KHOSLA TRADEWISE
PVT LTD

KHOSLA TRADEWISE PRIVATE LIMITED

POLICIES AND PROCEDURE FOR PREVENTION OF MONEY LAUNDERING

(As Per the PMLA Act (Amended), 2002)

KHOSLA TRADEWISE PVT LTD

Table of Contents

KHOSLA TRADEWISE PRIVATE LIMITED

KHOSLA TRADEWISE PVT LTD

This document outlines the Anti-Money Laundering (AML) Policy of KHOSLA TRADEWISE, developed in compliance with the Prevention of Money Laundering Act, 2002 (PMLA). The Policy incorporates the provisions of the PMLA, and relevant guidelines established by SEBI and the Financial Intelligence Unit (FIU). The previous policy created necessary amendments have been made to the existing AML Policy of the Company.

In line with these circulars and the PMLA, the Company is committed to prohibiting and actively preventing money laundering and any related activities, including terrorist financing. Money laundering is typically defined as actions aimed at concealing or disguising the true origins of proceeds or assets derived from criminal activities, so they appear legitimate.

According to the PMLA, all banking companies, financial institutions (including chit fund companies, cooperative banks, housing finance institutions, and non-banking financial companies), and intermediaries (such as stockbrokers, sub-brokers, share transfer agents, trustees, registrars, merchant bankers, underwriters, portfolio managers, and investment advisers registered under Section 12 of the Securities and Exchange Board of India Act, 1992) are required to maintain records of all transactions as specified in the Rules notified under the PMLA.

For the purposes of the PMLA, transactions include:

1. All cash transactions exceeding ₹10 lakhs or its equivalent in foreign currency.
2. Series of connected cash transactions valued below ₹10 lakhs or its equivalent in foreign currency within a single calendar month.
3. All transactions involving receipts by non-profit organizations (NPOs) valued over ₹10 lakhs or its equivalent in foreign currency.
4. All cash transactions where counterfeit currency or forged documents have been used to facilitate the transaction.
5. All suspicious transactions, regardless of whether they are conducted in cash, including credits or debits to non-monetary accounts such as Demat accounts and security accounts maintained by registered intermediaries.
6. All cross-border wire transfers exceeding ₹5 lakh or its equivalent in foreign currency, as well as any other forms of collection, regardless of their designation, must be monitored.

For the reporting of suspicious transactions, it is essential to consider both "transactions integrally connected" and "transactions remotely connected or related."

"Suspicious transactions" are defined as any transaction, including attempted transactions, whether conducted in cash or not, that raises reasonable grounds for suspicion to a person acting in good faith. This includes transactions that:

1. Suggest involvement of proceeds from illegal activities, regardless of their value.
2. Occur under unusual or unjustified complexities; or
3. Lack any economic rationale or bona fide purpose.

KHOSLA TRADEWISE PRIVATE LIMITED

Definitions and Terminology

All terms and phrases used in this policy document that are not explicitly defined herein will be interpreted according to their meanings as prescribed in the PMLA Act and its associated Rules and Regulations.

1. Overview of KHOSLA TRADEWISE Initiatives and Philosophy

This policy will be reviewed regularly to ensure the effectiveness of measures aimed at preventing money laundering, as well as to incorporate any updates necessitated by directives from the Central Government, SEBI, Exchanges, or Depositories. Reviews should be performed by an official other than the individual who originally formulated the policy.

The primary objective of this AML Policy is to establish a "Client Due Diligence Process" that enables **KHOSLA TRADEWISE** to engage in global efforts against money laundering and to ensure compliance with the detailed guidelines outlined in the aforementioned SEBI circulars and other legal requirements. This is essential to prevent **KHOSLA TRADEWISE** from being used as a vehicle for money laundering.

It is crucial for the management of **KHOSLA TRADEWISE** to regard "money laundering prevention" and "knowing your customer" as integral components of risk management strategies, rather than merely as obligations imposed by legislation or regulators. Consequently, the objectives of this policy include:

1. Implementing a robust Customer Due Diligence (CDD) process prior to client registration.
2. To monitor and maintain records of all cash transactions exceeding ₹10 lakhs.
3. To keep records of all series of integrally connected cash transactions within a single calendar month.
4. To monitor and report any suspicious transactions.
5. To discourage and identify activities related to money laundering or terrorist financing.
6. To take adequate measures to uphold the spirit of the PMLA.

2. What is Money Laundering?

Money laundering involves the illegal movement of cash obtained through criminal activities through financial systems to make it appear legitimate. It is a criminal practice that integrates proceeds from illegal activities back into the economy as if they are ordinary business funds. Driven by criminal intent, it conceals the true source, ownership, or intended use of the funds.

