KFIN TECHNOLOGIES LIMITED

ANTI-MONEY LAUNDERING AND KNOW YOUR CLIENT POLICY

SIGNATORIES

Version	Prepared by	Reviewed by	Approved by
1.0	Compliance Team	**Mr. Anish Kumar** Chief Compliance Officer	Board of Directors

VERSION CONTROL

Version	Date	Description	Description of Changes
1.0	April 08, 2026	Anti-Money Laundering and Know Your Client Policy	New Policy

TABLE OF CONTENTS

I. INTRODUCTION

In accordance with the SEBI Master Circular on Anti-Money Laundering (AML)/ Know Your Client (KYC)/ Standards and Combating the Financing of Terrorism (CFT) dated June 06, 2024 ("SEBI Master Circular"), PFRDA Master Circular on KYC/AML/CFT dated September, 25, 2025 and International Financial Services Centers Authority (IFSCA) AML/CFT and KYC Guidelines, 2022, as amended from time to time, KFIN Technologies Limited including its subsidiaries, joint ventures and branches (collectively referred to as "Company"/ "KFintech") is required to formulate and implement a policy for addressing risks related to money laundering and financing of terrorism, in line with applicable regulatory requirements. Accordingly, KFINTECH in its capacity as a SEBI, PFRDA and IFSCA registered intermediary, has formulated this policy, in its role as RTA, KCRA and Fund administrator which will cover various services provided to Mutual Funds, Listed Companies, NPS Trust, AIFs and others.

By means of this policy (Policy), KFINTECH will endeavor to uphold the spirit of the guidance and directives issued by SEBI, PFRDA, IFSCA and Prevention of Money Laundering Act, 2002 ("**PMLA**") along with Prevention of Money Laundering (Maintenance of Records) Rules, 2005 ("**PML Rules**"), and related circulars, guidelines, regulations, rules issued by SEBI, PFRDA, IFSCA, FIU India and other relevant authorities from time to time.

II. SCOPE AND APPLICABILITY

The scope of this Policy includes KFINTECH's policy for client identification, client due diligence, record maintenance on behalf of AMCs, providing various reports to AMCs, including suspicious transaction reports, risk profiling and others, in accordance with the applicable regulations. This Policy also provides the governance structure for the key appointments responsible for AML/CFT/KYC compliance, systems and controls in place to ensure adherence to the regulatory requirements with respect to services provided to AMCs. This policy also ensures that the concerned staff are adequately trained in KYC/AML procedures. The provisions of this Policy will be applicable to all employees, officials, agents, representatives of KFINTECH and all its subsidiaries with the following objectives:

a. To prevent KFINTECH from being misused by money launderers intentionally or unintentionally to facilitate their illicit business activities.
b. To enable KFINTECH in assisting law enforcement agencies across jurisdictions to identify and track down money launderers.
c. To ensure that KFINTECH is compliant with the relevant anti-money laundering legislations and regulations, as applicable.
d. To create awareness and provide clarity on the KYC standards and AML measures
e. To have a proper Client Due Diligence (CDD) process.
f. To undertake Enhanced Due Diligence (EDD) process in case of high-risk profile clients.
g. To monitor and report Suspicious Transactions.

III. KEY DEFINITIONS

For the purpose of this Policy, key definitions are as follows:

1. **"Act/ PML Act/PMLA/PMLR"** means the Prevention of Money Laundering Act, 2002 and the Prevention of Money Laundering (Maintenance of Records) Rules, 2005.

2. **"Beneficial owner"** shall mean and include a natural person or persons who ultimately owns, controls or influences a client/ or person on whose behalf a transaction is being conducted or a person who exercises ultimate effective control over a legal person or arrangement.

3. **"Client/Customer"** - refers to a person who is engaged in a financial transaction or activity with Asset Management Companies (AMCs) serviced by KFINTECH. This also includes any person on whose behalf the individual engaged in the transaction or activity is acting.

4. **"Central KYC Records Registry" ("CKYCR")** - the Government Company, authorized to receive, store, safeguard and retrieve the KYC records of a customer in digital form.

5. **"Client Due Diligence (CDD)"** shall mean the due diligence activity carried out on a client referred to in clause (ha) of sub-section (1) of section 2 of the PMLA using reliable and independent sources of identification.

6. **"Designated Director"** means a person designated by the reporting entity to ensure overall compliance with the obligations imposed under chapter IV of the Act and the Rules and includes-

    a. the Managing Director or a Whole-Time Director duly authorized by the Board of Directors if the reporting entity is a company,
    b. the managing partner if the reporting entity is a partnership firm,
    c. the proprietor if the reporting entity is a proprietorship firm,
    d. the managing trustee if the reporting entity is a trust,
    e. a person or individual, as the case may be, who controls and manages the affairs of the reporting entity if the reporting entity is an unincorporated association or a body of individuals, and
    f. such other person or class of persons as may be notified by the Government if the reporting entity does not fall in any of the categories above"

7. **"Digital KYC"** shall have the meaning assigned to it under clause (bba) of sub-rule (1) of Rule 2 of the PML Rules.

8. **"Employee"** means a person engaged by a company whose appointment, terms, and conditions of service or engagement are governed by the applicable rules of the company, and includes whole-time employees of a company or its group entities or subsidiaries or joint ventures, whether permanent or otherwise, as recognised under the relevant regulations.

9. **"e-KYC authentication facility"** means an authentication facility as defined in Aadhar (Authentication) Regulations, 2016.

10. **"Financial Intelligence Unit- India"** refers to a national agency, set by the Government of India, which is inter-alia responsible for receiving, processing, analyzing and disseminating information relating to suspicious financial transactions.

11. **"Group"** – The term group shall have the same meaning assigned to it in clause (cba) of sub-rule (1) of Rule 2 of the PML Rules and amended from time to time. Groups are required to implement group-wide policies for the purpose of discharging obligations under Chapter IV of the PMLA.

12. **"Know Your Client (KYC) Identifier"** means the unique number or code assigned to a client by the Central KYC Records Registry.

13. **"KYC User Agency (KUA)"** is an entity approved by UIDAI that, in addition to being an AUA, is authorised to use the Aadhaar e-KYC authentication facility to fetch a customer's Aadhaar demographic details (such as name, address, photograph) with the user's consent, for the purpose of completing KYC.

14. **"KYC Registration Agency (KRA)"** means an entity which has been granted certificate of registration under the International Financial Services Centres Authority (KYC Registration Agency) Regulations, 2025

15. **"On-going Due Diligence"** means regular monitoring of transactions to ensure that they are consistent with the subscriber's profile and source of funds.

16. **"Officially Valid Documents" or "OVD"** includes the following the passport; the driving license; proof of possession of Aadhaar number; the voter's identity card issued by Election Commission of India; Job card issued by NREGA, duly signed by an officer of the State Government; Letter issued by the National Population Register containing details of name, address, or any other document as notified by the Central Government in consultation with the regulator; the Permanent Account Number (PAN) Card; the letter issued by the Unique Identification Authority of India or the National Population Register containing details of name, address and Aadhaar number.

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

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

    b. letter issued by a gazetted officer, with a duly attested photograph of the person;

    Provided further that where simplified measures are applied for verifying the limited purpose of proof of address of clients, where a prospective client is unable to produce any proof of address, the following documents including e-documents thereof shall also be deemed to be 'officially valid document':

    a. utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, Water bill);
    b. property or Municipal tax receipt;

c. bank account or Post Office savings bank account statement or if the reporting entity is located in an International Financial Services Centre, statement of foreign bank;
d. pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
e. letter of allotment of accommodation from employer issued by State or Central Government Departments, statutory or regulatory bodies, Public Sector Undertakings, scheduled commercial banks, financial institutions and listed companies. Similarly, leave and license agreements with such employers allotting official accommodation.

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

Provided also that in an International Financial Services Centre, the national identity card and voter identification card, by whatever name called, are issued by the Government of foreign jurisdictions or agencies authorised by them capturing the photograph, name, date of birth and address of a foreign national shall also be considered as officially valid document

Provided also that where the client submits his proof of possession of Aadhaar number as an officially valid document, he may submit it in such form as are issued by the Unique Identification Authority of India.

17. **"Politically Exposed Persons (PEPs)"** - PEP shall have the same meaning as given in clause (db) of sub-rule (1) of rule 2 of the PMLR. The additional norms applicable to PEP as contained in the subsequent paragraph 20 of the SEBI Master Circular shall also be applied to the accounts of the family members or close relatives / associates of PEPs;

18. **"Principal Officer"** means an officer designated by reporting entity. Provided that such officer shall be an officer at the management level

19. **"Regulated Entity"** means a unit/entity which has been granted license, recognition, registration or authorization by the Authority.

20. **"Suspicious transaction"** - a transaction, including an attempted transaction, whether or not made in cash, which, to a person acting in good faith:

    a. gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the schedule to PMLA, regardless of the value involved; or
    b. appears to be made in circumstances of unusual or unjustified complexity; or
    c. appears to not have economic rationale or bona-fide purpose; or
    d. gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

Transaction involving financing of the activities relating to terrorism includes transaction involving funds suspected to be linked or related to, or to be used for terrorism, terrorist acts or by a terrorist, terrorist organization or those who finance or are attempting to finance terrorism.

21. **"Transaction"** means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes-
    a. opening of an account;
    b. deposits, withdrawal, exchange or transfer of funds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other nonphysical means;
    c. use of safety deposit box or any other form of safe deposits;
    d. entering into any fiduciary relationship;
    e. any payment made or received in whole or in part of any contractual or other legal obligation;

    establishing or creating a legal person or legal arrangement.
22. **"Unique Identification Authority of India (UIDAI)**" is the statutory authority established under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

23. **"Video based Customer Identification Process" or "V-CIP"** means an alternate method of customer identification with facial recognition and customer due diligence, by an authorized official of the Regulated Entity, by undertaking seamless, secure, live, informed & consent based audio-visual interaction with the customer to obtain identification information required for Customer Due Diligence purpose, and to ascertain the veracity of the information furnished by the customer through independent verification and maintaining audit trail of the process.

IV. KEY APPOINTMENTS

The following are the key appointments for the purpose of this Policy:

1. **PRINCIPAL OFFICER** - The Principal Officer shall be a senior management level officer appointed by KFINTECH, capable of discharging the functions with objectivity and authority and shall be responsible for:

    i. Ensuring that the relevant reports with respect to suspicious transactions are submitted to the concerned authorities;
    ii. Acting as a central reference point in facilitating onward reporting of suspicious transactions;
    iii. Actively identifying and assessing potentially suspicious transactions;
    iv. Reporting the suspicious transactions to the Designated Director and/or the Board of KFINTECH; and
    v. Advising and training employees, officers and representatives on developing and implementing internal policies, controls and Standard Operating Procedures (SOP) on Anti- Money Laundering (AML) /Combating Financing of Terrorism (CFT).
    vi. Promptly informing employees, officers and representatives of KFINTECH of any regulatory changes.

vii. Maintaining close liaisons with the regulator and other supervisory authorities.

viii. Periodically reporting information to the Designated Director in respect of transactions referred to in clauses (A), (B), (BA), (C), (E) and (F) of sub-rule (1) of Rule 3 of the PMLA Rules 2005.

ix. Periodic reporting on key AML/CFT risk assessment and control issues and allied necessary remedial actions, arising from audit, inspection and compliance reviews to the Board of Directors of KFINTECH.

x. Mandatorily[a] obtain the prescribed National Institute of Securities Markets (NISM) certification or any alternate certification as required by the regulatory bodies.

2. **DESIGNATED DIRECTOR** - The Designated Director[b] shall be responsible for ensuring the overall compliance with the obligations imposed under Chapter IV of the PMLA 2002 and PMLR 2005. The Designated director shall also oversee periodic review of KYC/AML/CFT policies and maintain board-level accountability for compliance. The Designated Director shall mandatorily[c] obtain the prescribed National Institute of Securities Markets (NISM) certification or any alternate certification as required by the regulatory bodies.

V. ANTI-MONEY LAUNDERING PROGRAM (AML)

The goal of having an AML program in place is to ensure appropriate policy, practice and procedure, subsequently aiding in preventing money-laundering activities. Such procedures would include the following:

- Entering into transactions and business relations with only those entities that are compliant with AML legislations, policies and procedures as applicable to them.
- Appointment of Principal Officer.
- Transaction monitoring to identify and report Suspicious Transactions (STR).
- Retention of records as per applicable regulation.
- Co-operation with law enforcement agencies to support in their efforts to trace money-laundering transactions and potential perpetrators involved in such activities.
- Providing training and awareness to the employees to ensure strict adherence to this policy.

The procedures and standards enshrined in this policy would typically assist in knowing and understanding the activities of the existing and prospective clients of KFINTECH and to prevent KFINTECH from being used as a medium, intentionally or unintentionally for carrying out money-laundering activities.

---

[a] *Certification Course on Anti-Money Laundering and Counter-Terrorist Financing in the IFSC as set out in the circular IFSCA-DAC/8/2024-AMLCFT dated November 17,2025.*

[b] *KFIN regulated by PFRDA shall submit the contact details of Designated Director and Principal Officer to PFRDA and FIU-IND, whereas if regulated by SEBI/IFSCA it shall submit the details to FIU-IND.*

[c] *Certification Course on Anti-Money Laundering and Counter-Terrorist Financing in the IFSC as set out in the circular IFSCA-DAC/8/2024-AMLCFT dated November 17,2025.*

VI. BOARD OVERSIGHT

The board shall be responsible for:

a. Approving the KYC/AML/CFT Policy framed and any amendments made to it thereto.
b. Reviewing the effectiveness of the policy and its implementation
c. Monitoring the relevant regulatory requirements.
d. Ensuring adequate resources and effective infrastructure are in place to support the AML efforts.
e. Overseeing investigations into AML breaches and ensuring appropriate corrective actions are taken.
f. Approving the client Due Diligence Program.
g. Reviewing and approving the actions taken in response to AML breaches, including disciplinary measures and enhancements to prevent future breaches.
h. Reviewing Audit notes and compliances in the absence of the Audit Committee.

