

POLICY ON KNOW YOUR CUSTOMER
AND ANTI MONEY LAUNDERING
MEASURES

ADOPTED BY

Provitt Consultants

Registered office:

246, Wework BlueOne Square, Udyog Vihar Phase 4 Road, Gurugram, Haryana, 122016

Table of Contents

Preface

1. PROVITT CONSULTANTS Initiatives C Philosophy
2. What is Money Laundering?
3. Principal Officer – Designation and Duties
4. Designated Partner – Designation and Duties
5. Know your customer
6. Customer Acceptance policy
7. Customer Identification Procedures
8. Customer Due Diligence
9. Monitoring of Transactions
10. Risk Assessment
11. Risk Management
12. Combating Financing of Terrorism
13. Freezing of funds, financial assets or related services
14. List of Designated Individuals/Entities.
15. Maintenance of Records
16. Retention of Records
17. Reporting to Financial Intelligence Unit - India
18. Employee's Hiring /Employee's Training / Investor Education

Preface

This is the Anti-Money Laundering (AML) Policy (the Policy) of Provitt Consultants and has been prepared in accordance with the Prevention of Money Laundering Act, 2002 (PMLA Act). This Policy also takes into account the provisions of the PMLA Act and other Rules laid down by SEBI and FIU. In the provisions of the Prevention of Money Laundering Act, 2002 (PMLA) the policy of the company is to prohibit and actively prevent money laundering and any activity that facilitates money laundering (ML) or terrorist financing. Money laundering is generally understood as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds or assets so that they appear to have derived from legitimate origins or constitute legitimate assets.

As per PMLA, every banking company, financial institution (which includes chit fund company, a cooperative bank, a housing finance institution and a non-banking financial company) and intermediary (which includes a stock-broker, sub-broker, share transfer agent, banker to an issue, trustee to a trust deed, registrar to an issue, merchant banker, underwriter, portfolio manager, investment adviser and any other intermediary associated with securities market and registered under section 12 of the Securities and Exchange Board of India Act, 1992) shall have to maintain a record of all the transactions; the nature and value of which has been prescribed in the Rules notified under the PMLA. For the purpose of PMLA, transactions include:

1. All cash transactions of the value of more than Rs 10 Lacs or its equivalent in foreign currency.
2. All series of cash transactions integrally connected to each other which have been valued below Rs 10 lakhs or its equivalent in foreign currency, such series of transactions within one calendar month.
3. All transactions involving receipts by NPO of value more than Rs 10 lakhs or its equivalent in foreign currency.
4. All cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine or where any forgery of valuable security or a document has taken place facilitating the transactions.
5. All suspicious transactions whether or not made in cash and including, inter-alia, credits or debits into from any non-monetary account such as Demat account, security account maintained by the registered intermediary.
6. All cross-border wire transfers of value of more than Rs 5 lakh or its equivalent in foreign currency or any other mode of collection in whatever

name it is referred to.

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

“Suspicious transactions” means a transaction, including an attempted transaction, whether or not made in cash which to a person acting in good faith –

1. gives rise to a reasonable ground of suspicion that it may involve the proceeds of offence regardless of the value involved; or
2. appears to be made in circumstances of unusual or unjustified complexity or
3. appears to have no economic rationale or bonafide purpose.

Definitions and Terminologies

All the words and phrases used in this policy documents, which have not been specifically defined under this policy shall derive its meaning as prescribed under the provisions of PMLA Act and its Rules/Regulations and so on.

1. Provitt Consultants Initiatives G Philosophy

PROVITT CONSULTANTS had undertaken a comprehensive review of its AML framework and laid down an Anti-Money Laundering Policy in 2006. This policy shall be regularly reviewed to ensure effectiveness of policies and procedures on prevention of money laundering or whenever any new updation is necessitated as per Central Government/SEBI/Exchange/Depository circulars or guidelines. The review of the policy should be done by the official other than the person who has framed the policy. The basic purpose of this AML Policy is to establish a system for “Client Due Diligence Process” for PROVITT CONSULTANTS to participate in the international efforts against ML and to duly comply with the detailed guidelines as described under above said circular of SEBI and other legal provisions as well as to ensure that PROVITT CONSULTANTS is not used as a vehicle for ML. The AML framework of the PROVITT CONSULTANTS would meet the extant regulatory requirements.

It is important that PROVITT CONSULTANTS’s management views “money-laundering prevention” and “knowing your customer” as part of the risk management strategies and not simply as standalone requirements that are being imposed by legislation/regulators’.