According to Section 3 of the PMLA Act, money laundering is defined as follows: "Whosoever directly or indirectly attempts to indulge or knowingly assists or is otherwise involved in any process or activity connected with the proceeds of crime, projecting it as untainted property, shall be guilty of the offence of money laundering." This includes:

a) A person is guilty of money laundering if they directly or indirectly attempt to engage in, knowingly assist, or are involved in any of the following activities related to proceeds of crime:
- Concealment
- Possession

KHOSLA TRADEWISE PRIVATE LIMITED

- Acquisition
- Use
- Projecting as untainted property
- Claiming as untainted property in any manner

b) The processes or activities connected with the proceeds of crime are ongoing and continue as long as a person enjoys the benefits from these proceeds through concealment, possession, acquisition, use, projection as untainted property, or claiming it in any form.

3. Principal Officer – Designation and Duties

The company has appointed **Subhash Sakharam Pattebahadur**, as the Principal Officer responsible for ensuring compliance with its Anti-Money Laundering Policies. He will serve as the central point of reference for reporting suspicious transactions and will actively participate in identifying and assessing potentially suspicious activities.

The Principal Officer's duties include:

- Monitoring the company's adherence to AML obligations.
- Overseeing the maintenance of AML records.
- Facilitating communication and training for employees.
- Ensuring the timely filing of necessary reports with the Financial Intelligence Unit (FIU – IND).

The Principal Officer is authorized to issue additional circulars and advisories and to seek information from relevant officials to ensure compliance with this policy. The company has provided the FIU with the contact details of the Principal Officer and will promptly inform the FIU of any changes to this information.

4. Designated Director – Designation and Duties

The company has appointed Designated Director responsible for ensuring overall compliance with the obligations outlined in Chapter IV of the Act and its associated Rules.

5. Know Your Customer (KYC)

KYC procedures enable the company to better understand its customers and their financial activities, helping to manage associated risks. One of the most effective ways to prevent and deter money laundering is to have a thorough understanding of a customer's business and financial transaction patterns. Implementing KYC processes is not only a good business practice but also a crucial measure to avoid involvement in money laundering.

In this document, the term KYC also encompasses e-KYC processes. **KHOSLA TRADEWISE** is committed to verifying and documenting the true identities of customers who establish relationships, open accounts, or conduct significant business transactions. This includes gathering essential background information.

Clients may be classified as suspicious if their identity cannot be verified, if they refuse to provide information, or if they present information with significant inconsistencies that remain unresolved after thorough investigation. Upon establishing an account-based relationship, the company will file an electronic copy of the client's KYC with the Central KYC Records Registry.

The company will ensure that KYC records are used solely for verifying the identity or address of clients and will not transfer KYC records or any contained information to third parties unless authorized by the customer, the regulator, or a director.

6. Customer Acceptance Criteria

Accounts cannot be opened under anonymous, fictitious, or benami names. A Permanent Account Number (PAN) is mandatory for each account, and each client is allowed only one account. If a client fails to provide a PAN, they must submit a certified copy of an officially valid document that includes their identity and address, along with a recent photograph and any additional documentation regarding the nature of their business and financial status.

The company will accept customers based on the following forms of identity proof: passport, driving license, voter ID card, or PAN card. Additional documents or information may be required from certain categories of customers.

For foreign nationals whose documents do not include an address, documents issued by government authorities in their home countries or letters from their embassy or mission in India will be accepted as proof of address.

The risk perception parameters—such as the nature of the business activity, customer location, client interactions, payment methods, turnover volume, and social and financial status—will be assessed at the account opening stage to categorize customers as low, medium, or high risk.

Categories and Required Documents/Information:

A Company:

1. Certificate of Incorporation
2. Memorandum of Association (MOA) & Articles of Association (AOA)
3. PAN Card
4. Board Resolution & Power of Attorney (POA) granted to its manager, officer, or employees
5. Any additional documents as needed

A Partnership Firm:

1. Registration Certificate
2. Partnership Deed
3. PAN Card
4. Any additional documents as needed

A Trust:

1. Registration Certificate
2. Trust Deed
3. PAN Card/Form 60 of the Trust
4. Any additional documents as needed

An Unincorporated Association:

1. Resolution from the managing body of the association
2. PAN Card/Form 60
3. Power of Attorney (POA)
4. Any document required to establish the existence of the association
5. Any additional documents as needed

Risk Categorization

For risk categorization, individuals or entities whose identities and sources of wealth can be easily verified, and whose account transactions generally align with their known profiles, will be classified as low risk. Examples of low-risk customers include salaried employees with defined salary structures, individuals working in government departments or government-owned companies, regulatory bodies, and those from lower economic strata.