VII. RISK ASSESSMENT AND FRAMEWORK

KFINTECH may be exposed to various risks, both on account of its own nature / activities and the attributes of its client such as their location (registered office addresses, correspondence addresses and other addresses if applicable), identity, nature of business activity, trading turnover, manner of making payment for transactions undertaken, etc. Based on these parameters, KFINTECH will then apply enhanced or simplified due diligence measures.

The methodology and guiding principles for assessing and managing risks associated with Anti-Money Laundering/Combating the Financing of Terrorism / Know Your Customer (AML/CFT/KYC) is outlined in **ANNEXURE I** attached with this policy.

VIII. CLIENT IDENTIFICATION AND KNOW YOUR CUSTOMER (KYC):

KFINTECH shall implement effective Client or Customer Identification Procedures (CIP), post the risk categorization of the client is done. For the purpose of CIP, KFINTECH shall adhere to the following principles:

- It shall identify the client by using reliable sources including documents / information.
- It shall obtain adequate information about the identity of each client and the purpose of the intended nature of the relationship.
- The obtained information must be adequate enough to satisfy competent authorities (regulatory / enforcement authorities) that due diligence was conducted in compliance with applicable laws.
- Each original document shall be seen prior to acceptance of a copy.

The detailed steps for implementing proper and effective client identification is mentioned in **ANNEXURE II** and undertaking KYC[d] norms are mentioned in **ANNEXURE III** as attached with this policy.

---

[d] *KFINTECH shall ensure its registration with the Central KYC Records Registry (CKYCR) and KYC Registration Agency ("KRA") as required under the SEBI (KYC Registration Agency) Regulations, 2011, and the KYC details of new/ existing client, as and when required shall be uploaded on these repositories, as prescribed under SEBI regulations.*

KFINTECH shall perform Client Due Diligence (CDD) measures as a SEBI/IFSCA/PFRDA regulated intermediary after assigning the risk rating for each Customer proportionate to their AML/CFT risks. The following measures shall also be considered during CDD:

a. Undertake CDD measures for all the customers.
b. Undertake Enhanced Customer Due Diligence measures in addition to CDD measures in respect of customer who has been assigned 'high risk' and,
c. Undertake Simplified Customer Due diligence measures by modifying Customer Due Diligence process in respect of customer who has been assigned 'low risk'.

KFINTECH shall apply the Enhanced Due Diligence (EDD) measures depending upon the risk profile, and the extent of its applicability shall be decided on case-to- case basis.

It is mandatory for KFINTECH to ensure that it does not have any account in the names of individuals/entities appearing in the list of individuals and entities, suspected of having terrorist links, which are approved by and periodically circulated by United Nations Security Council (UNSC) namely; the "ISIL (Da'esh) & Al-Qaida Sanctions List" and the "1988 Sanctions List", Local list of banned entities and individuals issued by the Ministry of Home Affairs.
Under Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS).
KFINTECH shall adhere to the provisions of Income Tax Rules[e] and determine whether it is a Reporting Financial Institution, if so, it shall take steps for complying with the reporting requirements.

CDD conducted by third parties

KFINTECH may engage 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 must have measures in place to comply with CDD and record-keeping requirements in line with the obligations under the PML Act.

It shall also be ensured that KFINTECH shall:

- immediately, obtains necessary information of the client due diligence carried out by the third party.
- Take adequate steps to satisfy itself that copies of identification data and other relevant documentation relating to the client due diligence requirements will be made available from the third party upon request without delay.
- Ensure that the third party is regulated, supervised or monitored and has system in place to comply with client due diligence and record-keeping obligations under the PMLA.

[e] *mentioned in clause 11.5 of the IFSCA (AML-CFT) Guidelines where acting as an IFSCA regulated entity*

- Ensure that the third party is not based in a country or jurisdiction assessed as high risk.
- KFINTECH shall be ultimately responsible for client due diligence and undertaking enhanced due diligence measures, as applicable.

IX. RECORD KEEPING AND AUDIT

KFINTECH shall ensure compliance with the record keeping requirements contained in the SEBI Act, 1992, Rules and Regulations made thereunder, PFRDA Guidelines, IFSCA Guidelines, PMLA as well as other relevant legislation, Rules, Regulations, Exchange Byelaws and Circulars

KFINTECH shall take appropriate steps to evolve an internal mechanism for proper maintenance and preservation of records and information.

The AML/CFT framework is required to be subjected to periodic audits.

The specific documentation standards and audit procedures referenced in this clause shall be read in conjunction with **ANNEXURE IV** of this Policy, which provides detailed guidance on record-keeping and audit requirements."

DATA SECURITY AND CONFIDENTIALITY

KFINTECH shall ensure strict confidentiality of all customer information, KYC documents, STRs, CTRs, NTRs, and AML related data, granting access only on a need to know basis and in compliance with the Information Security Management System (ISMS) and established security standards. Adequate technical and organizational safeguards shall be maintained to prevent unauthorized access, alteration, disclosure, or loss. All data shall be encrypted in transit and at rest using industry standard protocols.

Information may be disclosed only as per applicable laws and regulatory requirements, including to FIUIND, SEBI, PFRDA, IFSCA, or other competent authorities. Access to AML systems and customer data shall be strictly controlled via multifactor authentication and role based access.

Employees are strictly prohibited from tipping off customers regarding STR filings or related inquiries.

Regular VAPT (Vulnerability Assessment & Penetration Testing) shall be conducted to identify and mitigate security risks. All APIs or electronic interfaces used for KYC status sharing or data transmission shall be secured with authentication controls and continuous monitoring.

X. MONITORING OF TRANSACTIONS

KFINTECH shall implement a robust mechanism for identifying and reporting suspicious transactions. The Principal Officer shall be immediately apprised in the event any suspicious transaction has been identified by means of a detailed report comprising all the necessary particulars related to the transaction/client.

KFINTECH shall mandatorily pay attention to all complex, unusually large transactions and analyze unusual patterns/trends which potentially have no apparent economic or visible lawful purpose.

KFINTECH shall adopt the process of random sampling which involves examination of randomly selected series of transactions undertaken by clients. It shall thereafter comment on the nature of suspicion post analysis.

XI. IDENTIFYING SUSPICIOUS TRANSACTIONS

KFINTECH shall establish and maintain policies, procedures, systems and controls in order to monitor and detect suspicious transactions with respect to potential ML/TF.

KFINTECH shall put in place such policies, procedures, systems and controls which ensure that whenever any of its employee, acting in the ordinary course of his employment, either:

i. knows;
ii. suspects; or
iii. has reasonable grounds for knowing or suspecting.

that a person is engaged in or attempting ML/TF, that employee promptly notifies the Principal Officer of the Regulated Entity with all relevant details.

The prohibition of tipping off extends not only to the filing of the Suspicious Transaction Report (STR) and/ related information, but also includes during and after submission of STR.

Where a suspicion or detection of an indicator or combination of indicators arises KFINTECH shall promptly increase the monitoring as well as assess whether such transactions shall be reported to FIU-IND.

XII. REPORTING OF SUSPICIOUS TRANSACTIONS (STR)

The Principal Officer shall analyze and examine any suspicious transaction and then, based on reasonable justification, decide if any such transaction warrants a closer inspection. It shall maintain the records of such data received and the actions taken thereon.

In case the Principal Officer comes across any transaction that appears to be of suspicious nature, it shall submit the report of such transactions to the Director, Financial Intelligence Unit – India (FIU – IND), in the prescribed format and following guidelines in parlance to Regulation SEBI.

In terms of the rules, KFINTECH is mandated to report suspicious transactions to the above-mentioned authority at the following address[f]:

Director, FIU – IND,
Financial Intelligence Unit – India,
6th Floor, Tower 2, Jeevan Bharati Building,
Connaught Place, New Delhi – 110001,
Telephone: 91-11-23314429, 23314459
Website: http://fiuindia.gov.in

[f] *Only KFINTECH entity regulated by SEBI shall use the mentioned address and is not applicable for IFSCA & PFRDA regulated entity.*

KFINTECH shall from time to time abide and comply with the circulars and guidelines issued by the regulators in this regard.

KFINTECH shall promptly respond to all queries, notices, inspections, etc. issued by regulatory authorities. This shall include timely submission of requested data, explanations and reports. It shall extend complete co-operation to FIU-IND, law enforcement agencies and other government authorities in relation to AML/CFT investigations, inquiries or information requests.

The detailed process and guidelines with respect to identifying, monitoring and reporting the transactions is mentioned in **ANNEXURE-V** **(Suspicious Transaction Monitoring and Reporting)** and is attached with this policy.

XIII. COMPLIANCE OBLIGATIONS UNDER INTERNATIONAL AGREEMENTS AND DOMESTIC LAWS

KFINTECH shall comply with all obligations arising under international sanctions frameworks and domestic laws relating to counter-terrorism, counter-proliferation, and related financial restrictions, including the Unlawful Activities (Prevention) Act, 1967 (UAPA), the Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005, relevant UN Security Council Sanctions Lists, and FATF public statements on high-risk and monitored jurisdictions.

KFINTECH shall ensure adherence to the screening, verification, reporting, freezing, escalation, and confidentiality requirements prescribed under applicable Government Orders, notifications, and circulars issued by regulators.

The detailed processes, procedures, and regulatory requirements relating to the implementation of these obligations—including name screening, handling of designated persons, reporting to nodal authorities, compliance with UAPA Section 51A and WMD Act Section 12A, management of high-risk jurisdictions, and reporting under Foreign Account Tax Compliance Act/ Common Reporting Standards (FATCA/CRS)—are provided in **ANNEXURE-VI** **(Compliance Obligations under International Agreements and Domestic Laws).**

XIV. COMBATING FINANCING OF TERRORISM

KFINTECH will regularly screen all its clients against the UN Sanctions Lists and report such details to SEBI/IFSCA/PFRDA and FIU-IND in case any match is found.
It shall also regularly screen the list declared by the Ministry of Home Affairs ("**MHA**"), in pursuance of Section 35(1) of Unlawful Activities (Prevention) Act, 1967 ("**UAPA**"), of individuals/entities, from time to time, who are designated as 'Terrorists'.
KFINTECH shall also ensure that it will not engage with anyone whose name appears on the UN Sanctions Lists or the UAPA list. KFINTECH will also ensure expeditious and effective implementation of the procedure prescribed under Section 51A of UAPA with regard to freezing/ unfreezing of financial assets of the designated individuals/entities enlisted in the UN Sanctions Lists and especially, with regard to funds, financial assets or economic resources or related services held in the form of securities, if any.

XV. GENERAL COMPLIANCES

A. Training of employees:

The Principal Officer shall conduct or facilitate conducting AML awareness programs and related trainings for each employee of KFINTECH to ensure that they are aware of their obligation and duties under the provisions of this policy.

The training shall enable employees to:

- Comprehend the applicable laws in respect to money-laundering including but not limited to appropriate laws, regulations, rules and guidelines.
- Understand and comprehend policies, SOPs, systems, controls and any modifications thereto, put in place by the organization with respect to AML.
- Recognize and deal with transactions and other allied activities falling under the scope of money-laundering.
- Comprehend the nature of activity which may potentially constitute as suspicious transaction and promptly notify the same to the Principal Officer.
- Keeping abreast with prevailing techniques, methods and trends to deal with money-laundering scenarios, relevant to the business of KFINTECH.
- Understand their respective roles and responsibilities in combating money laundering cases as may be guided by the Principal Officer.
- Understand the relevant findings, recommendations, directives, resolutions, sanctions, notices or other conclusions as described in the Guidelines.

KFINTECH shall also ensure that such training shall be relevant and tailored to the business activities carried out by KFINTECH including products, services, customers, distribution channels, business partners.

B. Key reporting platform

i. KYC Registration Agency (KRA)

- KFINTECH shall maintain its registration with CERSAI for the purpose of KYC compliance.
- KFINTECH shall perform the initial KYC/due diligence of the client, upload the KYC information with proper authentication, including the scanned images of the KYC documents, on the system of the KRA within 3 working days from the date of execution of documents by the client, and retain the physical KYC documents.
- If the client is already registered with the KRA, KFINTECH shall verify and download the client's details from the system of KRA.
- If the client informs KFINTECH of changes in his KYC details and status or when such information comes to the knowledge of KFINTECH, at any stage, KFINTECH shall be responsible for uploading the updated information on the system of KRA and retaining the physical documents.

ii. *Central KYC Registry (CKYCR)*

- KFINTECH shall maintain its registration with CKYCR for the purpose of KYC compliance.
- KFINTECH within ten days after the commencement of an account-based relationship with a client, file the electronic copy of the client's KYC records with CKYCR.
- In the event that a client already possesses and submits a KYC Identifier to KFINTECH, KFINTECH shall retrieve the KYC records online from the CKYCR by using the KYC Identifier.
- In the event that KFINTECH receives updated or additional information about the client, it shall as soon as possible furnish the updated information to CKYCR.