Hence the objective of the policy is to –

1. To have a proper Customer Due Diligence (CDD) process before registering clients.

2. To monitor and report suspicious transactions.
3. To discourage and identify money laundering or terrorist financing activities.
4. To take adequate and appropriate measures to follow the spirit of the PMLA

2. What is Money Laundering?

Money laundering is moving illegally acquired cash through financial systems so that it appears to be legally acquired. It is a criminal practice of bringing proceeds of illegally acquired money back into the economy as if they are normal business funds. It is driven by criminal intentions and conceals the true source, ownership, or use of funds.

Section 3 of the PMLA Act defines money laundering in following words:

“Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime and projecting it as untainted property shall be guilty of offence of money-laundering and shall include:

a) A person shall be guilty of offence of money laundering if such person is found to have directly or indirectly attempted to indulge or knowingly assisted or knowingly is a party or is actually involved in one or more of the following processes or activities connected with proceeds of crime namely:

- concealment; or
- possession;
- acquisition
- use
- projecting as untainted property
- claiming as untainted property in any manner whatsoever;

b) The process or activity connected with proceeds of crime is a continuing activity and continues till such time a person is directly or indirectly enjoying the proceeds of crime by its concealment or possession or acquisition or use or projecting it as untainted property or claiming it as untainted property in any manner whatsoever”.

3. Principal Officer – Designation and Duties

The company has designated Ms. Shalini Gera, Partner as the Principal Officer for due compliance of its Anti-Money Laundering Policies. She will act as a Central reference point in facilitating onward reporting of suspicious transactions and for playing an active role in the identification and assessment of potentially suspicious transactions. The duties of the Principal Officer will include monitoring the company’s compliance with AML obligations and overseeing maintenance of AML records, communication and

training for employees. The Principal Officer will ensure filing of necessary reports with the Financial Intelligence Unit (FIU – IND). Principal Officer is authorized to issue additional circulars and advisories, to and seek information from the concerned officials for due compliance of this policy from time to time.

The company has provided the FIU with contact information of the Principal Officer and will promptly notify FIU of any change in this information.

4. Designated Partner – Designation and Duties

The company has designated Ms. Shalini Gera, Partner and Chief Executive Officer as the Designated Partner to ensure overall compliance with the obligations imposed under chapter IV of the Act and Rules.

5. Know Your Customer

KYC procedures enable the Company to know/understand the customers and their financial dealings in a better manner and manage the risk associated therein. One of the best methods of preventing and deterring money laundering is a sound knowledge of a customer's business and pattern of financial transactions. The adoption of procedures by which financial institutions "know their customer" is not only a principle of good business but is also an essential tool to avoid involvement in money laundering. The term KYC wherever used in this document shall also include processes of e-KYC. PROVITT CONSULTANTS shall determine and document the true identity of the customers who establish relationships, open accounts or conduct significant business transactions and obtain basic background information on customers.

In this regard, such clients shall be marked as suspicious whether an individual or entity whose identity cannot be determined or who refuses to provide information, or who have provided information that contains significant inconsistencies which cannot be resolved after due investigation. Further, the Company upon commencement of account-based relationship shall file the electronic copy of client's KYC to the Central KYC Records Register. The Company shall ensure that it shall not use the KYC records of customers for the purposes other than verifying identity or address of the client and shall not transfer KYC records or any information contained therein to any third party unless authorized by the customer or Regulator or Director.

6. Customer Acceptance Criteria

No account shall be opened in anonymous or fictitious / benami name(s). PAN shall be

mandatory for each account. In addition to Pan, client is also required to submit one certified copy of an 'officially valid document' containing details of his identity and address, one recent photograph and such other documents including in respect of nature or business and financial status of the client. The Company shall accept a customer on the basis of facilitation of any of the following identity proof i.e. passport, driving license, voter id card or PAN card. Further, following additional documents/information may be desired from following class of customers:

| Categories | Documents/Information Required |
|--------------------------------------|---|
| A Company | <ol style="list-style-type: none"> 1) Certificate of Incorporation 2) MOA & AOA 3) PAN Card 4) Resolution from the Board & POA granted to its manager, officer, employees. 5) Such documents as may be desired |
| A Partnership Firm | <ol style="list-style-type: none"> 1) Registration Certificate 2) Partnership Deed 3) PAN Card 4) Such documents as may be desired |
| A Trust | <ol style="list-style-type: none"> 1) Registration certificate 2) Trust Deed 3) PAN Card/Form 60 of the Trust 4) Such documents as may be desired |
| An Unincorporated Association | <ol style="list-style-type: none"> 1) Resolution of the Managing body of such association 2) PAN Card/Form 60 3) POA 4) Such document required to establish the existence of the association 5) Such documents as may be desired |

The parameters of risk perception in terms of the nature of business activity, location of customer and his clients, mode of payments, volume of turnover, social and financial status etc shall be captured at the account opening stage to enable categorization of customers into low, medium and high risk.