Customers posing a higher-than-average risk to **KHOSLA TRADEWISE** will be categorized as medium or high risk based on factors such as their background, nature and location of activities, country of origin, sources of funds, and client profiles. The company will create a profile for each new customer according to their risk category, which will include information about the customer's identity, social and financial status, nature of business, and client details.

KHOSLA TRADEWISE will implement Customer Due Diligence measures according to the risk assessment, requiring more extensive due diligence for high-risk customers, particularly when their sources of funds are unclear. The company will ensure it has appropriate systems to verify that the identity of customers does not match any individuals or entities listed in the sanction lists provided by the Reserve Bank.

7. Customer Identification Procedures

Customer identification procedures involve verifying a customer's identity using reliable, independent source documents, data, or information. **KHOSLA TRADEWISE** must gather sufficient information to establish, to its satisfaction, the identity of each new customer—whether regular or occasional—and understand the intended nature of the relationship. The company must also be able to demonstrate to regulators that due diligence has been conducted based on the customer's risk profile in compliance with existing guidelines.

I. The company will comply with KYC and client identification procedures as specified and updated by SEBI.

II. Concerned officials must exercise extra caution when dealing with existing or potential Politically Exposed Persons (PEPs), their families, or close associates. They should seek additional information and utilize publicly available resources.

III. No business relationships may be established with PEPs without prior approval from senior management. If a customer or beneficial owner is later identified as a PEP, continued business relationships must be approved by the designated officials.

IV. Officials should monitor the financial soundness of clients and take reasonable measures to verify the sources of funds for clients identified as PEPs.

V. The information gathered must be sufficient to satisfy competent regulatory and enforcement authorities in the future, demonstrating that due diligence was performed in accordance with guidelines.

VI. The Principal Officer will ensure that the Client Identification Programme is formulated and implemented as per the requirements outlined in RBI Notification No. 16/42 dated July 1, 2015 (as amended) and the PML Rules of 2009.

VII. While a risk-based approach may be taken during the establishment of a business relationship, no exemptions from obtaining the minimum required information/documents from clients, as specified in the PMLA Rules, will be permitted for any class of investors regarding identity verification.

VIII. There will be no minimum investment threshold or category-based exemption for conducting Customer Due Diligence measures by the company.

IX. If a prospective client fails to provide satisfactory evidence of identity, including address, financial status, and the purpose of the intended relationship, a new account will not be opened, and the matter will be reported to higher authorities. This applies if the client's identity cannot be verified, if the information appears non-genuine, or if there is perceived non-cooperation from the client in providing complete information.

X. If the particulars of any customer match those of designated individuals/entities, **KHOSLA TRADEWISE** must immediately, within 24 hours of discovery, report the full details of any funds, financial assets, or economic resources held by such a customer to the Joint Secretary (IS.I) at the Ministry of Home Affairs. **KHOSLA TRADEWISE** will send the details of the aforementioned communication via post, fax, and email (sebi_uapa@sebi.gov.in) to the UAPA nodal officer at 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. This information will also be sent to the UAPA nodal officer of the state/UT where the account is maintained, as applicable, as well as to FIU-IND.

In addition to the above requirements, personnel opening new accounts may gather other independent information to satisfactorily verify the identity of each new client and the intended nature of the relationship.

8. Customer Due Diligence

Customer Due Diligence (CDD) can be categorized into two types: due diligence at the time of client acceptance and due diligence during periodic updates.

A. Client Acceptance

The company will conduct Customer Due Diligence before accepting any client. The following steps will be taken:

i) Obtain one certified copy of an officially valid document that includes identity and address details, one recent photograph, and any other documents related to the client's business nature and financial status as required.

ii) Verify the client's identity through the e-KYC process available via the Unique Identification Authority of India (UIDAI), with the client's consent.

B. Periodic Updation

The company may periodically update the KYC information of every customer at intervals and in manners prescribed by various circulars and regulations from relevant authorities.

Periodic updates will involve measures to confirm the identity, address, and other details of the customer based on their risk profile and considering when the last client due diligence measures were taken. If no updates are necessary, a self-certification from the customer will suffice. During periodic

updates, the company will ensure that updated records are submitted to the Central KYC Records Register.

KHOSLA TRADEWISE will exercise Customer Due Diligence (CDD) during both client acceptance and the ongoing relationship with clients, which will include:

(a) Gather sufficient information to identify individuals who beneficially own or control the securities account. If it becomes clear that the securities acquired or held in an account are beneficially owned by someone other than the client, that individual must be identified using client identification and verification procedures. The beneficial owner refers to the natural person or persons who ultimately own, control, or influence the client, as well as those acting on their behalf. This definition also includes individuals who exercise ultimate effective control over a legal entity or arrangement.