For a detailed understanding and process for the pointers **i & ii** mentioned above, please refer **ANNEXURE III – KYC Norms and Procedure** as attached with this policy

iii. *Financial Intelligence Unit – India (FIU-IND)*

- KFINTECH shall maintain its registration with FIU-IND for making critical reporting.
- Any changes in the name, designation and address of the "Designated Director" or the "Principal Officer" shall be communicated to FIU-IND.
- KFINTECH shall have suitable processes in place for detecting transactions and for furnishing information about such transactions as specified by FIU-IND/IFSCA and SEBI.
- The Principal Officer will be responsible for the timely submission of the reports to FIU-IND and shall ensure that confidentiality is maintained at the time of submission.
- KFINTECH shall not put any restrictions on the activity where an STR has been made. Any suspicious transaction shall be immediately notified to the Principal Officer. It shall be ensured that there is no tipping off to the client at any level. 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.
- No nil reporting needs to be made to FIU-IND in case there are no cash/suspicious/non-profit organization transactions to be reported.

iv. *Nodal Officer for the UAPA*

- KFINTECH shall also report full details of accounts bearing resemblance with any of the individuals/entities in the UN Sanctions Lists lists and the MHA list immediately to the Central designated Nodal Officer for the UAPA at Fax No. 011-23092551 and also convey over telephone no. 011-23092548 as well as by email to jsctcr-mha@gov.in.

  A copy of the communication mentioned above to the UAPA Nodal Officer shall also be sent to UAPA Nodal Officer of the State/UT where the account is held and to SEBI through post and through email (sebi_uapa@sebi.gov.in) to the UAPA nodal officer of SEBI, Deputy General Manager, Division of FATF, Market Intermediaries Regulation and Supervision Department, Securities and Exchange Board of India,

SEBI Bhavan II, Plot No. C7, "G" Block, Bandra Kurla Complex, Bandra (E), Mumbai 400 051. The consolidated list of UAPA Nodal Officers is available at the website of Government of India, MHA.

v. Governance Structure

- In order to strengthen the compliance structure and enhance the awareness amongst the employees, professionals and other designated persons dealing with Anti-Money laundering procedures, the National Institute of Securities Markets (NISM) has developed "Certification Course on Anti-Money Laundering and Counter-Terrorist Financing in the IFSC" in collaboration with IFSCA.
- All Designated Directors and Principal Officers, as defined under these guidelines, shall mandatorily complete the aforementioned NISM certification[g]. They shall also be required to maintain a valid certification at all times while performing their duties and responsibilities under the Guidelines.

XVI. REVIEW OF POLICY

This policy shall be reviewed annually and modified/altered to accommodate within its purview any notifications/circulars/notices issued by SEBI/PFRDA/IFSCA/FIU/PMLA Amendments/FATF recommendations and any competent authority with respect to money-laundering activities from time to time. Any modifications or amendments made in the policy shall be communicated by KFINTECH to the employees on an immediate basis.

The Principal Officer shall be given the authority to make changes to the policy as directed by relevant Regulatory/Statutory bodies.

XVII. CODE OF CONDUCT AND ETHICAL STANDARDS

All employees shall adhere to highest standards of integrity and professionalism while performing their duties related to AML/CFT compliance. All employees involved in such activities shall:

- Maintain strict confidentiality of customer information, KYC data and internal AML records.
- Avoid any actual or potential conflicts of interest and disclose such situations immediately.
- Report to the Principal Officer without delay any suspected violations of the AML policy, data misuse, etc.
- Adhere at all times to applicable AML/CFT laws, regulatory requirements, data protection standards and internal procedures

[g] *The course is prescribed in the circular IFSCA-DAC/8/2024-AMLCFT dated November 17,2025*

XVIII. ENFORCEMENT

Any non-compliance with the AML policy or applicable laws may result in appropriate enforcement actions, including disciplinary measures against employees, regulatory penalties and suspension or blacklisting of intermediaries, service providers or partners involved in violation.

XIX. ANNEXURES

ANNEXURE I

RISK ASSESSMENT AND FRAMEWORK

(This process is in reference to point VII of AML Policy)

This Annexure outlines the methodology and guiding principles for assessing and managing risks associated with Anti-Money Laundering / Combating the Financing of Terrorism / Know Your Customer (AML/CFT/KYC) and comply with all statutory and regulatory requirements, primarily the Prevention of Money Laundering Act, 2002 (PMLA) and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 (PML Rules). This Annexure applies to all employees, branches, and majority-owned subsidiaries of KFin Technologies Limited.

Risk assessment

- KFINTECH shall carry out risk assessments as provided in sub rule (13) of Rule 9 of PML Rules, annually or upon any material changes in business operations to identify, assess and take effective measures.
- The risk assessment shall also consider any overall sector specific or country specific information that is circulated by the Government of India, SEBI, PFRDA and IFSCA 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 the UNSC website).
- The internal risk assessment carried out by KFINTECH shall be commensurate to their size, geographical presence, complexity or activities/ structure etc.
- The assessment shall be documented, updated regularly and made available to competent authorities and self-regulating bodies, as and when required.
- KFINTECH shall take effective measures to mitigate its ML and TF risk for subscribers or specific geographic areas, products, services, nature and volume of transactions or delivery channels etc.
- KFINTECH shall identify and assess the Money-laundering/Terror Financing ("**ML/TF**") risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and existing products. KFINTECH shall ensure:
    i. To undertake the ML/TF risk assessments prior to the launch or use of such products, practices, services, technologies; and
    ii. Adoption of a risk-based approach to manage and mitigate the risks.

Analysis of Risk:

- KFINTECH shall include the consolidated assessment of the ML/TF risk perception that exists across all its business units, product lines and delivery channels.

- The outcomes of risk assessment shall be properly documented and shall include the Enterprise-Wide Risk Assessment (EWRA), details of implementation and controls. KFINTECH must outline a larger ML/FT risk management and compliance framework post assessing such risks.
- KFINTECH shall review and update the EWRA at least once every two (2) years or upon a significant change in risk parameters or business operations, whichever is earlier.

***AML/CFT systems and controls*:**

- The nature and extent of KYC/AML/CFT systems and controls implemented by KFINTECH shall be commensurate with the ML/TF risks identified via the enterprise-wide ML/TF risk assessment, wherever applicable.
- The information obtained from the risk assessment shall be used to:
    i. establish and maintain effective policies, procedures, systems and controls to prevent ML/TF.
    ii. ensure that KYC/AML/CFT policies, procedures, systems and controls adequately mitigate the risks identified and shall include a provision enabling the senior management to regularly review the information on operations and effectiveness of its AML systems and controls
- The systems and controls shall enable KFINTECH to determine whether a customer or a Beneficial Owner is a Politically Exposed Person (PEP).

S***ituations Where Relationship Must Not Be Established:***

- KFINTECH shall not establish the business relationship with the customer, which is a legal person or legal arrangement, in the following cases: -
    i. where the ownership or control arrangements of the customer prevent KFINTECH from identifying one or more of the customer's Beneficial Owners;
    ii. where there are anonymous accounts, accounts in fictitious names, or a nominee account which is held in the name of one person, but is controlled by or held for the benefit of another person whose identity has not been disclosed to KFINTECH; or
    iii. a Shell Financial Institution.

ANNEXURE II

CLIENT IDENTIFICATION AND DUE DILIGENCE

(This process is in reference to point VIII of AML Policy)

I. CLIENT ACCEPTANCE

KFINTECH shall develop client acceptance policy and procedure that shall aim at **identifying the type of clients that pose a higher risk**. KFINTECH shall follow the following safeguards while accepting the clients:

i. No accounts shall be opened in anonymous account or account in fictitious names or accounts whose identity cannot be disclosed or verified.
ii. The clients shall be classified into low, medium and high-risk categories based on the parameters such as location, business activity, trading turnover, etc
iii. Clients of special category (CSC) must undergo Enhanced Due Diligence (EDD). CSCs shall include the following:
    a. Non - resident clients;
    b. High net-worth clients;
    c. Trust, Charities, Non-Governmental Organizations (NGOs) and organizations receiving donations;
    d. Companies having close family shareholdings or beneficial ownership;
    e. Politically Exposed Persons (PEPs)
    f. Clients in high-risk countries- KFINTECH to access and consider publicly available information apart from being guided by FATF guidelines.
    g. Non-face to face clients
    h. Clients with dubious reputation as per public information available etc.

The above-mentioned list is only illustrative, KFINTECH shall exercise independent judgment to ascertain whether any other set of clients shall be classified as CSC or not.

iv. KFINTECH to collect documents and required information based on the risks perceived for clients having regard to the requirements of Rule 9 of the PML Rules, Directives and Circulars issued by the regulators from time to time.
v. KFINTECH shall not open an account where Client Due Diligence (CDD) measures cannot be applied.
vi. Where KFINTECH suspects that the information provided is non-genuine or there is perceived non - co-operation of the client in providing full and complete information, it shall discontinue the business activities with such clients and shall file a suspicious activity report.
vii. In case of suspicious trading, KFINTECH shall evaluate freezing or closure of such accounts and ensure that it shall not return securities or money forming a part of such suspicious trading.
viii. KFINTECH may clearly define conditions under which a client may act on behalf of another, including account operation, transaction limits, required authorizations, rights and responsibilities of both parties, and ensure adequate verification of the person's authority.
ix. Necessary checks and balances to be carried out by KFINTECH to ensure that the identity of the client does not match with any person having known criminal background or is not

banned in any other manner whether in terms of criminal or civil proceedings by any enforcement agency worldwide.

II. CLIENT IDENTIFICATION PROCEDURE (CIP)

KFINTECH shall carry out client identification procedure at different stages such as while establishing the intermediary – client relationship, while carrying out transactions for the client or when KFINTECH has doubts regarding the veracity or the adequacy of previously obtained client identification data.

KFINTECH shall comply with the following requirements while undertaking CIP:

i. To put in place appropriate risk management systems for determining whether the client/potential client/beneficial owner is a PEP.
ii. Obtain senior management approval prior to establishing business relationships with PEPs and also where such client subsequently is found to be or becomes a PEP.
iii. Take reasonable measures to verify the sources of funds as well as the wealth of clients and beneficial owners identified as PEP.
iv. It is the responsibility of KFINTECH to verify the legal form, proof of existence, constitution and powers that regulate and bind the customer, using reliable and independent source data.
v. Document verification should mainly rely on government issued identity cards or valid passport, reports from independent company registries, published or audited annual reports and other reliable sources of information.
vi. Risk profiling of customers is mandatory, and the rigor of the verification process should commensurate the same.
vii. Obtain adequate information including additional information on the customer's background such as occupation, employer's name, nature of business, range of annual income and shall also confirm whether the customer holds any prominent public position to satisfactorily establish the identity of each new client and the purpose of the intended nature of the relationship.
viii. Conduct ongoing due diligence where it notices inconsistencies in the information provided by following the requirements enshrined in rules and regulations, directives and circulars.
ix. Where a failure by the client to provide satisfactory evidence is noted by KFINTECH, it shall report the same to the higher authority.
x. Except for high-risk customers, the following mode of verifications are also considered as sufficient to satisfy the requirements of client verification:
    a. downloading publicly available information from an official source (such as a regulators or other official government website);
    b. CDD information and research obtained from a reputable company or information obtained from reliable and independent public information found on the internet and commercial databases, provided that the commercial database is recognized for such purpose by the home regulator, if any, of the database.
xi. Independently verify the identity of a high-risk customer using both public and non-public sources.

xii. Formulate and implement a CIP which shall incorporate the requirements of the PML Rules Notification No. 9/2005 dated July 01, 2005.

Note: No minimum investment threshold/category-wise exemption available for carrying out the CDD measures, non-compliance of which shall attract appropriate sanctions.

VIDEO BASED CUSTOMER IDENTIFICATION PROCESS (VCIP):

As a consent based alternate method of establishing the subscriber's identity using an equivalent e-document of any officially valid document, KFINTECH shall verify the digital signature as per the provisions of the Information Technology Act, and any rules issues thereunder.

The following are the modes in VCIP:

i. **Assisted VCIP with Human Officer[h] Review:**
A KFINTECH official shall conduct a live video call with the subscriber to verify their identity. The official shall guide the subscriber through the process, ensuring real-time interaction and document verification.

ii. **Unassisted VCIP (Self-Service Video KYC):**
The subscriber may complete the KYC process independently via a secure video-based platform or app, without direct human interaction, using automated systems for verification.

iii. **Hybrid VCIP (Combination of Assisted and Automated Verification):**
KFINTECH may undertake combined VCIP, where automated systems would handle initial verification of the subscribers, and a human officer duly appointed by KFINTECH shall intervene for final review or complex cases.

KFINTECH shall also extend the facility of online / digital / VCIP to persons with disability by adopting accessibility standards.

On request of the subscriber, KFINTECH shall extend their assistance for video capturing in live environment to facilitate online /Video for persons with disability.

For the purpose of 'liveliness' check, KFINTECH may use various parameters which not only involves checking the movement of eyelid and eyeball or blinking, but also may use other factors viz live facial expressions, nodding of head, subscriber showing OTP while being clearly visible on-screen, real-time video recording and displaying copies of documents on the screen etc.

Where a subscriber is unable to perform OTP-based or expression-based checks, the KFINTECH shall provide alternative authentication methods, such as:

i. Document-based Officially Valid Document (OVD) verification with live photo capture.
ii. Use of CKYCR/UIDAI/DigiLocker records for identity confirmation.

The liveliness check shall not result in exclusion of person with special needs and at the same time the accessibility options shall not dilute liveness/integrity checks under PML Rules.

[h] *Human officer is specifically required to be appointed by the KFINTECH entity regulated by PFRDA.*

Following are the minimum standards to be followed while undertaking V-CIP:

1. Undertaking of V-CIP

- V-CIP may be undertaken for:
    i. Customer Due Diligence for new individual customers;
    ii. Proprietor in case of proprietorship firms;
    iii. Authorised signatories and Beneficial Owners in case of non-natural persons;
    iv. Updation/periodic updation of KYC for eligible customers.

