It is the responsibility of the business to ensure that procedures are in place to raise general employee awareness on money laundering prevention on an ongoing basis and that periodic, more job specific, training is provided to relevant staff.

2. The term "relevant staff" should be given the widest possible interpretation and will include staff involved in activities from account opening and providing advice to Investors, through to all aspects of transaction processing. Temporary, part time and contract staff must be included.

Raising Awareness and Providing Information

1. During the course of normal induction procedures, all new staff must, as a minimum, be made aware of their basic responsibilities for the reporting of suspicious transactions.
Thereafter, on periodic basis, "relevant staff" who, for example, handle, or are managerially responsible for the handling of, transactions which may involve money laundering, must be made aware of:

- what is expected of them and the consequences for the Company and for themselves if they fall short of expectations i.e. the potential effect on the Company, its employees and its clients, of any breach of the law.
- policies, procedures and controls in place in their business to prevent money laundering
- the requirements of relevant legislation and regulations, including, where appropriate, a clear understanding of their own potential legal liability and the implications of processing
- "suspect" transactions without the approval of the authorities, or deciding not to process such transactions.
- their responsibilities under the Company's arrangements for money laundering
- prevention, including those for obtaining sufficient evidence of identity, recognizing and reporting knowledge or suspicion of money laundering and the use of national and international findings on countries with material deficiencies.

2. Awareness can be raised using a variety of methods. Written information on the above topics should be available (in hard copy or electronically) to all staff from the time they join a relevant role to the time they leave. Appropriate materials will vary across different businesses and countries; from a full handbook of policy, procedures, and regulations, to a simple awareness leaflet.

Training

In addition to providing information and raising general awareness on an ongoing basis, periodic job specific and more detailed training must be provided to "relevant staff". Training requirements shall have specific focuses for frontline staff, back-office staff, compliance staff, risk management staff and staff dealing with new clients. It is crucial that all those concerned fully understand the rationale behind these directives, obligations and requirements, implement them consistently and are sensitive to the risks of their systems being misused by unscrupulous elements. The content of the training will vary to take account of different roles and levels of seniority.

Treatment of Deficient and incomplete Applications

Further, as the Client Identification process involves collecting and verifying of proof of identity / Address as well as checking of some details disclosed in the Application Form, it may not be possible to complete the process across the counter while accepting transactions. There could, therefore, be instances of detecting deficiencies in the documentation after accepting of the transactions. In such cases, the application may have to be rejected

Investor Education:

Implementation of AML/CFT measures requires registered intermediaries to demand certain information from investors which may be of personal nature or has hitherto never been called for. Such information can include documents evidencing source of funds/income tax returns/bank records etc. This can sometimes lead to raising of questions by the client with regard to the motive and purpose of collecting such information. There is, therefore, a need

for registered intermediaries to sensitize their clients about these requirements as the ones emanating from AML and CFT framework. Registered intermediaries shall prepare specific literature/ pamphlets. so as to educate the client of the objectives of the AML/CFT programmed.

Amendments to the Policy

The policy shall be ideally reviewed once in a year. In case of any regulatory changes between the two review cycles, the policy shall be deemed as amended in accordance with the changes in regulations. In other words, in case of conflict between Regulations and this policy, the regulations shall prevail.

ANNEXURE A

Risk Parameter	**Associated Rating (0 being lowest and 10 being highest)**	**Weight age (%) [Tota should be 100]**
Tax Status		**10**
Bank / Financial Institution	0	
Provident Fund / EPF	0	
Superannuation Fund	0	
Gratuity Fund	0	
Pension Fund	0	
NPS Trust	0	
Foreign Portfolio Investor – Category I	0	
Individual	1	
On Behalf of Minor	1	
HUF	1	
Sole Proprietorship	1	
Public Sector undertakings /government undertaking /	2	
Insurance Companies	2	
Partnership Firm	3	
Body Corporate	4	
Society	4	
Foreign Portfolio Investor – Category II	5	
AOP/BOI	5	
Limited Liability Partnership	5	
Private Family Trust	6	
Foreign Investor	7	
Foreign Portfolio Investor – Category III	8	
Other Trust	8	
NRI Through NRO A/c	8	
NRI	8	
NRI – Others	8	
Non-Resident Minor	8	
Non-Resident HUF	8	
Charitable Trust	10	
Others	10	