(b) Verify the client's identity using reliable, independent source documents, data, or information.

(c) Identify beneficial ownership and control by determining which individual(s) ultimately own(s) or control(s) the client and/or the person on whose behalf a transaction is conducted.

(d) Confirm the identity of the beneficial owner and/or the person on whose behalf a transaction is executed, corroborating the information provided in relation to (c).

(e) Understand the ownership and control structure of the client.

(f) Conduct ongoing due diligence by regularly scrutinizing transactions and the account throughout the business relationship to ensure that activities align with the Company's understanding of the client, their business, and risk profile, including the client's source of funds when necessary.

(g) Periodically update all documents, data, or information related to clients and beneficial owners collected during the CDD process.

(h) **KHOSLA TRADEWISE** will verify the client's identity using reliable, independent source documents, data, or information, particularly when the client claims to act on behalf of a legal entity, individual, or trust.

(i) Specifically verify the identity of the customer for any transaction exceeding Rs. 50,000, whether as a single transaction or multiple connected transactions, including any international money transfers.

(j) For non-profit organizations, **KHOSLA TRADEWISE** will register the client's details on the DARPAN portal of NITI Aayog and maintain records for five years following the end of the client relationship.

(k) If a client's transactions are suspected to involve money laundering or terrorist financing, **KHOSLA TRADEWISE** will not continue the CDD process and will instead file a Suspicious Transaction Report (STR) with FIU-IND.

Beneficial Ownership

Beneficial ownership refers to the ultimate individual owner of an entity. For non-individual shareholders, owners, partners, or beneficiaries, the ultimate individual beneficial owner must be identified in all instances, except for listed companies.

KHOSLA TRADEWISE PRIVATE LIMITED

KHOSLA TRADEWISE PVT LTD

Determination of Beneficial Ownership

According to SEBI Circulars CIR/MIRSD/2/2013 (dated January 24, 2013) and SEBI/HO/MIRSD/MIRSDSECFATF/P/CIR/2023/091 (dated June 16, 2023), when the client is not an individual or a trust (e.g., a company, partnership, or unincorporated association/body of individuals), the company must identify the beneficial owners and take reasonable steps to verify their identities. This includes:

Customer Due Diligence Procedures

When accepting a new client, the company shall:

i. Adopt a Risk-Based Approach.

ii. Verify identity, address, and financial status of the client and any individuals acting on their behalf, ensuring compliance with KYC norms established by the relevant exchange, depositories, and SEBI

The company should gather sufficient information to satisfactorily establish each new client's identity and the purpose of the intended relationship. KYC norms should be strictly followed when establishing client relationships and during transactions, especially if there are doubts about the accuracy or completeness of previously obtained identification data.

Accounts may only be opened after completing all required documentation and verifying it against original documents. In-person verification must be conducted in accordance with the guidelines set by SEBI, exchanges, or depositories.

Reliance on Third Parties

The Company may depend on a third party for (a) the identification and verification of a client's identity and (b) determining whether the client is acting on behalf of a beneficial owner, as well as identifying and verifying that beneficial owner's identity. This third party must be regulated, supervised, or monitored and have appropriate measures in place to comply with Customer Due Diligence (CDD) and record-keeping requirements in accordance with the PML Act. Such reliance must adhere to the conditions outlined in Rule 9(2) of the PML Rules and comply with the regulations and guidelines issued by SEBI from time to time.

Account Opening Restrictions

No accounts shall be opened under fictitious, benami names, or anonymously. The identity of the prospective client must not match any individual with a known criminal background or be subject to any bans, including those under UN sanction resolutions available at [UN Security Council Consolidated List](https://www.un.org/securitycouncil/content/un-sc-consolidated-list) or orders from other enforcement agencies.

When establishing and managing a client relationship, the Company will adopt a Risk-Based Approach as follows:

Risk Categories:

Low Risk: Individual clients with a clean image, not classified as Politically Exposed Persons (PEPs), and investments up to Rs. 50 lakhs, whose identity and sources of wealth can be easily verified.

Medium Risk: Clients with investments over Rs. 50 lakhs, where identity and sources of wealth are not substantiated by public documents (e.g., income tax returns, registered conveyance deeds).

High Risk: High Net Worth Individuals (HNIs) with a net worth exceeding Rs. 500 lakhs and no clear sources of income.

Other high-risk indicators include:

- Clients exhibiting sudden increases in investment or trading volumes without apparent justification.
- Clients who subsequently raise suspicions of money laundering or terrorist financing (ML/FT) activities.
- Government-owned companies, regulated entities such as banks, and PMLA-regulated intermediaries.