2. V-CIP Infrastructure Requirements

- Ensure compliance with prescribed cyber security and IT risk management frameworks.
- Ensure V-CIP technology infrastructure is hosted within KFINTECH's own premises or its Financial Group supervised by a financial regulator or a KYC Registration Agency (KRA) and the connections and interactions for undertaking V-CIP originates from its secured network domain.
- Ensure any technology outsourcing, if undertaken, complies with applicable regulatory standards.
- Ensure end-to-end encryption between customer device and V-CIP hosting environment.
- Record customer consent in an auditable and tamper-proof manner.
- Prevent V-CIP access from IP addresses outside India or from spoofed IP addresses.
- Ensure video recordings include:
    i. Live GPS coordinates (geo-tagging);
    ii. Date and time stamp;
    iii. Video quality sufficient to establish customer identity beyond doubt.
- Deploy face liveness detection, spoof detection and face matching technologies with high accuracy.
- Appropriate artificial intelligence (AI) technology with randomness and anti-deep fake and anti-fraud checks must be used to ensure that the V-CIP is robust.
- Regularly upgrade technology and workflows based on detected or attempted forged identity cases.
- Report any detected forged identity through V-CIP as a cyber event under applicable regulatory guidelines.
- Conduct periodic:
    i. Vulnerability Assessment;
    ii. Penetration Testing;
    iii. Security Audit;
    iv. Functional, performance and API testing.
- For resident Indian customers, the IP address shall emanate from India and for Non-Resident Indian it shall emanate either from India or from any one of the following countries where he or she is resident:
    i. United States of America;
    ii. Japan;
    iii. South Korea;

iv. United Kingdom excluding British Overseas Territories;
v. Canada;
vi. UAE;
vii. Singapore;
viii. Australia.
ix. European Union excluding Croatia

Provided that the aforementioned jurisdictions shall not be identified by FATF as High-Risk Jurisdictions subject to a Call for Action or Jurisdictions under Increased Monitoring or by Central Government as high-risk jurisdiction for money laundering, terrorist financing or proliferation financing.

- Ensure all critical gaps identified during testing are mitigated prior to deployment or continuation.
- Such tests shall be conducted by the empaneled auditors of Indian Computer Emergency Response Team (CERT-In) or any such other suitably accredited agencies as may be specified.

3. V-CIP Operational Procedure

- Operate V-CIP only through officials of KFINTECH who are:
  i. Specifically trained for V-CIP; and
  ii. Capable of performing liveliness checks and detecting suspicious behaviour.
- Abort the V-CIP session and initiate a fresh session in case of any disruption.
- Vary the sequence and nature of questions to establish live, real-time interaction.
- Reject the onboarding or KYC process if any prompting or coaching of the customer is observed.
- Factor in:
  i. Whether the customer is new or existing;
  ii. Any earlier rejected cases;
  iii. Appearance of customer name in negative or alert lists.
- Record audio-video interaction and capture photograph of the customer during V-CIP.
- Obtain identification information using any one of the following:
  i. Offline Aadhaar verification;
  ii. CKYCR records using KYC Identifier;
  iii. Equivalent e-documents of OVDs, including documents obtained through DigiLocker.
  iv. Biometric based e-KYC authentication, including Aadhaar Face Authentication
  v. OTP[i] based Aadhaar e- KYC authentication.
- Redact or blackout Aadhaar number as per the KYC Policy.
- Ensure Aadhaar XML file or Secure QR Code is not older than three days from the V-CIP date.
- Ensure V-CIP video process is completed within three days of obtaining identification data through Aadhaar / CKYCR / e-documents.
- Capture and record current address separately where it differs from the OVD address.

i Inserted vide Circular dated February 26,2026 issued by IFSCA.

- Upon verification of the proof of identity of the NRI Customer, in cases where current address of NRI customer cannot be verified from reliable /issuing authority sources, KFINTECH shall open the account of the customer in the debit freeze / inactive mode; and shall communicate such customer the manner of activation of debit freeze / inactive account.
- Confirm economic and financial profile information directly from the customer during V-CIP.
- Capture a clear image of PAN card during V-CIP, except where e-PAN is provided.
- Verify PAN details from the issuing authority database, including through DigiLocker.
- Do not accept printed copies of equivalent e-documents or e-PAN for V-CIP.
- Ensure photograph and details in Aadhaar/OVD and PAN/e-PAN match with:
    i. The customer undertaking the V-CIP; and
    ii. The information provided by the customer.
- Make accounts opened through V-CIP operational only after concurrent audit verification.
- Ensure compliance with other applicable laws, including the Information Technology Act.

4. V-CIP Records and Data Management

- Store all V-CIP data and recordings only in systems located within India.
- Ensure recordings are stored securely with date and time stamp for easy retrieval.
- Maintain activity logs capturing:
    i. Details of the authorised official conducting V-CIP; and
    ii. System access credentials.
- Retain all V-CIP records in accordance with record retention requirements under the AML/KYC Policy.

Additional conditions or requirements for Onboarding Non-Resident Indian (NRI) Customers (classified as low-risk) through V-CIP:

i. The Regulated Entities may onboard customers, who are Non- Resident Indian ('NRI Customers'), through V-CIP to carry out:
    a. CDD in case of on-boarding of new customers such as individual, proprietor in case of proprietorship, authorised signatories and Beneficial Owners (BOs) in case of customers which are non-natural persons and other connected parties appointed to act on behalf of the customer;
    b. Updation/Periodic updation of KYC.

ii. While undertaking the V-CIP for onboarding the NRI customers, KFINTECH shall ensure that the IP address emanates from the jurisdiction specified in the current address proof submitted to it.

iii. KFINTECH shall also capture the bank account details, maintained by NRI Customer with any bank in the jurisdiction, for the purpose of verification of the current address.

iv. Upon verification of the proof of identity of the NRI Customer, in cases where current address of NRI customer cannot be verified from reliable /issuing authority sources KFINETCH shall open the account of the customer in the debit freeze/inactive mode; and shall communicate such customer the manner of activation of debit freeze/inactive account.

v. The said debit freeze/inactive account of the NRI Customer shall be made operational only upon the receipt and verification of first credit from the bank account provided by such customer as proof of current address at the time of V-CIP onboarding process.

Additional conditions or requirements for Onboarding Non-Resident Indian (NRI) and Overseas Citizen of India (OCI) Customers through V-CIP *(identity & document provisions consolidated from PFRDA amendment:*

i. For NRI/OCI digital onboarding, capture live photograph, digital copy of an OVD, and geo-coordinates electronically by an authorized official; physical presence in India is not required for such digital KYC.
ii. The GPS location captured must match the country declared in the Proof of Address; prevent connections from spoofed IP addresses and apply liveness, randomness, and anti-spoofing/anti-deepfake controls.
iii. While undertaking the V-CIP for onboarding NRI customers, ensure that the IP address emanates from the jurisdiction specified in the current address proof submitted.
iv. Capture the bank account details maintained by the NRI customer in the same jurisdiction for the purpose of verifying current address.
v. The subscriber is responsible for providing correct and authentic documents to establish NRI/OCI status. Forged, falsified or misleading submissions shall result in rejection and may be reported to the appropriate authorities as required under applicable PMLA provisions.
vi. All onboarding KYC modes (including V-CIP) are permitted for updation.
vii. Updation of KYC documents may be carried out at any overseas branch of KFINTECH with which the subscriber maintains the account, or through digital/electronic means, or by self-attested and duly attested copies (Passport, OCI Card, overseas address proof, etc.). Attestation may be by Indian Embassy/Consulate/Notary/Court Magistrate/Judge/authorised officials of overseas branches of Scheduled Commercial Banks registered in India and shall be deemed "Original Seen and Verified (OSV)" compliance under PML Rules.
viii. In no-change scenarios, a self-declaration from the NRI subscriber through registered email/mobile/letter (as prescribed) only for periodic updation—not at exit/withdrawal. During periodic updation, KFINTECH shall reconfirm FATCA/CRS declarations, tax residency and current residency status (NRI/OCI/Resident); verify the validity of Passport/Visa/Residence Permit/OCI Card and obtain updates where required.

III. CLIENT DUE DILIGENCE (CDD)

KFINTECH shall undertake CDD as per the provisions of Rule 9 of the PML Rules using reliable and independent sources of identification.

The CDD shall have regard to the money laundering and terrorist financing risks and the size of the business and shall include policies, controls and procedures, approved by the senior management, to enable, to manage and mitigate the risk that have been identified either by the registered intermediary or through national risk assessment.

KFINTECH shall undertake CDD as below:

1. **Knowing new subscriber-**
   i. At the time of commencement of account-based relationship in case of new subscribers including persons with disabilities, necessary CDD with valid KYC shall be done.
   ii. KFINTECH shall ensure the reporting requirements under Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS).
   iii. KFINTECH shall develop and implement a mechanism where subscribers who have already completed their KYC process with one regulated entity may authorize the sharing of their KYC information with other entities through the Central KYC Registry (CKYC).
   iv. KFINTECH shall ensure it refers to the following guidelines while dealing with persons with disabilities:
      a. Establishing account-based relationship under the name of persons with disabilities.
      b. In accordance with the provisions of the Mental Health Care Act, 2017 and the National Trust for the Welfare of Persons with Autism, Cerebral Palsy, Mental Retardation and Multiple Disabilities Act, 1999, where an individual requires a guardian, KFINTECH may rely upon the Guardianship Certificate issued by the Local Level Committee under the National Trust for the Welfare of Persons with Autism, Cerebral Palsy, Mental Retardation and Multiple Disabilities Act, 1999.
      c. Where the person is unable to sign for herself/himself, the account may be opened using their thumb impression or with the signature of the guardian.
      d. KFINTECH shall extend their facility of all forms of permitted KYC, including the assistance for video capturing in live environment.
      e. Establish a dedicated helpline offering step by step assistance in completing the KYC process through voice or video support.

2. **Knowing existing subscribers:**
   i. CDD and KYC must be conducted for existing subscribers periodically, guided by the adequacy and currency of previously obtained data and regulatory requirements under extant PML Rules.
   ii. Risk categorization shall be performed using defined parameters including subscriber identity verification, nature of employment, high-value deposits in Tier II accounts or in Tier I accounts near superannuation, unusual withdrawals in Tier II accounts, and the ability to confirm identity documents via online services or issuing authorities.
   iii. Enhanced Due Diligence (EDD)[j] shall be applied, with documented additional verification steps and escalation procedures. The detailed process for EDD is mentioned in section IV below.
   iv. For Low-risk subscribers whose identities and sources of income are readily verified and whose transactions align with their known profile; for such subscribers, basic requirements of identity verification, current address, annual income, and source of funds shall be met.

[j] *Only for PFRDA regulated entity EDD shall apply to Tier II accounts under NPS All Citizen / Corporate model.*

v. KFINTECH shall ensure that the KYC procedures for High-risk categories including non-residents, high-net-worth individuals, politically exposed persons (PEPs), and individuals with adverse public reputation; enhanced verification, counter-checks, and senior-level approval shall be required for onboarding and material changes.

vi. Accordingly, periodic updation[k] of KYC shall be done as follows:

Low-Risk-where periodic updation of KYC is done once in every ten years from the date of opening of the account / last KYC updati on	**Medium-Risk**-where periodic updation of KYC is done once in every Eight years from the date of opening of the account / last KYC updation	**High-Risk**-where periodic updation of KYC is done once in every two years from the date of opening of the account / last KYC updation
Salaried pensioners Employees or of Govt/PSUs/Listed Companies; Self-employed, including Individuals engaged in Agri, Allied and MSMEs; Minors/Student/Homemaker	Other Salaried Employees; Business person; Professionals; Non-Resident Individuals Others	Politically Exposed Persons (PEP) or Related to PEP; High-net worth individuals (HNI);

Note: Above list is indicative and not exhaustive. KFINTECH may consider additional factors using its own judgement and past experience.

IV. ENHANCED DUE DILIGENCE (EDD)

1. Identification of High-Risk Customers

- Customers classified as High Risk based on Customer Risk Assessment or other risk indicators shall be subjected to Enhanced Due Diligence as mandated under Section 12AA of the PML Act.
- KFINTECH shall examine unusual patterns of transactions that have no apparent economic or lawful purpose and apply enhanced due diligence where ML/TF risks are higher.
- The extent of EDD shall be determined on a case-to-case basis, proportionate to the identified ML/TF risk.

2. Collection of Additional Customer Information

- Obtain additional information on the customer and Beneficial Owner, including:
  - i. Occupation and nature of business
  - ii. Volume and nature of assets
  - iii. Ownership and control structure
- Review reliable public-domain information, including regulatory databases and internet-based sources.

k The provision for KYC updation is mentioned in Annexure- III Know Your Customer Norms and procedure.

- Update customer and Beneficial Owner identification information at an enhanced frequency.

3. Verification of Identity

- KFINTECH to verify the identity of the customer/subscriber preferably using the CKYC Identifier or Aadhaar, subject to customer consent.
- If CKYC or Aadhaar verification is not available, it shall verify the customer through any other KYC method prescribed under applicable regulatory guidelines.

4. Verification of Ownership, Source of Wealth and Source of Funds

- Examine and document the ownership and control structure of the customer.
- KFINTECH shall examine the ownership and financial position, including the customer's source of funds, commensurate with the assessed risk and profile.
- Identify and verify the source of wealth, explaining how overall wealth has been acquired, while also identifying and verifying the source of funds for the specific transaction or business relationship.
- Ensure that the source of funds is consistent with the customer's source of wealth and risk profile.