For the purpose of risk categorization, individuals/entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile, shall be categorized as low risk. Illustrative examples of low-risk customers can be salaried employees whose salary structures are well defined; or people belonging to Government Departments and Government owned companies or

Regulators and statutory bodies or those belonging to lower economic strata etc.

Customers that are likely to pose a higher-than-average risk to PROVITT CONSULTANTS shall be categorized as medium or high risk depending on customer's background, nature and location of activity, country of origin, sources of funds and his client profile etc. The Company shall prepare profile for each new customer based on the risk categorization and shall contain information relating to customer's identity, social/financial status, nature of business activity, information about the clients; business and their location etc. PROVITT CONSULTANTS shall apply Customer Due Diligence measures based on the risk assessment, thereby requiring intensive 'due diligence' for higher risk customers, especially those for whom the sources of funds are not clear. The Company ensures that it has suitable systems in place to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanction lists circulated by the Reserve Bank.

7. Customer Identification Procedures

Customer identification procedure means verifying the identity of the customer by using reliable, independent source documents, data or information. PROVITT CONSULTANTS needs to obtain sufficient information necessary to establish, to its satisfaction, the identity of each new customer, whether regular or occasional, and the purpose of the intended nature of relationship. PROVITT CONSULTANTS must also be able to satisfy the regulators that due diligence was observed based on the risk profile of the customer in compliance with the extant guidelines in place.

- I. The Company shall duly comply with the KYC /client identification procedures that may be specified and strengthened by SEBI from time to time.
- II. The concerned officials should take extra caution in case of existing or potential Politically Exposed Persons (PEP)/PEP Family or close relatives of PEPs. They may seek additional information and also take the help of publicly available information.

No business relationships can be established with PEP without prior approval of the senior management. Where a customer has been accepted and the customer or beneficial owner is subsequently found to be, or subsequently becomes a PEP, the approval from the above said officials is required to continue the business relationship.

- III. The concerned officials of the Company should track the financial soundness of the clients and shall take reasonable measures to verify source of funds of clients identified as PEP.
- IV. The information should be adequate enough to satisfy competent authorities

(regulatory / enforcement authorities) in future that due diligence was observed by the Company in compliance with the Guidelines.

- V. The principal Officer shall ensure that the Client Identification Programme has been formulated and implemented as per the requirements of the Notification of RBI No. 16/42 dated July 01, 2015 (as amended from time to time) and the PML Rules 2009.
- VI. It may be noted that while risk-based approach may be adopted at the time of establishing business relationship with a client, no exemption from obtaining the minimum information/documents from clients as provided in the PMLA Rules is available to any class of investors with regard to the verification of the records of the identity of clients.
- VII. There shall be no minimum investment threshold/ category-wise exemption available for carrying out CDD measures by the Company.
- VIII. On failure by prospective client to provide satisfactory evidence of identity including address, financial status and the purpose of intended nature of relationship, new account shall not be opened and the matter shall be reported to the higher authority. This shall also apply where it is not possible to ascertain the identity of the client, or the information provided to the Company is suspected to be non-genuine, or there is perceived non-co-operation of the client in providing full and complete information.
- IX. In the event, particulars of any of customer/s match the particulars of designated individuals/entities, PROVITT CONSULTANTS as a intermediaries shall immediately, not later than 24 hours from the time of finding out such customer, inform full particulars of the funds, financial assets or economic resources or related services held in the form of securities, held by such customer on their books to the Joint Secretary (IS.I), Ministry of Home Affairs, at Fax No.011-23092569 and also convey over telephone on 011-23092736. The particulars apart from being sent by post should necessarily be conveyed through e-mail at jsis@nic.in.