Additionally:

- Single share companies or those with bearer shares.
- Day traders and arbitrageurs.
- Clients with profiles perceived as uncertain or dubious by the branch.

Special Categories:

- Politically Exposed Persons (PEPs): Systems should be in place to identify PEPs, and reasonable measures should be taken to establish the source of wealth and funds on an ongoing basis.

Clients may be reclassified in real-time based on their evolving profiles. The CDD process will be revisited whenever there are suspicions of money laundering or financing of terrorism (ML/FT).

Clients of Special Category

Extra precautions will be taken when opening accounts for Clients of Special Category, which include:

a. Non-resident clients
b. High Net Worth Individuals (HNIs) with a net worth exceeding Rs. 500 lakhs
c. Trusts, charities, NGOs, and organizations receiving donations
d. Companies with closely held family shareholdings or beneficial ownership
e. Politically Exposed Persons (PEPs) of foreign origin
f. Current or former heads of state, high-profile politicians, and their close associates (including immediate family and advisors, as well as companies where they hold significant influence)
g. Companies involved in foreign exchange transactions
h. Clients from high-risk countries (where money laundering controls are ineffective, banking secrecy is unusually strong, narcotics production is active, corruption is prevalent according to the Transparency International Corruption Perception Index, or where government sanctions are in place; additionally, countries recognized as havens for international terrorism, offshore financial centers, tax havens, or those with high levels of fraud)
i. non-face-to-face clients
j. Clients with questionable reputations based on publicly available information

This list is illustrative, and the Company retains the discretion to determine whether new clients should be classified as Clients of Special Category.

In addition to the above, following is the broad categorization of clients based on various risk factors.

KHOSLA TRADEWISE PVT LTD

PMLA client categorization - KYC – Categorization of clients

Low Risk category (Investments up to Rs. 50 lakhs)	Medium Risk Category (Investments over Rs. 50 lakhs)	High Risk Category (annual income > Rs 1 cr or net-worth > Rs 5 cr)	Clients of Special Category
At the time of account opening			
1. Private Sector 2. Public Sector 3. Government Sector 4. Public Limited Companies 5. Private limited Companies 6. Institutional clients 7. Foreign Portfolio Investors 8. Foreign Direct Investors 9. Hindu Undivided Family	1. Agriculturist 2. Retired 3. Housewife 4. Student 5. Business 6. Professional 7. Any Others occupation 8. Partnership firms/Limited Liability Partnership /Association 9. Any other non-individual account	1. Politically exposed person 2. Terror list of clients as per SEBI AML circular 3. Non-face-to-face customers 4. Any Others not covered under low and medium risk category 5. Clients with dubious reputation as per public information available 6. Clients in high-risk countries	1. NRI 2. HNIs 3. Trusts, Charities, NGOs 4. Companies having close family shareholdings or beneficial ownership 5. Politically exposed person 6. Non face to face clients 7. Clients with dubious reputation as per public information available 8. Clients in high-risk countries 9. Companies dealing in foreign exchange offerings
Ongoing*			
	1. Change of e mail ID/mobile number more than 3 times in a FY 2. Multiple accounts opened by same client/family	1. Change of address made more than 3 times in a FY 2. Change of bank accounts more than 10 times in a FY 3. Sudden spurt in volume as per alerts sent by exchange not supported by sufficient collateral. 4. Frequent transactions within the family accounts/self	

Note:

1. HNI means individuals with annual income > Rs 1 Cr. or net-worth > Rs 5 Cr.
2. Frequent transactions means those transactions alerted by exchanges/depositories

* Change in Risk Categorization under Ongoing monitoring mechanism will be effective based on the recommendation of Operations head and approval by Business Head.

KHOSLA TRADEWISE PRIVATE LIMITED

9. Transaction Monitoring

Ongoing monitoring is a critical component of effective KYC procedures. **KHOSLA TRADEWISE** can better manage and mitigate risks by understanding the typical activities of its customers, enabling the identification of transactions that deviate from normal patterns. The Company will implement a robust transaction monitoring process from a KYC/AML perspective, establishing strong alert systems to proactively flag suspicious transactions and potential money laundering activities.

Awareness of transaction monitoring will be promoted at all departmental levels. The Principal Officer and other designated officials will work to update monitoring criteria based on current market conditions and client trading patterns. In addition to alerts generated internally, the Surveillance and Compliance team will also track alerts from various Exchanges and Depositories.

When a breach occurs, the Principal Officer will evaluate the situation based on the severity, account behaviour, and frequency of breaches, and will send inquiries to the relevant business unit, expecting responses within seven working days. If concerns persist or responses are unsatisfactory, the query will be escalated to the Compliance Head for further resolution.