5. Assessment of Purpose and Intended Nature of Relationship

- Record the purpose of the transaction.
- Record and assess the intended nature of the business relationship between the transaction parties.
- Review consistency of the transaction purpose with the customer's profile and risk classification.
- Examine, as far as reasonably possible, any unusual, complex or non-economic transaction patterns.

6. First Payment Verification

- Ensure that the first payment is received only through a bank account held in the customer's own name with:
    i. A bank; or
    ii. A regulated financial institution complying with Fast Action Task Force (FATF) - equivalent AML/CFT standards; or
    iii. A regulated subsidiary thereof with assured group-wide AML/CFT compliance.

7. Senior Management Approval

- Obtain prior approval from Senior Management, or an authorised senior committee/member, before:
    i. Commencing a business relationship with a high-risk customer; or
    ii. Continuing an existing relationship where the risk level has escalated

8. Enhanced Ongoing Monitoring

- Apply enhanced monitoring measures including:
    i. Increased frequency of transaction reviews

ii. Increased depth of scrutiny over transactions
iii. Identification of unusual or complex patterns requiring investigation

- Review customer risk classification periodically and update EDD measures as required.
- KFINTECH shall examine transactions with no apparent economic or lawful purpose and apply EDD measures where risks are higher.

9. Review of Complex Structures

- Where customers use complex legal structures, trusts or private investment vehicles:
  i. Assess whether such structures serve a genuine and legitimate purpose
  ii. Identify and verify all relevant Beneficial Owners
  iii. Document the rationale for accepting or continuing the relationship

10. Source of Funds Documentation

- KFINTECH shall require customers to demonstrate and document the origin of funds, including the underlying activity that generated the funds.
- Acceptable evidence may include:
  i. Bank statements
  ii. Salary slips, bonus certificates or employment contracts
  iii. Dividend statements
  iv. Sale deeds or proof of sale proceeds
  v. Loan agreements or repayment schedules
  vi. Any other transaction specific supporting documents

11. Documentation and Record Maintenance

- Document all EDD measures, verification steps, approvals, findings and observations.
- Retain all records and supporting documents in line with the AML Policy and regulatory retention requirements.

V. ONGOING DUE DILIGENCE REQUIREMENTS

Ongoing Due Diligence (ODD) is an integral part of the risk-based AML/CFT framework and must be applied throughout the duration of the customer relationship.
Beyond verification of identity at the time of account opening or initial contribution, Reporting Entities shall conduct regular and event-based monitoring whenever additional or subsequent contributions, transactions or account activities occur.
Any activity that appears inconsistent with the customer's known profile, expected behaviour or declared financial standing shall trigger further due diligence, review and escalation, as appropriate.
Ongoing due diligence shall be carried out:

i. at the time of each additional or subsequent contribution, transaction or activity during the course of the relationship.

ii. Where any activity that deviates from the normal or expected pattern of the customer shall be scrutinised and, where necessary, subject to further due diligence.
iii. KFINTECH shall consider the following factors during ongoing due diligence:
    a. Source of contribution.
    b. Mode of contribution (e.g., cash, online transfer, cheque, demand draft, card payments, employer's bank account, etc.).
    c. Regularity and pattern of contributions, including expected flows under employer–employee arrangements.
    d. Withdrawals or redemptions under the respective account or product structure.
    e. Residence status of the customer, especially if residing in jurisdictions with higher national or international ML/TF risk assessments.
    f. Contributions made vis-à-vis the customer's declared income or income range, ensuring consistency with financial standing.
iv. Verification shall be carried out at the time of account exit (superannuation, premature exit, death or closure), ensuring:
    a. No payments are made to third parties except duly verified nominee(s) or legal heir(s) in the event of death.
    b. Appropriate due diligence on the customer, nominee(s) or legal heir(s) is completed before settlement of claims or pay-outs.
v. Where suspicion of money laundering or terrorist financing exists and there is a reasonable belief that carrying out the Client Due Diligence (CDD) process may lead to tipping-off, the Reporting Entity shall not proceed with CDD and shall file a Suspicious Transaction Report (STR) with FIU-IND.
vi. KFINTECH shall ensure that no vulnerable cases go undetected. In situations indicating suspicion of ML/TF or the presence of high-risk factors, an STR shall be filed with FIU-IND, and Enhanced Due Diligence (EDD) shall be applied, consistent with the risks identified.

ANNEXURE III

KNOW YOUR CUSTOMER (KYC) NORMS AND PROCEDURE

(This process is in reference to point VIII of AML Policy)

KFINTECH shall make best efforts to determine the true identity of subscriber(s). It shall follow the guidelines issued by regulators in this regard as mentioned below and obtain and verify the Proof of Identity (PoI) and Proof of Address (PoA) from the client at the time of commencement of an account-based relationship.

1. ***Uniform KYC Format:***
   - KFINTECH shall perform KYC in securities market through physical mode/ digital (online or app based) mode.
   - In order to bring uniformity in the securities market, KFINTECH shall use the same KYC form and supporting documents.
   - KFINTECH shall refer to the circular issued by SEBI SEBI/HO/AFD-2/CIR/P/2022/175 dated December 19, 2022 and further amendments thereto for undertaking the KYC of the Foreign Portfolio Investors and Eligible Foreign Investors.
   - KFINTECH shall use the templates as provided by Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI) for individuals and for legal entities for capturing the KYC information.

2. ***Requirement of Permanent Account Number (PAN):***
   - KFINTECH shall verify the PAN of their clients online at the Income Tax website without insisting on the original or copy of PAN card.
   - KFINTECH shall ensure that the PAN allotted to a person is linked with his/her Aadhaar, failing which the PAN shall be rendered inoperative.
   - KFINTECH shall flag the status of Aadhaar and PAN linkage at the system of KRA
   - The requirement of PAN shall be exempted by KFINTECH in the following cases:
     i. Transactions undertaken on behalf of Central Government and/or State Government and by officials appointed by Courts
     ii. Investors residing in the state of Sikkim.
     iii. UN entities/multilateral agencies exempt from paying taxes/filing tax returns in India.
     iv. Systematic Investment Plan of Mutual Funds upto ₹50,000/- per year.

3. ***Proof of Identity (PoI):***
   - KFINTECH at the time of commencement of an account-based relationship shall identify the clients, verify their identity and obtain information on the purpose and intended nature of the business relationship.
   - KFINTECH shall ensure that the name mentioned on the KYC form matches the name on the PoI as submitted
   - where KFINTECH applies simplified measures for verifying the identity of the clients, the following documents shall also be deemed to be officially valid document:

i. Identity card/ document with applicant's photo, issued by the Central/State Government Departments, Statutory/Regulatory Authorities, Public Sector Undertakings, Scheduled Commercial Banks and Public Financial Institutions;
ii. Letter issued by a gazetted officer, with a duly attested photograph of the person.

- KFINTECH shall not store/ save the Aadhaar number of clients in their system.
- Further, where the client submits his Aadhaar number, KFINTECH shall ensure that Aadhaar number is redacted or blacked out by appropriate means where the authentication of Aadhaar number is not required under the sub rule (15) of Prevention of Money Laundering (PML) Rule 9.

4. Proof of Address (PoA):

- At the time of commencement of an account-based relationship, KFINTECH shall along with the PoI, obtain documents as proof of address. The following documents shall be accepted as PoA:
  a. "Officially valid document" (OVD) defined as per Rule 2 (d) of Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 (PML Rules):
     i. the passport;
     ii. the driving licence;
     iii. proof of possession of Aadhaar number;
     iv. the Voter's Identity Card issued by Election Commission of India;
     v. job card issued by National Rural Employment Guarantee Act (NREGA) duly signed by an officer of the State Government;
     vi. the letter issued by the National Population Register containing details of name, address; or
     vii. any other document as notified by the Central Government in consultation with the Regulator.
  b. Further, in terms of Rule 9 (18) of PML rules, 2005, in case the OVD furnished by the client does not contain updated address, the following documents (or their equivalent e-documents thereof) shall be as deemed to be OVD for the limited purpose of proof of address, provided that the client shall submit updated OVD (or their equivalent e-documents thereof) with current address within a period of three months of submitting the following documents:
     i. utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
     ii. property or municipal tax receipt;
     iii. pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
     iv. letter of allotment of accommodation from employer issued by state or central government departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and licence agreements with such employers allotting official accommodation.

I. MODES OF KYC:

KFINTECH may perform KYC process for all subscribers including Persons with Disabilities by any of the following methods:

1. **Using unique CKYC identifier**:
   KFINTECH may perform the KYC process preferably by using the unique CKYC identifier in both physical and digital modes with an explicit consent to download records from CKYCR, in order to avoid collection of KYC documents repeatedly.
2. **Physical / Face-to-Face Verification:**
   KYC process may be performed by obtaining CKYC identifier and in case, if the same is not available, KFINTECH through its authorized officer may perform the KYC process by verifying original OVDs and maintaining a copy of the same as 'original seen and verified.
3. **Aadhaar based KYC:**
   Subject to notification by the Government under section 11A of PML Act:
   iii. OTP based e-KYC authentication or Biometric e-KYC (fingerprint/IRIS/face) authentication; (including use of e-KYC Setu System)
   iv. Aadhaar offline XML/Aadhaar QR code.
4. **Digital KYC:**
   To ensure secure, compliant, and fully digitized onboarding and establishment of account-based relationship, KFINTECH shall**:**
   i. Facilitate completion of KYC requirements through digital means, including online/app-based KYC, video in-person verification, Aadhaar e-KYC, offline Aadhaar verification, digital submission of OVDs, and authentication through electronic/digital signatures including Aadhaar e-Sign.
   - Obtain explicit consent from the customer prior to initiating the digital KYC process.
   - Capture and verify customer details digitally, including PAN, photograph, name, address, mobile number, email ID, and bank account information.
   - Authenticate digitally submitted documents using electronic/digital signatures, including Aadhaar e-Sign, and accept Aadhaar-seeded mobile numbers for KYC purposes.
   - Verify mobile number and email address using OTP or other verifiable authentication mechanisms.
   - Verify bank account details through Penny Drop verification or other secure bank API-based mechanisms.
   - Accept electronic/digital signatures, including Aadhaar e-Sign, in lieu of wet signatures on all KYC documents, including signatures digitally affixed on online KYC forms.
   - Ensure that Aadhaar XML files or Secure QR Codes used for offline Aadhaar verification are not older than three days from the date of performing KYC.
   - Accept any document (other than those excluded under the First Schedule of the Information Technology Act, 2000) authenticated through electronic/digital signature including Aadhaar e-Sign to complete the KYC process digitally.

- Exercise due diligence for non-individual clients to confirm the genuineness of authorisations, identity of authorised signatories, and authenticity of documents submitted through digital channels.
- Obtain Aadhaar number where voluntarily provided, or proof of possession of Aadhaar (with or without offline verification capability), or any OVD/e-document containing identity and address details from Indian nationals undergoing CDD.
- Obtain PAN or equivalent e-document as defined under the Income-tax Rules, 1962, and any additional documents required to assess the nature of business, financial profile, or other due-diligence requirements.
- Conduct Aadhaar e-KYC authentication when Aadhaar number is voluntarily submitted, and accept a self-declaration of current address if it differs from the Aadhaar database.
- Carry out offline Aadhaar verification when proof of possession of Aadhaar is submitted and offline verification is feasible.
- Verify digital signatures on e-documents submitted as OVDs and capture a live photograph as required under Digital KYC guidelines.
- Undertake Digital KYC as per Annexure I of the KYC Rules when offline verification cannot be performed on OVDs or Aadhaar documents.
- For the period permitted by the Government for relevant classes of Regulated Entities, obtain a certified copy of Aadhaar proof or OVD and a recent photograph when an equivalent e-document is not submitted, instead of performing Digital KYC.
- Ensure that all digital KYC activities comply with applicable laws, the Aadhaar Act, UIDAI guidelines, KYC Rules, and the Information Technology Act, 2000, maintaining the authenticity, integrity, confidentiality, and security of customer information.

II. **IN- PERSON VERIFICATION (IPV):**

- KFINTECH shall mandatorily carry out In-Person Verification (IPV) of their clients as part of the KYC process, and shall ensure that the name, designation, organisation, signature of the person conducting the IPV and the date of IPV are duly recorded on the KYC form.
- Where mutual fund applications are received directly from clients (i.e., not routed through a distributor), reliance may also be placed on IPV conducted by scheduled commercial banks.
- To enable ease of completing IPV of an investor KFINTECH may undertake the Video in Person Verification (VIPV) of an individual investor through their App. The following process shall be adopted in this regard:
    i. KFINTECH through their authorised official, specifically trained for this purpose, may undertake live VIPV of an individual client, after obtaining his/her informed consent. The activity log along with the credentials of the person performing the VIPV shall be stored for easy retrieval.
    ii. The VIPV shall be in a live environment.
    iii. The VIPV shall be clear and still, the client in the video shall be easily recognisable and shall not be covering their face in any manner.

iv. The VIPV process shall include random question and response from the investor including displaying the officially valid document, KYC form and signature or could also be confirmed by an OTP.
v. KFINTECH shall ensure that photograph of the client downloaded through the Aadhaar authentication / verification process matches with the investor in the VIPV.
vi. The VIPV shall be digitally saved in a safe, secure and tamper-proof, easily retrievable manner and shall bear date and time stamping.
vii. KFINTECH may have additional safety and security features other than as prescribed above.