Occupation	**10**
Service	1
Retired	1
Professional	5
Business	7
Housewife	7
Senior citizen / Retired	7
Student	7
Agriculture	4

Business - Arms Dealer, Money Chan Exchang Houses, Gems/ Jewellery/ Preci metals/ Bullion dealers (including sub-deale Real Estate Agents Construction, Offsh Corporation, Art/ antique dealers, Restaurant/ B Casino/ Night club Import/ Export age (traders, goods not used fo own manufacture retailing), Share & Stock broker, Transp Operators, Auto dealers (used recondition vehicles/ motorcycles), Scrap meta dealers.	10
Others	10

PEP Status	**15**
No	1
Yes	10

KYC Validated	**10**
Yes	1
No	8

Investment amount (single investment)	**10**
Upto 1 cr	1
>= 1 Crore < 2.5 Crore	2
>= 2.5 Crore < 5 Crore	3
>= 5 Crore < 10 Crore	4
=>10 Crore <20 Cr	5
=>20 Cr and above	6

Country of Residence	**10**
North Korea	5
Iran	5
OFAC sanctions list	5
FATF sanctions list	5
Other Countries	1

Bank accounts held [Inv. + Redemption]	**5**
Upto 3	0
3 to 5	4
> 5	8

World Check / UNSC / MHA Listed	**20**
No	0
Yes	10

Accounts held [as 1st holder]	**5**
<= 5	1
5 to 10	4
>10	7

Accounts held [as JHs]	**5**
<= 5	1
5 to 10	4
>10	8

Computation of Risk Rating (0 being lowest and 10 being highest

Step 1	Compute the rating in each risk parameters the product of the associated rating and weight age
Step 2	Add the rating for each risk parameter to arrive the total risk rating
Step 3	Classify Risk Rating of up to **1.5** as **"Low"**, **1.5 to 2.5** as **"Medium"** and above **2.5** as **"High"**

Examples	
Example 1	An individual businesswoman with no politic affiliations (as per KYC declarations), featuring in any negative lists, residing in Kan who has made 1
Rating: (1*0.10) + (7*0.10) + (1*0.15) + (1*0.10) + (1*0.10) + (1*0.10) + (1*0.10) + (0*0.20 + (7*0.05) + (1*0.05) which results in a total rating of 1.75	
Example 2	An NRI into service with no political affiliati (as per KYC declarations), not featuring in a negative lists, residing in Iran and holding 1 fo and has made an investment of INR 2 Crs. holds 6 bank accounts, 1 folio as 1st holder and as 2ndholder.
Rating: (8*0.10) + (1*0.10) + (1*0.15) + (1*0.10) + (2*0.10) + (5*0.10) + (8*0.05) + (0*0.20) + (1*0.05) + (5*0.05) which results in a total rating of 2.7	

Sr. no.	Particulars	Alert Details
1	Additional investment of more th INR 1cr (individuals) and INR (non-individuals)	An amount of 10 or more times (of the upper band of the annual income) specified by the investor in the KYC form.
2	PEP status	Investors tagged as PEP in KYC data
3	Change of bank accounts andaddress	Investment via more than 5 bank account by individual
		Change of bank mandate for more than 5 times by individual in life time
		Investment via more than10 bank account by Non individual
		Change of bank mandate for more than 10 times by Nonindividual life time
		Change of bank mandate more than 3 times in rolling 12 months
		Change of bank mandate more than 3 times in rolling 12 months
4	Disqualified Cos and director’s database	Investors appearing in MCA list issued for Disqualified Directors Companies
5	Additional	Gross Annual Income
		Change of address

Annexure B

CRITERIA/PARAMETERS FOR STR

Version Control

Version Control	Date	Details	Maker	Checker	Approver
V1		Drafting of Policy	Compliance Team		Board of Directors

Policy Approval Matrix

Stage	Description
Policy Title	**Anti-Money Laundering and Know Your Client Policy**
Policy Owner	**Swyom Advisors Alternative Investment Trust**
Prepared by	**Compliance Team**
Approved by	**Board of Directors**