For accounts with recurring alerts, risk categorization will be adjusted, in collaboration with the AML monitoring team and the Compliance Officer and reviewed at least monthly. Special scrutiny will be given to complex or unusually large transactions that lack a clear economic purpose. Comprehensive background checks, including all relevant documents and records, will be conducted, and findings will be documented.

All records related to these findings, including documentation, will be made available for review by auditors, SEBI, Stock Exchanges, FIU-IND, and other relevant authorities during audits or inspections. These records must be preserved for ten years as mandated by the PMLA 2002. The Company will ensure compliance with Section 12 of the PMLA 2002 and the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, reporting any suspicious transactions to the appropriate authorities.

10. Risk Assessment Strategies

i. The Company will conduct a risk assessment of clients through the Due Diligence process, identifying and evaluating risks related to money laundering and terrorist financing. This assessment will consider factors such as client profiles, geographical locations, transaction types and volumes, and payment methods. The assessment will also incorporate country-specific information provided by the Government of India and SEBI, as well as the updated list of sanctioned individuals and entities available through various United Nations Security Council Resolutions.

ii. The Company will identify and assess potential ML/TF risks arising from new delivery mechanisms and the use of emerging technologies for both new and existing clients.

iii. The risk assessment will take into account all relevant risk factors to determine the overall risk level and the appropriate mitigation strategies. This assessment will be documented, regularly updated, and made available to competent authorities and self-regulatory bodies as required.

11. Risk Management Approaches

KHOSLA TRADEWISE adopts a Risk-Based Approach (RBA) for the mitigation and management of identified risks, supported by policies approved by senior management, as well as relevant controls and procedures. The Company will monitor the implementation of these controls and enhance them as

needed. The Compliance, Risk Management, and Surveillance Departments are responsible for overseeing adherence to these practices. Concurrent and Internal Auditors will specifically review the application of KYC/AML procedures and report any lapses. Compliance reports will be presented to the Board's Member Committee.

12. Combating Financing of Terrorism (CFT)

KHOSLA TRADEWISE will maintain heightened awareness to identify transactions that may raise reasonable suspicion of financing activities related to terrorism.

13. Freezing of Funds, Financial Assets, or Related Services

Upon direction from the Central Government, FIU, SEBI, or any regulatory authority, **KHOSLA TRADEWISE** will freeze, seize, or attach funds and other financial assets associated with individuals or entities listed in relevant orders, or anyone suspected of involvement in terrorism. The Company will assess any suspicious transactions and consult the regulatory authority regarding the decision to freeze or close an account, following the provisions of Section 51A of the UAPA. The Government of India has outlined a procedure for compliance in an order dated February 2, 2021, which has been amended through a Gazette Notification dated June 8, 2021, and a corrigendum issued on March 15, 2023. The list of Nodal Officers for UAPA is available on the Ministry of Home Affairs website.

Maintenance of Records

Additionally, the Principal Officer will oversee the maintenance of the following records:

(i) All cash transactions exceeding ten lakh rupees or its equivalent in foreign currency.

(ii) All series of interconnected cash transactions that individually fall below ten lakh rupees but collectively exceed that amount within a month.

(iii) All cash transactions involving counterfeit currency or valuable securities.

(iv) All suspicious transactions, regardless of whether they are cash-based. A suspicious transaction refers to any transaction, including credits or debits to non-monetary accounts such as demat or security accounts, that raises reasonable suspicion for a person acting in good faith because it:

- Suggests a possibility of proceeds of crime,
- Exhibits unusual or unjustified complexity, or
- Lacks economic rationale or a bona fide purpose.

Below is a list of circumstances that may indicate suspicious transactions. This list is illustrative, and whether a transaction is deemed suspicious will depend on the specific context, details, and circumstances surrounding it.

a) Clients whose identity verification is challenging or who appear uncooperative;

b) Asset management services for clients with unclear sources of funds that do not align with their apparent status or business activities;

c) Clients located in high-risk jurisdictions;

d) Significant increases in business activity without a clear explanation;

e) Clients transferring large amounts of money to or from overseas, with cash payment instructions;

f) Attempts to transfer investment proceeds to seemingly unrelated third parties;

g) Unusual transactions by clients of special category and businesses involved with offshore banks or financial services, particularly those reported to engage in small-scale export-import activities.