- However, IPV shall not be required in the cases where:
  i. the KYC of the client has been completed using the Aadhaar authentication/ verification of UIDAI.
  ii. the KYC form has been submitted online; documents have been provided through Digilocker or any other source which could be verified online.

Provisions for KYC updation:

1. Fresh KYC shall be conducted for every subscriber/customer at the time of withdrawal, exit, or closure of the account under any applicable model or scheme, irrespective of whether earlier KYC is updated.
2. All KYC modes permitted for onboarding new subscribers/customers shall also be applicable for KYC updation or re-KYC.
3. For periodic KYC updation where there is no change in the customer's KYC details, a self-declaration may be obtained through the registered email ID, registered mobile number, letter, or other approved channels. This shall not be permitted at the time of exit or withdrawal.
4. Wherein, only the address has been changed, the CKYC Identifier shall preferably be used to update the address; if not available or not updated, a valid OVD reflecting the new address shall be obtained within timelines specified under applicable PML rules.
5. Periodic KYC updation or re-KYC may be carried out through Video-based KYC (V-CIP), including for persons with disabilities, using acceptable liveliness checks such as head nodding, facial expressions, movement of eyes, OTP display, real-time video, or document display, ensuring no exclusion of persons with special needs.
6. During re-KYC triggered by periodic updation or change in risk category, the CKYC Identifier shall be used to update the latest photograph and signature; if unavailable, these may be collected through physical or digital means.
7. For low-risk accounts, all transactions shall be permitted while ensuring KYC updation within one year of becoming due; regular monitoring shall be conducted, and failure to update KYC within timelines shall result in freezing of service requests such as investment pattern changes, fund changes, partial withdrawals, or exit-related services.
8. For medium-risk accounts, all transactions shall be permitted while ensuring KYC updation within six months of becoming due; accounts shall be regularly monitored, and failure to update KYC shall result in freezing of investment pattern changes, fund changes, partial withdrawals, or exit-related services.
9. For high-risk accounts, failure to complete KYC within the prescribed timelines shall lead to immediate freezing of investment pattern changes, fund changes, partial withdrawals, or exit-related services.

10. The risk category (Low / Medium / High) shall be updated accurately in the system for each account and maintained based on periodic review.
11. The system shall record the date of last KYC and the due date for the next re-KYC, and re-KYC shall be initiated and completed before it becomes due.
12. Periodic reports indicating accounts due for KYC updation or accounts with revised risk categories shall be reviewed, and the KYC of such accounts shall be updated within prescribed timelines.
13. Timely communication shall be sent to subscribers/customers regarding due KYC updation through SMS, email, or letters, based on the risk based approach.
14. When a subscriber/customer shifts from one sector (e.g., Government to Private) or category to another, fresh KYC shall be conducted through any permitted KYC mode.
15. When a subscriber/customer shifts between different Reporting Entities (REs) within or outside the group, the new RE shall preferably complete KYC using the CKYC Identifier; if unavailable, any other permitted KYC method may be used.

III. SHARING AND UPDATING KYC INFORMATION WITH CENTRAL KYC RECORDS REGISTRY (CKYCR):

To ensure uniformity, regulatory compliance, and efficient management of KYC information across the Group, all requirements under the Prevention of Money-laundering (Maintenance of Records) Rules, 2005, the PFRDA guidelines, SEBI guidelines and other applicable regulatory instructions shall be strictly adhered to for the purpose of maintaining complete, accurate, and up-to-date KYC information of clients and subscribers.

KFINTECH shall comply with all obligations relating to the sharing, retrieval, updating, and utilisation of KYC records with the Central KYC Records Registry (CKYCR), operated by the Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI).

- KFINTECH shall perform all CKYCR related functions, including filing, retrieval, updating, and utilisation of KYC records, in the manner prescribed under the PML Rules.
- KFINTECH shall register[l] themselves with CERSAI; where KFINTECH is already registered under another financial-sector regulator it may use the existing registration.
- For verification of identity or ongoing due diligence, KFINTECH shall seek the KYC Identifier from the subscriber, or retrieve it with the subscriber's consent, where available.
- Where a KYC Identifier exists, KFINTECH shall obtain KYC records online from CKYCR using the identifier and shall not require resubmission of KYC documents except where:
    i. there is a change in subscriber information recorded with CKYCR;
    ii. retrieved information is incomplete or not aligned with the applicable KYC norms;
    iii. the validity period of downloaded documents has expired;

l Applicable for entity regulated by PFRDA (Point of Presence) as specified under the master guidelines PFRDA/Master Circular/2024/04/PoP-02 updated as on September 25,2025.

iv. additional verification is necessary to confirm identity or address, perform enhanced due diligence, or assess risk profile.

- Where, an information regarding the demise of a customer is confirmed, KFINTECH may use the CKYCRR Update process to flag the customer's KYC record as 'Deceased' along with the date of demise, documentary evidence, and remarks, if any. These details may be captured under the "Other Details/Deceased Information" section available on the "Update KYC – Individual" screen.
- KFINTECH shall furnish updated subscriber information to CKYCR **within seven (7) days** or within such period as may be notified by Government, upon verification or during ongoing due diligence.
- CKYCR shall electronically notify KFINTECH that have dealt with the subscriber when updated KYC information is uploaded.
- Upon receiving CKYCR notifications of updated subscriber records, KFINTECH shall retrieve and update their internal KYC records accordingly.
- If a KYC Identifier is unavailable or not provided, KFINTECH shall capture and upload KYC details in accordance with PML Rules using the KYC template for individuals as specified by CERSAI.
- KFINTECH shall upload electronic KYC records to CKYCR **within ten (10) days** from commencement of any account-based relationship with a subscriber or client.
- Once a KYC Identifier is generated or allotted by CKYCR, KFINTECH shall immediately communicate it to the subscriber confidentially, highlighting its purpose and benefits.
- If Aadhaar is used for online authentication, KFINTECH shall upload the redacted Aadhaar number (last four digits), demographic details, and confirmation that authentication was performed.
- If Aadhaar is used for offline verification, KFINTECH shall upload KYC data along with the redacted Aadhaar number (last four digits).
- At the time of periodic updation, all existing KYC records must be incrementally uploaded to CKYCR in accordance with current Client Due Diligence standards.
- KFINTECH shall ensure updated KYC records of active pension accounts are uploaded where KYC Identifiers are yet to be generated.
- KFINTECH shall not use CKYCR retrieved KYC records for any purpose other than verifying identity or address, nor transfer such information to third parties unless authorised by the subscriber, SEBI, PFRDA, or the Director (FIUIND).
- KFINTECH shall ensure that KYC records for accounts opened prior to CKYCR becoming operational are updated during periodic KYC and migrated to current CDD standards.
- KFINTECH shall submit CKYCR-related MIS[m] reports as required.
- KFINTECH shall capture KYC[n] information in accordance with PML Rules and the CERSAI finalised KYC template for uploading to CKYCR.
- KFINTECH shall upload KYC records of all individual and legal entity clients when updated information is obtained.

[m] *Applicable for KFINTECH entity regulated by PFRDA only*
[n] *Applicable for KFINTECH entity regulated by SEBI only*

- The CKYCR User Manual for uploading KYC records (available on **https://www.ckycindia.in**) shall be followed for all technical and operational requirements.
- CERSAI's helpdesk shall be used for addressing operational difficulties in uploading or retrieving CKYCR information (Phone: 022-61102592 / 022-50623300; Email: **helpdesk@ckycindia.in**).
- KFINTECH shall ensure full compliance with PML Rules, PFRDA regulations, SEBI guidelines, and any instructions issued by regulators from time to time regarding CKYCR obligations.

IV. ADAPTATION OF AADHAAR BASED E-KYC PROCESS AND E-KYC AUTHENTICATION FACILITY FOR RESIDENT INVESTORS UNDER SECTION 11A OF THE PREVENTION OF MONEY LAUNDERING ACT, 2002: KYC USER AGENCY (KUA) AND SUB KYC USER AGENCY (SUB-KUA) MECHANISM[o]

To enable seamless digital onboarding and strengthen identity verification standards for resident investors, KFINTECH shall adopt Aadhaar-based e-KYC and Aadhaar Authentication in line with Section 11A of the Prevention of Money Laundering Act, 2002 and the framework prescribed by the Central Government and Unique Identification Authority of India (UIDAI). These requirements shall support secure client authentication and allow utilisation of the KUA and Sub-KUA mechanism for conducting e-KYC in an efficient and compliant manner.

- KFINTECH shall treat the Aadhaar-based e-KYC service provided by UIDAI as a valid and approved method for completing customer KYC verification.
- KFINTECH shall utilise Aadhaar Authentication for KYC purposes only in accordance with Section 11A of the PMLA and the process notified by the Department of Revenue, Ministry of Finance.
- KFINTECH shall, where applicable, operate under the KUA/Sub-KUA framework and shall ensure adherence to UIDAI-prescribed standards for Aadhaar Authentication.
- KFINTECH shall rely on authorised KUAs for Aadhaar Authentication and shall onboard itself as a Sub-KUA by entering into the required agreement with the selected KUA and completing UIDAI registration formalities.
- KFINTECH shall coordinate with the designated KUAs to enable Aadhaar Authentication services for its clients —namely:
    i. Bombay Stock Exchange Limited
    ii. National Securities Depository Limited
    iii. Central Depository Services (India) Limited
    iv. CDSL Ventures Limited
    v. NSDL Database Management Limited
    vi. NSE Data and Analytics Limited
    vii. CAMS Investor Services Private Limited
    viii. Computer Age Management Services Private Limited

---

[o] For KFINTECH entity regulated by SEBI as specified under the master circular SEBI/HO/MIRSD/SECFATF/P/CIR /2023 /169 dated October, 12 2023.

ix. National Stock Exchange of India Limited

- KFINTECH shall comply with Gazette Notifications S.O. 3187(E) dated July 13, 2022 and S.O. 446(E) dated January 30, 2023, which permit specific reporting entities to use Aadhaar Authentication as Sub-KUAs, and shall ensure its operational processes align with these regulatory permissions.
- KFINTECH shall rely on KUAs to facilitate its onboarding as a Sub-KUA and ensure uninterrupted access to the Aadhaar Authentication service for KYC completion.

A. ONBOARDING PROCESS OF SUB-KUA BY UIDAI

To ensure compliant implementation of Aadhaar-based e-KYC Authentication for resident investors, KFINTECH shall follow the guidelines prescribed under Section 11A of the Prevention of Money Laundering Act, 2002, and the processes issued by UIDAI, the Department of Revenue (DoR), Ministry of Finance, SEBI, and other applicable authorities. These requirements govern the onboarding of Sub-KUAs, execution of Aadhaar Authentication, operational processes, data-handling safeguards, and ongoing compliance obligations. KFINTECH shall follow the guidelines outlined below.

KFINTECH shall:

- Follow the DoR circular-prescribed process whereby SEBI scrutinises KUA applications and forwards them, along with recommendations, to UIDAI.
- Adhere to the onboarding framework in which the KUA submits the list of proposed Sub-KUAs to SEBI, and SEBI forwards recommended Sub-KUAs to UIDAI for approval.
- Execute the UIDAI-prescribed agreement between KUA and Sub-KUA and comply with all obligations under the Aadhaar Act, 2016, and relevant regulations, circulars, and guidelines.
- Use the unique Sub-KUA code allotted by UIDAI for all Aadhaar Authentication activities.
- Be guided by the prescribed KUA/Sub-KUA processes while using UIDAI Aadhaar Authentication services for e-KYC.

1. Aadhaar e-KYC Process for Resident Investors:

A. Online Portal-Based Investor (Resident) e-KYC Process

KFINTECH shall:

- Provide an online platform through which clients may initiate account opening or investment processes as a Sub-KUA.
- Redirect clients to the KUA portal for Aadhaar Authentication and ensure that Aadhaar numbers are never stored by KFINTECH or the KUA.
- Ensure that the client receives an OTP on their Aadhaar-registered mobile number and enters it on the KUA portal.
- Receive e-KYC details from the KUA in encrypted form and display them securely to the client.
- Clearly disclose the names of the KUA and Sub-KUA and the nature of e-KYC data sharing at the time of obtaining client consent.

- Capture any additional information required under KYC norms after Aadhaar authentication.

B. Assisted Investor (Resident) E-Kyc Process

Kfintech Shall**:**

- Allow clients to complete Aadhaar-based e-KYC through authorised KFINTECH locations functioning as Sub-KUAs.
- Use only registered/whitelisted devices linked to the KUA for biometric Aadhaar authentication.
- Ensure that the client enters Aadhaar number/Virtual ID (VID) and provides consent on the registered device.
- Capture the client's biometric for authentication through UIDAI, via the KUA.
- Retrieve and display the e-KYC details received from UIDAI and collect any additional mandatory information.

2. Requirements While Performing Aadhaar Authentication:

KFINTECH shall:

- Ensure the KUA obtains special permission from UIDAI before sharing e-KYC data with KFINTECH as a Sub-KUA under Regulation 16 (2) of the Aadhaar (Authentication) Regulations, 2016.
- Ensure the KUA does not share UIDAI-signed e-KYC data with other KUAs and only shares digitally signed data using KUA's own signature for system processing.
- Store e-KYC data strictly in compliance with the Aadhaar Act, Aadhaar Regulations, and UIDAI circulars.
- Never store full Aadhaar numbers under any circumstances and rely solely on UIDAI-approved Aadhaar Number Capture Services (ANCS).
- Maintain auditable logs of all transactions where e-KYC data is shared by the KUA for periods mandated by UIDAI.
- Display only the last four digits of the Aadhaar number on systems where disclosure is required.
- Implement exception-handling mechanisms and backup authentication methods to ensure uninterrupted service.
- Undergo UIDAI audits and ensure full compliance with audit requirements.
- Establish monitoring mechanisms to detect and report irregular Aadhaar authentication transactions to UIDAI.
- Ensure investor grievances relating to e-KYC are resolved within UIDAI-prescribed timelines and reported accordingly.