PROVITT CONSULTANTS shall send the particulars of the communication mentioned above through post/fax and through e-mail (sebi_uapa@sebi.gov.in) to the UAPA nodal officer of SEBI, Officer on Special Duty, Integrated Surveillance Department, Securities and Exchange Board of India, SEBI Bhavan, Plot No. C4-A, "G" Block, Bandra Kurla Complex, Bandra (E), Mumbai 400 051 as well as the UAPA nodal officer of the state/UT where the account is held, as the case may be, and to FIU-IND.

Without diluting the above requirements, the personnel opening a new account may obtain other independent information to satisfactorily establish the identity of each new client and the purpose of the intended nature of the relationship.

8. Customer Due Diligence

The Customer Due Diligence can be of two type's i.e. due diligence at the time of acceptance of client and that at the time of periodic updation.

A. Client Acceptance

The Company shall exercise Customer Due Diligence before accepting any client/customer. The Company shall ensure following:

- i) Obtain one certified copy of officially valid document containing details of identity and address one recent photograph and such other documents pertaining to the nature of business and financial status of the customer as may be required.
- ii) Verification through the e-KYC process available on Unique Identification Authority of India (UIDAI) with the consent of the client.

B. Periodic Updation

The Company may carry out periodical updation of KYC information of every customer at such interval and in such manner as prescribed by various circulars and Regulations issued by various authorities.

The periodic updation may include all measures for confirming the identity and address and other particulars of the customer based on the risk profile of the customer and after taking into account whether and when client due diligence measures were last taken. In case of no updation, a self-certification by the customer to that effect shall be sufficient. In periodic updation, the Company shall ensure updated records are submitted to Central KYC Records Register.

The Company will exercise Customer Due Diligence (CDD) in client acceptance and subsequent continuing relationship with the clients. It will include:

- (a) 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.
- (b) Verify the client's identity using reliable, independent source documents, data or information;
 - (c) 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;
 - (d) 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 (c);
 - (e) Understand the ownership and control structure of the client;
 - (f) 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 Company's knowledge of the client, its business and risk profile, taking into account, where necessary, the client's source of funds; and
 - (g) Periodically updating all documents, data or information of all clients and beneficial owners collected under the CDD process.
- (h) PROVITT CONSULTANTS shall verify the client's identity using reliable, independent source documents, data or information. Where the client purports to act on behalf of juridical person or individual or trust.
- (i) Specifically verify identity of the customer where the transaction exceeds Rs. 50,000 whether conducted as a single transaction or several transactions that appear to be connected or in case of any international money transfer operations.
- (j) If the client is a non-profit organization, the PROVITT CONSULTANTS will register the client details on the DARPAN portal of NITI Aayog and maintain the records for a period of five years after the relationship with the clients.
- (k) Where client's transactions relate to money laundering or terrorist financing, the PROVITT CONSULTANTS shall not pursue the CDD process, and shall instead file a STR with FIUIND.”

Beneficial ownership:

Beneficial ownership implies the ultimate individual beneficial owner of the entity. In case of non-individual shareholders/ owners/ partners/Beneficiaries as the case may, the ultimate individual beneficial owner should be identified in all cases except for listed companies.

Determination of beneficial ownership (SEBI Circular CIR/MIRSD/2/2013 Dated 24.01.2013 & SEBI/ HO/MIRSD/MIRSDSECFATF/P/CIR/2023/091 dated June

16, 2023) Where the client is a person other than an individual or trust, viz., company, partnership or unincorporated association/body of individuals, the company shall identify the beneficial owners of the client and take reasonable measures to verify the identity of such persons, through the following information: The identity of the natural person, who, whether acting alone or together or through one or more judicial person, exercise control through ownership or who ultimately has controlling ownership interest.

Controlling ownership interest means:

- I. More than 10% of shares or capital or profits of the juridical person, where it is a company.
- II. More than 15 % of the capital or profits of the juridical person, where it is a partnership.
- III. More than 15 % of the property or capital or profits of the juridical person, where it is an unincorporated person or body of individuals.

Where the client is a trust, the company shall identify the beneficial owner of the client through the identity of the settler of the trust, the trustee, the protector or the beneficiaries with 10% or more interest in the trust or any natural person exercising ultimate effective control over the trust.