14. Record-Keeping Requirements

The records shall include the following details:

- The nature of the transactions
- The transaction amount and the currency used
- The date of the transaction

- The parties involved in the transaction

The Company will also strive to maintain adequate records to reconstruct individual transactions (including amounts and types of currencies involved) to provide evidence for criminal investigations if necessary. To this end, we will retain documents related to:
(a) The beneficial owner of the account
(b) The volume of funds flowing through the account
(c) For selected transactions:
- The origin of the funds
- The method of funds offered or withdrawn (e.g., cash, cheques)
- The identity of the person conducting the transaction
- The destination of the funds
- The form of instruction and authority

The Principal Officer must ensure that all customer and transaction records are readily available to competent investigating authorities. When appropriate, he may choose to retain certain records, such as customer identification, account files, and business correspondence, for periods that exceed the requirements set by the SEBI Act, the PMLA 2002, other relevant laws, and Exchange/Depository regulations or circulars.

15. Retention of Records

(a) The Company will maintain necessary records of both domestic and international transactions for at least the minimum period prescribed under the SEBI Act, 1992, its associated Rules and Regulations, the PMLA, and other relevant legislation, Rules, Regulations, and Exchange/Depository Bye-laws and Circulars issued periodically.

(b) Records related to client identification (such as copies of official identification documents like passports, identity cards, and driving licenses), account files, and business correspondence will also be retained for the same duration.

(c) For records associated with ongoing investigations or transactions, whether attempted or executed, that have been reported to the Director of FIU-IND as required under Rules 7 and 8 of the PML Rules, these will be maintained for a minimum of eight years from the date of the transaction or until it is confirmed that the case has been resolved.

(d) Additionally, in accordance with Regulations 54 and 66 of the SEBI (Depositories and Participants) Regulations, 2018, **KHOSLA TRADEWISE** will preserve records and documents for a minimum of eight years.

16. Procedure for implementation of Section 12A of the Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005

In compliance with the Section 12A of the WMD Act, KTWPL shall maintain and update the list of individuals/entities ("**Designated List**") on regular interval.

KTWPL shall inform the transaction details to the Central Nodal Officer of FIU India & also to the Nodal Officer of SEBI in following instances:

KHOSLA TRADEWISE PRIVATE LIMITED

1. Verify if the particulars of the entities/individual, party to the financial transactions & it matches with the particulars of the Designated List.
2. At the time of establishing a relation with a client and on a periodic basis to verify whether individuals and entities in the Designated List are holding any funds, financial assets or economic resources or related services, in the form of bank accounts, stocks, insurance policies etc.

KTWPL shall prevent such individual/entity from conducting financial transactions, under intimation to the CNO, without delay, in case there are reasons to believe beyond doubt that funds or assets held by a client would fall under the purview of Section 12A (2)(a) or Section 12A(2)(b) of the WMD Act & file a Suspicious Transaction Report (STR) with the FIU-IND covering all transactions in the accounts.

KTWPL shall also comply with the provisions regarding exemptions from the above orders of the CNO and inadvertent freezing of accounts, as may be applicable.

List of Designated Individuals/ Entities

The Ministry of Home Affairs, in pursuance of Section 35(1) of UAPA 1967, declares the list of individuals/entities, from time to time, who are designated as 'Terrorists'. The registered intermediaries shall take note of such lists of designated individuals/terrorists, as and when communicated by SEBI. All orders under section 35 (1) and 51A of UAPA relating to funds, financial assets or economic resources or related services, circulated by SEBI from time to time shall be taken note of for compliance.

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. The details of the lists are as under:

- The "ISIL (Da'esh) & Al-Qaida Sanctions List", which includes names of individuals and entities associated with the Al-Qaida.
- The list issued by United Security Council Resolutions 1718 of designated Individuals and Entities linked to Democratic People's Republic of Korea.

KTWPL shall ensure that accounts are not opened in the name of anyone whose name appears in said list. Registered intermediaries shall 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 list.

KTWPL shall maintain updated designated lists in electronic form and run a check on the given parameters on a regular basis to verify whether the designated individuals/entities are holding any funds, financial assets or economic resources or related services held in the form of securities with them. KTWPL shall leverage latest technological innovations and tools for effective implementation of name screening to meet the sanctions requirements.

KTWPL shall file a Suspicious Transaction Report (STR) with FIU-IND covering all transactions carried through or attempted in the accounts covered under the list of designated individuals/entities under Section 35 (1) and 51A of UAPA ,Report should include full details of accounts bearing resemblance with any of the individuals/entities in the list shall immediately be intimated to the Central [designated] Nodal Officer for the UAPA & also send a copy of the communication mentioned above to the UAPA Nodal Officer of the State/UT where the account is held and to SEBI and FIU-IND.