3. Regulatory Oversight & Compliance Obligations

KFINTECH shall:

- Recognise that SEBI may take action for any non-compliance and may escalate matters to DoR, FIU-IND, or UIDAI where necessary.
- Adhere to all continuing compliance, privacy, security, and data-protection standards required by UIDAI for KUAs/Sub-KUAs.

- Be aware that the Central Government may withdraw authorisation for Aadhaar authentication if KFINTECH fails to meet statutory requirements, after providing an opportunity to be heard.

4. KYC Requirements for SARAL Account Opening (Resident Individuals)

KFINTECH shall:

- Accept a single proof of address (either permanent or correspondence) for SARAL accounts in the cash segment.
- Obtain a declaration from the client if the correspondence address differs from the OVD address, without requiring proof for the correspondence address.
- Ensure address verification through positive confirmation methods such as delivery acknowledgment, phone confirmation, or physical visits.
- Send KYC completion intimation letters via registered/speed post or courier to the correspondence address; block transactions and alert exchanges/depositories if letters are returned undelivered.
- Flag such accounts appropriately in internal and KRA systems.

5. Confidentiality of Client Information

KFINTECH shall:

- Maintain strict confidentiality of all client information and disclose it only where required under applicable laws.

V. KNOW YOUR CLIENT (KYC) REGISTRATION AGENCY

The Know Your Client (KYC) Registration Agency (KRA)[p] framework was established in the Indian securities market to centralize and streamline the maintenance of KYC records across intermediaries. Under the SEBI KYC Registration Agency (KRA) Regulations, 2011, this mechanism ensures that client identification data is verified, stored, and made uniformly accessible to all market intermediaries. By enabling a single KYC process that can be used across multiple entities, the KRA system enhances efficiency, reduces duplication, and strengthens regulatory oversight in the securities market.

A. Guidelines for Intermediaries

i. Clients must be allowed to open accounts and transact in the securities market as soon as the KYC process is completed.
ii. After completing the KYC of new clients, intermediaries must upload the KYC information to the KRA system within 3 working days.
iii. If the KYC documents submitted to the KRA are incomplete, the KRA will notify the intermediary, who must promptly forward the required information/documents.
iv. For existing clients, intermediaries shall upload KYC data only if it conforms to the uniform KYC format while ensuring no data duplication in the KRA system.
v. Intermediaries must maintain electronic KYC records; physical records are not required.

[p] *KFIN Services Private Limited is registered as KYC KRA and shall follow these guidelines.*

vi. Intermediaries must promptly provide KYC-related information to the KRA whenever sought.
vii. Adequate internal controls must be in place to ensure security and authenticity of uploaded data.

B. Guidelines for KFINTECH

i. KFINTECH must provide KYC information to intermediaries in both data and image form.
ii. Within 2 working days of receiving initial or updated KYC documents, KFINTECH must send a confirmation letter to the client and maintain proof of dispatch.
iii. KFINTECH must coordinate to avoid duplication of KYC entries and ensure uniformity in the formats used for uploading, modifying, and downloading KYC data.
iv. KFINTECH must maintain an audit trail of uploads, modifications, and downloads made by intermediaries.
v. KFINTECH must conduct an annual comprehensive audit of systems, controls, procedures, safeguards, and data security through an independent auditor.
vi. The audit report and corrective steps must be presented to the Board of Directors.
vii. An Action Taken Report (ATR) must be submitted[q] within 3 months.
viii. KFINTECH must clearly indicate clients who fall under PAN-exempt categories such as residents of Sikkim, UN entities, multilateral agencies, etc.

C. Rationalisation of Risk Management Framework at KFINTECH

i. As part of risk management, KFINTECH must verify the following attributes within 2 days of receiving KYC records:
    a. PAN (including PAN–Aadhaar linkage)
    b. Name
    c. Address
ii. KFINTECH must also verify clients' mobile numbers and email IDs.
iii. For PAN-exempt clients, KFINTECH must verify:
    a. Name
    b. Address
    c. Mobile number
    d. Email ID
iv. Clients whose attributes cannot be verified must not be allowed to transact further in the securities market until verification is completed.
v. Records in which all attributes (as per paras i/ii) are successfully verified through official databases (e.g., Income Tax, Aadhaar XML, DigiLocker, mAadhaar) will be classified as Validated Records.
vi. Validated Records will enjoy portability, meaning the client does not need to repeat the KYC process when moving between intermediaries.
vii. KFINTECH must adopt uniform internal verification standards and procedures in consultation with SEBI.
viii. Systems of intermediaries and KFINTECH must be integrated to enable seamless document and information flow for verification under the risk-management framework.

[q] *This is mandatory only for SEBI, no provision under any other regulators.*

D. Processing of Investor complaints against KRA {KYC (Know Your Client) Registration Agency} in SEBI Complaints Redress System (SCORES)

i. All complaints pertaining to KFINTECH will be electronically sent through SCORES at **http://scores.gov.in/Admin**.

ii. KFINTECH is directed to view the pending complaints and submit the Action Taken Report (ATR) along with supporting documents electronically in SCORES.

iii. Updation of action taken would not be possible with physical ATRs. Hence, submission of physical ATR will not be accepted for complaints lodged in SCORES.

iv. KFINTECH shall take adequate steps for redressal of grievances within one month from the date of receipt of the complaint and keep the investor duly informed[r] on the action taken thereon failure of which shall lead to penal consequences.

v. KFINTECH is advised to:
   a. develop the monitoring mechanism through internal audit and inspections.
   b. encourage investor to use SCORES for lodging their grievances.

[r] *KFINTECH shall also inform SEBI on the same.*

ANNEXURE IV

RECORD KEEPING AND MANAGEMENT

(This process is in reference to point IX of AML Policy)

1. INFORMATION TO BE MAINTAINED

- KFINTECH shall maintain and preserve information in respect of transactions in accordance with the requirements of the Policy, including the following:
  i. The nature of the transaction.
  ii. The amount of the transaction and the currency in which it is denominated;
  iii. The date on which the transaction was conducted; and
  iv. The parties to the transaction.
- KFINTECH shall also maintain information and records relating to verification of identity of clients/subscribers, identification of beneficial owners, due diligence carried out and analysis and monitoring of transactions and business relationships.

2. GENERAL RECORD-KEEPING REQUIREMENTS

- KFIN shall ensure compliance with record-keeping requirements prescribed under:
  i. the SEBI Act, 1992 and the Rules and Regulations made thereunder;
  ii. the Prevention of Money Laundering Act, 2002 (PMLA);
  iii. the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PMLR);
  iv. Master Circular issued by PFRDA on "Guidelines on Know Your Customer / Anti-Money Laundering/Combating the Financing of Terrorism (KYC/AML/CFT)"
  v. The International Financial Services Centres Authority (Anti-Money Laundering, Counter Financing of Terrorism and Know Your Customer) Guidelines, 2022 ("IFSCA (AML-CFT) Guidelines);
  vi. applicable Rules, Regulations, Exchange Bye-laws and Circulars; and
  vii. any other relevant legislation.
- Records shall be maintained in a manner sufficient to permit reconstruction of individual transactions, including the amounts involved and the type of currency, where applicable.
- Such records shall be capable of providing evidence for investigation, enforcement or prosecution of criminal or regulatory non-compliance, where required.
- Records may be maintained in electronic form and/or physical form, provided such records are secure, complete, accurate and readily accessible.
- Where KFINTECH utilizes third-party service providers for record storage, processing or management, KFINTECH shall ensure that adequate safeguards are in place to protect the confidentiality, integrity and availability of records. Physical and electronic access to premises, systems and data storage sites (including back-up facilities) shall be controlled, monitored and recorded. Secure transmission methods, encryption standards and non-repudiation safeguards shall be implemented, and applicable data protection and confidentiality requirements shall be complied with.

- KFINTECH shall establish internal procedures and controls to enable timely response to requests for information from competent authorities.
- Records relating to AML/CFT training conducted, including training material and attendance records, shall also be maintained.

3. AUDIT TRAIL AND TRANSACTION RECONSTRUCTION

- KFINTECH shall maintain adequate audit trails to facilitate reconstruction of the financial profile of accounts and transactions, where required.
- For client/subscriber accounts, records shall include, as applicable, identification of beneficial owners, volume of funds flowing through the account, and for selected transactions, details relating to the source and destination of funds, the form in which funds were offered or withdrawn, the identity of the person carrying out the transaction, and the form of authorization and instructions for the transaction.
- Audit trails and system logs shall be maintained in a tamper-proof manner and protected against unauthorized alteration through appropriate access controls, logging and monitoring mechanisms.

4. AVAILABILITY OF RECORDS

- KFINTECH shall ensure that all client/subscriber and transaction records are made available on a timely basis to competent authorities, as required.
- Where directed, such records shall be retained beyond the minimum retention period and produced in the manner specified by the authorities.

5. MAINTENANCE OF TRANSACTION RECORDS

- KFINTECH shall maintain a system for recording transactions, including transactions exceeding prescribed thresholds, series of transactions that are integrally or remotely connected, transactions involving forged, counterfeit or fraudulent instruments or documents, and suspicious transactions, whether attempted or executed, including transactions through non-monetary accounts.

6. CLIENT / SUBSCRIBER IDENTITY RECORDS

- KFINTECH shall obtain and maintain updated identification and due diligence records for all clients/subscribers and beneficial owners.
- Where such records are not available or cannot be obtained, KFINTECH may initiate appropriate action, including restriction or closure of the relationship, after providing due notice and in accordance with internal procedures.
- Identity-related records shall include identification and verification documents, beneficial ownership information, account files, business correspondence and results of any analysis undertaken in relation to transactions or relationships.

7. RETENTION AND PRESERVATION OF RECORDS

- Transaction records shall be preserved for a minimum period of five (5) years from the date of the transaction, unless a longer period is required.
- Records relating to client/subscriber identity, account files and business correspondence shall be preserved for a minimum period of five (5) years after the end of the business relationship or account closure, whichever is later.
- Where applicable requirements prescribe a longer retention period, including retention of records for at least six (6) years after the end of the business relationship, the longer retention period shall apply.
- Records relating to accounts settled by claim shall be preserved for at least five (5) years from the date of settlement.
- Records relating to transactions or relationships that are subject to investigation, disclosure, audit, inquiry or litigation shall be preserved until confirmation that the matter has been closed, irrespective of the minimum retention periods specified above.
- KFINTECH shall maintain a system for recording the nature and value of transactions prescribed[s] including:
    i. All cash transactions exceeding ₹10 lakh or its equivalent in foreign currency;
    ii. All series of cash transactions integrally connected, where:
        - individual transactions are below ₹10 lakh; and
        - the aggregate value exceeds ₹10 lakh within a month.

        For the purpose of suspicious transaction reporting, transactions that are remotely connected or related shall also be considered.
    iii. All cash transactions involving forged or counterfeit currency notes, or where any forgery of valuable security or document has taken place facilitating the transaction;
    iv. All suspicious transactions, whether or not made in cash, including credits or debits into or from non-monetary accounts, such as demat or securities accounts.

[s] *Prescribed under Rule 3 of the PML Rules,2005*

ANNEXURE V

SUSPICIOUS TRANSACTION MONITORING AND REPORTING (STR)

(This process is in reference to point XII *of AML Policy)*

This Annexure consolidates the key regulatory requirements on Suspicious Transaction Monitoring and Reporting (STR) as prescribed under the Prevention of Money Laundering Act (PMLA), the PML Rules, and guidelines issued by sectoral regulators and FIU-IND. It sets out the minimum standards that intermediaries and reporting entities shall adhere to for the identification, examination, escalation, documentation, and reporting of suspicious transactions, in order to ensure effective implementation of AML/CFT obligations and maintain the integrity of the financial system.

KFINTECH shall follow the below mentioned process effective monitoring and reporting of STRs:

1. REGULAR MONITORING, RISK ALIGNMENT & CDD

- KFINTECH shall apply client due diligence measures (**Refer Annexure II - Client Identification and Due Diligence for detailed process**) also to existing clients on the basis of materiality and risk, and conduct due diligence on such existing relationships appropriately. The extent of monitoring shall be aligned with the risk category of the client.

2. SPECIAL ATTENTION, THRESHOLDS & DOCUMENTATION

- KFINTECH shall pay special attention to all complex unusually large transactions/patterns which appear to have no economic purpose.
- KFINTECH may specify internal threshold limits for each class of client/subscriber accounts and pay special attention to transactions which exceed these limits.
- The background including all documents/ office records/ memorandums/ clarifications sought pertaining to such transactions and purpose thereof shall also be examined carefully and findings shall be recorded in writing.
- Such findings, records and related documents shall be made available to auditors and also to SEBI/stock exchanges/PFRDA/FIU-IND/other relevant Authorities, during audit, inspection or as and when required.
- These records are required to be maintained and preserved for a period of five years from the date of transaction.

3. RECORDKEEPING & INTERNAL REPORTING

- KFINTECH shall ensure a record of the transactions is preserved and maintained in terms of Section 12 of the PMLA and that transactions of a suspicious nature or any other transactions notified under Section 12 of the Act are reported to the Director, FIU-IND.

- Suspicious transactions shall also be regularly reported to the higher authorities within the intermediary.
- Further, KFINTECH's compliance cell shall randomly examine a selection/sample of transactions undertaken by clients/subscribers to comment on their nature i.e., whether they are in the nature of suspicious transactions or not.