While implementing CDD procedures the Company, in accepting a new client, shall:

- i. Adopt a Risk Based Approach
- ii. Verify proofs of identity, address, and financial status of the client and persons acting on its behalf, ownership and control structure by scrupulously following the KYC norms of the relevant exchange / Depositories / RBI. Adequate information to satisfactorily establish the identity of each new client and the purpose of the intended nature of the relationship should be obtained. KYC norms shall be followed while establishing the client relationship and may further be followed while carrying out transactions for the client or when there is doubt regarding the veracity or the adequacy of previously obtained client identification data. Account should be opened only after the completion of all the required documents and after due verification with originals. In person verification shall be carried in a manner provided by SEBI/Exchange/Depositories.
- iii. The Company may rely on a third party for the purpose of (a) identification and verification of the identity of a client and (b) determination of whether the client is acting on behalf of a beneficial owner, identification of the beneficial owner and verification of the identity of the beneficial owner. Such third party shall be regulated, supervised or monitored for, and have measures in place for compliance with CDD and record-keeping requirements in line with the obligations under the PML Act. Such reliance shall be subject to the conditions that are specified in Rule 9 (2) of the PML Rules and shall be in accordance with the regulations and circulars/ guidelines issued by SEBI from

time to time.

- iv. Not open any account in a fictitious / benami name or on an anonymous basis. Ensure that the identity of the proposed client does not match with any person having known criminal background and his is not banned in any other manner, whether in terms of UN sanction resolutions available or on website at <https://www.un.org/securitycouncil/content/un-sc-consolidated-list> or orders of any other enforcement agency.

While accepting and executing a client relationship the Company will adopt a Risk Based Approach as under:

| Low Risk | Medium Risk | High Risk |
|--|--|---|
| Individual clients, with clean image, not PEP, with investment upto Rs. 50 Lakhs, whose identity and sources of wealth can be easily identified. | Clients over investment of Rs. 50 Lakhs where identity and sources of wealth are not supported by public documents like Income Returns, Registered conveyance Deeds etc. | HNI Clients (having Net worth over 500 Lakhs) with no known sources of Income |
| Listed Companies | Clients with sudden spurt in volumes or investment without apparent reasons | Clients subsequently becoming suspicious of ML/FT activities |
| Govt. owned companies, regulated bodies like banks and PMLA regulated intermediaries | Persons in business/ industry or trading activity where scope or history of unlawful trading/business activity dealings is more. | Single Share Companies Or Companies with bearer shares |
| Day traders and arbitrageurs | Where the client profile of the person/s opening the account, according to the perception of the | All Clients of Special Category |

| | | |
|---|---|--|
| | branch is uncertain and/or doubtful/dubious. | |
| Clients having regular relationship or low volumes (e.g. upto 25 lakhs) | Clients having occasional relationship but with moderate volumes (upto 100 lakhs) | Clients having occasional relationship with large volumes (over 100 lakhs) |

| | | |
|--|--|---|
| | | Politically Exposed Persons Systems should be there to find out whether a person is PEP- Take reasonable measures to establish source of wealth and source of funds on ongoing basis. |
| | | Client accounts opened by professional intermediaries |

The clients shall be shifted from one category to another on real-time basis, if at any time they satisfy the above-mentioned criteria. The CDD process shall necessarily be revisited when there are suspicions of money laundering or financing of terrorism (ML/FT).

Clients of Special Category: Special care shall be taken while opening accounts of Clients of Special Category. Such clients include the following

- a. Non-resident clients
- b. HNI clients (having Net worth over 500 Lakhs)
- c. Trust, Charities, NGOs and organizations receiving donations
- d. Companies having close family shareholdings or beneficial ownership
- e. Politically exposed persons (PEP) of foreign origin
- f. Current / Former Head of State, Current or Former Senior High profile politicians and connected persons (immediate family, Close advisors and companies in which such individuals have interest or significant influence)
- g. Companies offering foreign exchange offerings
- h. Clients in high risk countries (where existence / effectiveness of money laundering controls is suspect, where there is unusual banking secrecy, Countries active in narcotics production, Countries where corruption (as per Transparency International Corruption Perception Index) is highly prevalent, Countries against which government sanctions are applied, Countries reputed to be any of the following – Havens / sponsors of international terrorism, offshore financial centers, tax havens, countries where fraud is highly prevalent.
- i. Non face to face clients
- j. Clients with dubious reputation as per public information available etc.

The above-mentioned list is only illustrative and the company may exercise independent

judgment to ascertain whether new clients should be classified as CSC or not.

10. Monitoring of Transactions

Ongoing monitoring is an essential element of effective KYC procedures. PROVITT CONSULTANTS can effectively control and reduce their risk only if they have an understanding of the normal and reasonable activity of the customer so that they have the means of identifying transactions that fall outside the regular pattern of activity.