17. Employee Hiring, Training, and Investor Education

We have implemented comprehensive screening procedures, including background checks, to ensure high standards during the hiring process. Considering the risks associated with money laundering and terrorist financing, as well as the size of our business, the Company will identify key positions and ensure that employees filling these roles are qualified and capable of performing their responsibilities.

An ongoing training program has been developed under the leadership of the Principal Officer to ensure that staff members are adequately trained in AML and CFT procedures. Training will be tailored to different roles, including frontline staff, back-office personnel, compliance teams, risk management staff, and those interacting with new clients. Employees will gain a thorough understanding of this policy, its obligations, and requirements, enabling them to implement it consistently while being aware of the risks of misuse by unscrupulous entities.

We have established in-house training initiatives, which include educational pamphlets, videos, intranet resources, in-person lectures, and explanatory memos. Implementing AML/CFT measures necessitates requesting certain personal information from investors, such as documents that verify the source of funds, income tax returns, and bank records. This may raise questions from customers regarding the rationale behind collecting such information. Therefore, we will inform our customers about these requirements as mandated by the AML and CFT framework. We will create specific literature, pamphlets, and hold conferences to educate customers on the objectives of our AML/CFT program.

We will apply the same AML procedures to employee accounts as we do for customer accounts, with oversight from the Principal Officer. The Board of Directors will review the accounts of the Principal Officer.

Employees are required to report any violations of the company's AML compliance program to the Principal Officer, unless the violations involve the Principal Officer, in which case the report should be made to the Board. All reports will be confidential, and employees will not face any retaliation for making them

18. Reporting to the Financial Intelligence Unit-India

As per PMLA rules, the Principal Officer is required to report information regarding cash and suspicious transactions to the Director of the 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: fiuindia.gov.in

KHOSLA TRADEWISE PRIVATE LIMITED

For Cash Transaction Reporting (CTR), any dealings in cash that require reporting to FIU-IND will be done in the CTR format at intervals prescribed by the FIU-IND. The monthly Cash Transaction Report (CTR) will be submitted to FIU-IND by the 15th of the following month.

For Suspicious Transaction Reporting (STR), we will document any suspicious transactions that are not satisfactorily explained to the Principal Officer and report these to FIU-IND within the required deadlines. If a client aborts or abandons a suspicious transaction after being questioned by Company officials, this will also be reported to FIU in the STR, regardless of the transaction amount.

Our decision to file an STR will not solely depend on whether a transaction exceeds a specific threshold. We will report all transactions that raise identifiable suspicions of criminal or terrorist activity to law enforcement.

We will not inform any parties involved in the transaction or any third party that a report has been made, except as permitted by the PML Act and its Rules.

The Suspicious Transaction Report (STR) will be submitted within seven days of concluding that any transaction, whether cash or non-cash, or a series of connected transactions, is suspicious in nature. The Principal Officer will document the reasons for classifying any transaction or series of transactions as suspicious, ensuring there is no undue delay in reaching this conclusion.

The Non-Profit Organization Transaction Reports (NTRs) will be submitted to FIU-IND by the 15th of the following month.
The Principal Officer will be accountable for the timely submission of Cash Transaction Reports (CTR), Suspicious Transaction Reports (STR), and Non-Profit Organization Transaction Reports (NTR) to FIU-IND, and will report to senior management or the Board of Directors as needed. It is crucial to maintain strict confidentiality when filing CTR, STR, and NTR with FIU-IND. These reports may be submitted online or sent via speed/registered post or fax to the designated address. There is no requirement to submit a nil report to FIU-IND if there are no cash or suspicious transactions to report. We will ensure that no operational restrictions are placed on accounts associated with an STR.

KHOSLA TRADEWISE, along with its directors, officers, and employees (both permanent and temporary), is prohibited from disclosing or "tipping off" anyone about the filing of an STR or related information to FIU-IND. It is imperative to prevent any such disclosure to clients at any level. Our company will create and maintain STRs, NTRs, and CTRs, along with the relevant documentation concerning customer identity and verification. We will retain these records for at least ten years, adhering to the prescribed formats and utilizing the necessary hardware and technical requirements for report generation.

.

The Principal Officer will ensure that this policy is communicated to all management and relevant staff, including directors, department heads, branches, and group companies.

Should there be any changes to the PMLA Act or its Rules that render any provision of this policy inconsistent with the law, the Act or Rules will take precedence, and the policy will be modified accordingly to ensure compliance.

KHOSLA TRADEWISE PRIVATE LIMITED

KHOSLA TRADEWISE PVT LTD

This revised AML program has been approved as adequately designed to ensure our company's ongoing compliance with the requirements of the PMLA and its implementing regulations. The Member Committee will oversee the implementation of the AML policy framework.
This policy was last reviewed and presented to the Member Committee on September 27, 2024.