PROVITT CONSULTANTS shall have in place a comprehensive transaction monitoring process from a KYC/AML perspective. PROVITT CONSULTANTS shall put in place strong transaction alerts which will provide proactive signals on suspicious transactions and possible money laundering. The Company has created awareness at each level of department and principal officer along with other officials of the Company shall endeavor to update the list based on current understanding of the market scenario and trading patterns followed by clients. In addition to the alerts from internal sources, the Surveillance & compliance team shall also monitor the alerts provided by the various Exchanges & Depositories.

On the basis of criticality of the breach, observation of account behavior, repetitive breaches, the Principal Officer shall send a query to the concerned business. Responses would be expected within 7 working days. If the alerts still persist or the Principal Officer is not satisfied with the responses, then he shall send the query to the Compliance Head for resolution.

In case of any account wherein alerts are observed on a regular basis, the risk categorization would be increased based on the consensus of the AML monitoring team and the compliance officer. Such a review would be done at least once every month. Special attention is required for all complex, unusually large transactions / patterns which appear to have no economic purpose. The background including all documents, office records and clarifications pertaining to such transactions and their purpose will be examined carefully and findings will be recorded. Such findings, records and related documents would be made available to auditors and also to SEBI/Stock Exchanges/FIU-IND/Depositories /other relevant authorities, during audit, inspection or as and when required. These records to be preserved for ten years as required under PMLA 2002.

It would be ensured that record of transaction is preserved and maintained in terms of section 12 of the PMLA 2002, Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 or any other notification issued in due course and that transaction of suspicious nature or any other transaction notified under section 12 of the act is reported to the appropriate law authority.

11. Risk Assessment:

- i. Company shall carry out risk assessment of the clients by undertaking the client Due Diligence process to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk with respect to clients, countries or geographical areas, nature and volume of transactions, payment methods used by clients, etc. 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 (these can be accessed at http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml and <http://www.un.org/sc/committees/1988/list.shtml>).
- ii. The Company will identify and evaluate ML/TF risks that may arise in connection with the development of new delivery mechanisms and the use of new or developing technologies for both new and existing clients.
- iii. 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. The assessment shall be documented, updated regularly and made available to competent authorities and self regulating bodies, as and when required.

10. Risk Management

PROVITT CONSULTANTS have a Risk Based Approach (RBA) for mitigation and management of the identified risk and have policies approved by their senior management, controls and procedures in this regard. Further, PROVITT CONSULTANTS shall monitor the implementation of the controls and enhance them if necessary.

The overall responsibility/implementation and adherence of this shall lie with the Compliance, RMS & Surveillance Department of the Company.

The Concurrent / Internal Auditors shall specifically check and verify the application of KYC/AML procedures and comment on the lapses observed in this regard. The reports and compliance in this regard shall also put up before the ODM Committee of the Board.

11. Combating Financing of Terrorism (CFT)

PROVITT CONSULTANTS shall have a heightened awareness in the system to check for transactions which give rise to a reasonable ground of suspicion that these may involve financing of the activities relating to terrorism.

12. Freezing of funds, financial assets or related services

On the directions of the Central Government/FIU/SEBI or any regulatory authority, PROVITT CONSULTANTS shall freeze, seize or attach funds and other financial assets or economic resources held by, on behalf of, or at the direction of the individuals or entities listed in the Schedule to the Order, or any other person engaged in or suspected to be engaged in terrorism.

PROVITT CONSULTANTS shall also evaluate whether there is any suspicious transaction and accordingly consult the regulatory authority, in determining whether to freeze or close the account and also follow the provisions of Section 51A of UAPA, Government of India has outlined a procedure through an order dated February 02, 2021 (Annexure 1) for strict compliance. These guidelines have been further amended vide a Gazette Notification dated June 08, 2021 (Annexure 2) and a corrigendum dated March 15, 2023 has also been issued in this regard (Annexure-3). The list of Nodal Officers for UAPA is available on the website of MHA.

List of Designated Individuals/Entities.

PROVITT CONSULTANTS monitor a list of individuals/entities who have been designated as 'terrorists'. Which the Home Ministry announces from time to time as per Section 35(1) of UAPA 1967. Further, we also verify and monitor client details along with 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)/ The "ISIL (Da'esh)

&Al-Qaida Sanctions List", can be accessed at following websites/links/press release

[https://press.un.org/en/content/press-release.](https://press.un.org/en/content/press-release)
[www.un.org/securitycouncil/sanctions/1718/press-releases.](http://www.un.org/securitycouncil/sanctions/1718/press-releases)

We ensure that accounts are not opened in the name of anyone whose name appears in above list. We will continuously scan all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the above list.

13. Maintenance of Records

In addition, the Principal Officer will ensure the maintenance of the following records:

- (i) all cash transactions of the value of more than rupees ten lakh or its equivalent in foreign currency;
- (ii) all series of cash transactions integrally connected to each other which have been valued below rupees ten lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the aggregate value of such transactions exceeds rupees ten lakh;
- (iii) all cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security has taken place;
- (iv) all suspicious transactions whether or not made in cash

Suspicious transaction means a transaction whether or not made in cash and including, inter-alia, credits or debits into or from any non-monetary account such as demat account, security account etc. which, to a person acting in good faith –

- gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime; or
- appears to be made in circumstances of unusual or unjustified complexity; or
- appears to have no economic rationale or bona fide purpose;

A list of circumstances which may be in the nature of suspicious transactions is given below. 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:

- a) Clients whose identity verification seems difficult or clients that appear not to cooperate
- b) Asset management services for clients where the source of the funds is not clear or not in keeping with client's apparent standing /business activity;
- c) Clients based in high-risk jurisdictions;

- d) Substantial increases in business without apparent cause;
- e) Clients transferring large sums of money to or from overseas locations with instructions for payment in cash;
- f) Attempted transfer of investment proceeds to apparently unrelated third parties;
- g) Unusual transactions by CSCs and businesses undertaken by offshore banks/financial services, businesses reported to be in the nature of export-import of small items.

The records shall contain the following information:

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

The Company shall also endeavour to 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 to the investigating agencies for prosecution of criminal behavior. For this purpose, we shall retain the documents as to

- (a) the beneficial owner of the account;
- (b) the volume of the funds flowing through the account; and
- (c) for selected transactions:

- the origin of the funds;
- the form in which the funds were offered or withdrawn, e.g. cash, cheques etc.;
- the identity of the person undertaking the transaction;
- the destination of the funds;
- the form of instruction and authority.

Principal Officer should ensure that all customer and transaction records and information are available on a timely basis to the competent investigating authorities. Where appropriate, he may consider retaining certain records, e.g. customer identification, account files, and business correspondence, for periods which may exceed that required

under the SEBI Act, Rules and Regulations framed there-under PMLA 2002, other relevant legislations, Rules and Regulations or Exchange / Depositories bye-laws or circulars.

14. Retention of Records

(a) The Company shall maintain necessary records on transactions, both domestic and international, at least for the minimum period prescribed under the SEBI Act, 1992, Rules and Regulations made there-under, PMLA as well as other relevant legislation, Rules, Regulations, Exchange / Depositories Bye-laws and Circulars issued from time to time.

(b) Records on client identification (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence shall also be kept for the same period.

(c) In situations where the records relate to on-going investigations or transactions, whether attempted or executed, which are reported to the Director, FIU-IND, as required under Rules 7 C 8 for the PML Rules, shall maintain at least for a period of eight years from the date of the transaction or shall be retained until it is confirmed that the case has been closed.

(d) Further, in terms of Regulations 54 and 66 of the SEBI (Depositories and Participants) Regulations, 2018 (herein referred to as DCP Regulations, 2018) notified on October 03, 2018, PROVITT CONSULTANTS shall preserve the records and documents for a minimum period of eight years.

15. Reporting to Financial Intelligence Unit-India

In terms of the PMLA rules, principal Officer is required to report information relating to cash and suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND) at the following address:

Director, FIU-IND,
Financial Intelligence Unit-India,
6th Floor, Tower-2, Jeevan Bharati Building Connaught Place,
New Delhi-110001, INDIA
Telephone: 91-11-23314429, 23314459
91-11-23319793(Helpdesk) Email: helpdesk@fiuindia.gov.in (For
FINnet and general queries)
ctrcell@fiuindia.gov.in
(For Reporting Entity / Principal Officer Registration related queries)
complaints@fiuindia.gov.in
Website: <http://fiuindia.gov.in>

For Cash Transaction Reporting (CTR)

Dealings in Cash, if any, requiring reporting to the FIU IND will be done in the CTR format in the matter and at intervals as prescribed by the FIU IND. The Cash Transaction Report (CTR) (wherever applicable) for each month shall be submitted to FIU-IND by 15th of the succeeding month.

For Suspicious Transactions Reporting (STR)

We will make a note of Suspicious Transaction that have not been explained to the satisfaction of the Principal Officer and thereafter report the same to the FIU IND within the required deadlines.

Where a client aborts/abandons a suspicious transaction on being asked some information by the company officials, the matter should be reported to FIU in the STR irrespective of the amount.

We will not base our decision on whether to file a STR solely on whether the transaction falls above a set threshold. We will file a STR and notify law enforcement of all transactions that raise an identifiable suspicion of criminal or terrorist corrupt activities.

We will not notify any person involved in the transaction or any third person, that the transaction has been reported, except as permitted by the PML Act and Rules thereof.

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.

The Non Profit Organization Transaction Reports (NTRs) for each shall be submitted to FIU-IND by 15th of the succeeding month.

The Principal Officer will be responsible for timely submission of CTR, STR and NTR to FIU-IND and will be able to report to senior management or the Board of Directors at the next reporting level.

Utmost confidentiality should be maintained in filing of CTR, STR & NTR to FIU- IND. The reports may be transmitted online or by speed/registered post/fax at the notified address.

No nil reporting needs to be made to FIU-IND in case there are no cash/suspicious transactions to be reported. We shall ensure not to put any restrictions on operations in

the accounts where an STR has been made. PROVITT CONSULTANTS and its directors, officers and employees (permanent and temporary) will be prohibited from disclosing (“tipping off”) the fact that a STR or related information is being reported or provided to the FIU-IND. Thus, it should be ensured that there is no tipping off to the client at any level. Our company will create and maintain STRs, NTRs and CTRs and relevant documentation on customer identity and verification. We will maintain STRs, NTRs and CTRs their accompanying documentation for at least ten years and will also use the prescribed formats and related hardware and technical requirements for generating reports.

16. Employee’s Hiring /Employee’s Training / Investor Education:

We have adopted adequate screening procedures including background check to ensure high standards while hiring employees. Having regard to the risk of money laundering and terrorist financing and size of the business, the Company will identify the key positions and will ensure that the employees taking up such key positions are suitable and competent to perform their duties.

We have developed an ongoing employee training under the leadership of the Principal Officer so that the members of the staff are adequately trained in AML and CFT procedures. Training requirements shall have specific focuses for frontline staff, back-office staff, compliance staff, risk management staff and staff dealing with new clients. They shall be made to fully understand the rationale behind this policy, obligations and requirements, implement them consistently and are sensitive to the risks of their systems being misused by unscrupulous elements.

We have developed in-house training in the company. Means of the training includes educational pamphlets, videos, intranet systems, in-person lectures, and explanatory memos.

Implementation of AML/CFT measures requires us to demand certain information from investors which may be of personal nature or which have hitherto never been called for, such as documents evidencing source of funds/income tax returns/bank records etc., which can sometimes lead to raising of questions by the customer with regard to the motive and purpose of collecting such information. Therefore, we will sensitize our customers about these requirements as the ones emanating from AML and CFT framework. We will prepare specific literature/ pamphlets etc/ hold conference so as to educate the customers of the objectives of the AML/CFT program.

Monitoring Employee Conduct and Accounts:

We will subject employee accounts to the same AML procedures as customer accounts, under the supervision of the Principal Officer. The Principal Officer’s accounts will be reviewed by the Board of Directors.

Confidential Reporting of AML Non-Compliance:

Employees will report any violations of the company's AML compliance program to the Principal Officer, unless the violations implicate the Principal Officer, in which case the employee shall report to the Board. Such reports will be confidential, and the employee will suffer no victimization for making them.

Communication of this Policy:

Principal Officer shall ensure that this policy is communicated to all management and relevant staff including partner, Head of the department (s), branches and group companies.

Review and Modification:

In case of any subsequent changes in the provisions of the PMLA Act and its Rules, which makes any of the provisions in the policy inconsistent with the provision of law, the provisions of the Act or Rules would prevail over the policy and the provisions in the policy would be modified in due course to make it consistent with law.

Approval of ODM Committee of the Board of Directors

We have approved this revised AML program as reasonably designed to achieve and monitor our company's ongoing compliance with the requirements of the PMLA and the implementing regulations under it. This Committee shall supervise the implementation of the AML Policy framework.

This Policy last reviewed and placed before ODM Committee on 25th February, 2025.