4. RECOGNITION OF SUSPICIOUS TRANSACTIONS & ILLUSTRATIVE CIRCUMSTANCES

- KFINTECH shall ensure that appropriate steps are taken to enable suspicious transactions to be recognized and have appropriate procedures for reporting suspicious transactions.
- While determining suspicious transactions, KFINTECH shall be guided by the definition of a suspicious transaction contained in PML Rules as amended from time to time.
- **Illustrative circumstances** which may be in the nature of suspicious transactions (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):
    i. Clients whose identity verification seems difficult or clients that appear not to cooperate;
    ii. Asset management services for clients where the source of the funds is not clear or not in keeping with clients' apparent standing/business activity;
    iii. Clients based in high risk jurisdictions;
    iv. Substantial increases in business without apparent cause;
    v. Clients transferring large sums of money to or from overseas locations with instructions for payment in cash;
    vi. Attempted transfer of investment proceeds to apparently unrelated third parties;
    vii. Unusual transactions by CSCs and businesses undertaken by offshore banks/financial services.

5. INTERNAL ESCALATION & ACCESS TO INFORMATION

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

6. ATTEMPTED/ABORTED TRANSACTIONS

- KFINTECH shall report all such attempted transactions in STRs, even if not completed by clients, irrespective of the amount of the transaction**.**

7. HIGHRISK COUNTRIES & COUNTERMEASURES

- Clients of high-risk countries, including countries where existence and effectiveness of money laundering controls is suspected or which do not or insufficiently apply FATF standards, shall be subject to appropriate countermeasures.
- These measures may include a further enhanced scrutiny of transactions, enhanced relevant reporting mechanisms or systematic reporting of financial transactions, and applying enhanced due diligence (**Refer Annexure II - Client Identification and Due Diligence for detailed process**) while expanding business relationships with the identified country or persons in that country etc.

8. RESPONSIBILITY FOR REPORTING[t]

- Where KFINTECH maintains records centrally, it is responsible for filing of reports to Director, FIU-IND in accordance with PML Rules.

9. REGISTRATION WITH FIUIND & REPORTING MECHANICS

- KFINTECH should register with FIU-IND and mention a separate line of business on FINNET 2.0 by selecting the appropriate regulator, and shall furnish to the Director, FIU-IND, information referred to in Rule 3 in terms of Rule 7 of the PML (Maintenance of Records) Rules, 2005.
- The Director, FIU-IND shall have powers to issue guidelines to the reporting entities for detecting transactions referred to in Rule 3(1), to direct them about the form of furnishing information and to specify the procedure and the manner of furnishing information.
- The reporting formats and comprehensive reporting format guide prescribed/released by FIU-IND and Report Generation Utility and Report Validation Utility developed to assist reporting entities shall be taken note of by KFINTECH. The editable electronic utilities to file electronic CTR/STR on FIU-IND's website shall be made use of by reporting entities which are yet to install/adopt suitable technological tools.
- KFINTECH's Principal Officers, whose branches are not fully computerized, shall have suitable arrangement to cull out the transaction details and feed the data into an electronic file with the help of the editable electronic utilities of CTR/STR.

10. REDFLAG INDICATORS (FIUIND)

- Red Flag Indicators issued by FIU-IND also be considered for Suspicious Transaction, wherever necessary.

[t] *Applicable only for KFINTECH entity regulated by PFRDA*

11. TIMELINES, DELAYS & CONFIDENTIALITY

- While furnishing information to the Director, FIU-IND, delay of each day in not reporting a transaction or delay of each day in rectifying a mis-represented transaction beyond the time limit as prescribed in the Rule shall be constituted as a separate violation.
- Robust software, throwing alerts when the transactions are inconsistent with risk categorization and updated profile of the customers/subscribers shall be put in to use as a part of effective identification and reporting of suspicious transactions; adoption of automated fraud monitoring, machine learning for anomaly detection, and annual policy reviews addressing technology shifts and new compliance threats.
- KFINTECH shall leverage the broadest number of data points/records available with them in implementing alert generation systems.
- KFINTECH should not enter into arrangement with any unregulated entity which may have the effect of directly or indirectly impairing any reporting obligations.
- KFINTECH shall not put any restriction on operations in the accounts where an STR has been filed.
- Utmost confidentiality shall be maintained in filing of STR/NTR to FIU-IND. It shall be ensured that there is no tipping off to the customer at any level. Confidentiality requirement does not inhibit information sharing among entities in the group.

12. STR/NTR FILING REQUIREMENTS

- The STR shall be submitted **within 7 days** of arriving at a conclusion that any transaction or a series of transactions that are 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 month shall be submitted to FIU-IND **by 15th of the succeeding month**.
- The Principal Officer shall be responsible for timely submission of STR and NTR to FIU-IND.
- **No Nil reporting** needs to be made to FIU-IND in case there are no suspicious/non-profit organization transactions to be reported.

13. CONFIDENTIALITY OF STR (PERMITTED DISCLOSURES & PROTECTION)

- KFINTECH and its employees or agents shall not disclose to any person (including the customer):

  i. that it has reported or will be reporting a suspicious transaction to the FIU-IND;
  ii. that it has formed a suspicion on a particular customer's transaction; or
  iii. any other information which may cause the person to conclude that a suspicion has been formed or that a report has been or may be made to the FIU-IND.

- Disclosure is only allowed to:

    i. an officer, employee or agent of KFINTECH for any purpose connected to the performance of that person's duties;
    ii. a lawyer for the purpose of obtaining legal advice on the matter;
    iii. a supervisory authority (to enable it to carry out its supervisory role); or
    iv. disclosure in compliance with the court order.
- KFINTECH and its employees are protected from any civil, criminal or disciplinary action taken against them for reporting a suspicious transaction in good faith.
- This prohibition on tipping off extends not only to the filing of the STR and/or related information but even before, during and after the submission of an STR.

ANNEXURE VI

COMPLIANCE OBLIGATIONS UNDER INTERNATIONAL AGREEMENTS AND DOMESTIC LAWS

(This annexure is in reference to point XIII of the Group-AML Policy)

This section consolidates the compliance obligations imposed on regulated entities under various international agreements, UNSC sanctions regimes, and domestic laws, including the **Unlawful Activities (Prevention) Act, 1967 (UAPA), the Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005**, and obligations arising from FATF public statements and **FATCA/CRS** reporting requirements. It outlines the procedures to be followed for screening, reporting, freezing of assets, information-sharing, and confidentiality, in accordance with Government of India orders, regulatory circulars, and directives issued by SEBI, PFRDA, and IFSCA.

1. SECTION 51A OF THE UNLAWFUL ACTIVITIES (PREVENTION) ACT, 1967 (UAPA): APPLICABILITY & ORDERS

- Section 51A of the UAPA, relating to the purpose of prevention of, and for coping with terrorist activities was brought into effect through UAPA Amendment Act, 2008. In this regard, the Central Government has issued an Order dated 2nd February 2021 detailing the procedure for the implementation of Section 51A of the UAPA.
- By virtue of Section 51A of the UAPA, the Central Government is empowered to freeze, seize or attach funds of and/or prevent entry into or transit through India any individual or entities that are suspected to be engaged in terrorism. [The list is accessible at website **http://www.mha.gov.in**].
- In order to ensure expeditious and effective implementation of 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. The list of Nodal Officers for UAPA is available on the website of Ministry of Home Affairs (MHA).

2. PROHIBITION ON ACCOUNTS / NAME SCREENING AGAINST UN SANCTIONS LISTS

- KFINTECH shall ensure that in terms of Section 51A of UAPA and amendments thereto, they do not have any accounts (or open pension accounts) in the name of individuals/entities appearing in the lists of individuals and entities suspected of having terrorist links, which are approved by and periodically circulated by the United Nations Security Council (UNSC).
- KFINTECH should not open pension account of a subscriber whose identity matches with any person in the UN sanction list and those reported to have links with terrorists or terrorist organizations.
- KFINTECH to ensure that accounts are not opened in the name of anyone whose name appears in said list. It 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.

3) MAINTENANCE AND USE OF DESIGNATED LISTS; PERIODIC CHECKS

- KFINTECH shall periodically check MHA website for updated list of banned individuals.
- KFINTECH shall maintain an updated list of designated individuals/entities in electronic form and run a check on the given parameters on a regular basis to verify whether designated individuals/entities are holding any pension accounts or any funds, financial assets or economic resources or related services held in the form of securities with them.
- An updated list of individuals and entities which are subject to various sanction measures as approved by Security Council Committee pursuant to UNSC 1267 can be accessed at:
    i. **ISIL (Da'esh) & Al-Qaida Sanctions List:** https://www.un.org/securitycouncil/sanctions/1267/aq_sanctions_list and press releases at https://www.un.org/securitycouncil/sanctions/1267/press-releases
    ii. **UNSC 1988 (Taliban) Sanctions:** https://www.un.org/securitycouncil/sanctions/1988/materials
    iii. **UNSCR 1718 (DPRK) press releases:** https://www.un.org/securitycouncil/sanctions/1718/press-releases
    iv. **Consolidated UNSC press releases:**
    v. https://press.un.org/en/content/press-release
- KFINTECH shall leverage latest technological innovations and tools for effective implementation of name screening to meet the sanctions requirements.

4) REPORTING AND FREEZING PROCEDURES UNDER UAPA (SECTION 35(1) & 51A)

- The MHA, in pursuance of Section 35(1) of UAPA 1967, declares the list of individuals/entities, from time to time, who are designated as 'Terrorists'. All orders under section 35(1) and 51A of UAPA relating to funds, financial assets or economic resources or related services, circulated by regulators from time to time shall be taken note of for compliance.
- KFINTECH shall also file a 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.
- Full details of accounts bearing resemblance with any of the individuals/entities in the list shall immediately be intimated to the Central Nodal Officer[u] for the UAPA, at Fax No. 011-23092551 and also conveyed over telephone No. 011-23092548. The particulars apart from being sent by post shall necessarily be conveyed on email id: **jsctcr-mha@gov.in.**
- KFINTECH[v] shall 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, without delay. The communication shall be sent to SEBI through post and through email (**sebi_uapa@sebi.gov.in**) to the UAPA nodal officer of SEBI, Deputy General Manager, Division of FATF, Market Intermediaries Regulation and Supervision Department, Securities and Exchange Board of India, SEBI Bhavan II, Plot No. C7, "G" Block, Bandra

---

[u] *For SEBI Regulated entity.*
[v] *For SEBI Regulated entity. However, in case of entities regulated by PFRDA and IFSCA, no separate communication to these regulations is required apart from FIU-IND and MHA.*

Kurla Complex, Bandra (E), Mumbai 400051. The consolidated list of UAPA Nodal Officers is available at the website of Government of India, MHA.

- The procedure laid down in the UAPA Order bearing file no.14014/01/2019/CFT dated February 2, 2021, issued by the CTCR Division of the Ministry of Home Affairs, Government of India, shall be strictly followed and compliance with the Order shall be ensured.

5) WEAPONS OF MASS DESTRUCTION AND THEIR DELIVERY SYSTEMS (PROHIBITION OF UNLAWFUL ACTIVITIES) ACT, 2005 – SECTION 12A

- In terms of Section 12A of the WMD Act, the Central Government is empowered to:
    1. Freeze, seize or attach funds or other financial assets or economic resources—
        (i) owned or controlled, wholly or jointly, directly or indirectly, by such person; or
        (ii) held by or on behalf of, or at the direction of, such person; or
        (iii) derived or generated from the funds or other assets owned or controlled, directly or indirectly, by such person; and
- Prohibit any person from making funds, financial assets or economic resources or related services available for the benefit of persons related to any prohibited activity under the WMD Act/UNSC Act/any other relevant Act. The Central Government may exercise its powers through any authority assigned under Section 7(1).
- KFINTECH is directed to comply with the procedure laid down in the said Order and shall:
    (i) Maintain the list of individuals/entities ("Designated List") and update it, without delay;
    (ii) Verify if the particulars of the parties to financial transactions match with the Designated List; in case of match, do not carry out such transaction and immediately inform the Central Nodal Officer (CNO) (The Director, FIU-INDIA; Tel.: 011-23314458, 011-23314459 (FAX); Email: dir@fiuindia.gov.in), without delay;
    (iii) Run a check at onboarding and on a periodic basis to verify whether individuals/entities in the Designated List are holding any funds, financial assets or economic resources or related services (bank accounts, stocks, insurance policies etc.); where matched, immediately inform full particulars to the CNO, without delay;
    (iv) Send a copy of the communication in (ii) and (iii) to the Nodal Officer of SEBI, without delay (email: sebi_uapa@sebi.gov.in; address as above);
    (v) Prevent such individual/entity from conducting financial transactions, under intimation to the CNO, without delay, where there are reasons to believe beyond doubt that funds/assets fall under Section 12A(2)(a) or 12A(2)(b) of the WMD Act;
    (vi) File an STR with the FIU-IND covering all transactions in the accounts covered under (ii) and (iii), carried through or attempted through.
- Upon receipt, the CNO would cause verification; where confirmed, an order to freeze these assets under Section 12A would be issued and conveyed to the concerned reporting entity. KFINTECH shall also comply with provisions regarding exemptions and inadvertent freezing, as may be applicable.

6) FATF PUBLIC STATEMENTS AND HIGH-RISK JURISDICTIONS

- FATF Statements circulated by SEBI/IFSCA from time to time, and publicly available information, for identifying countries which do not or insufficiently apply the FATF Recommendations, shall be considered by KFINTECH.
- KFINTECH shall consider the risks arising from the deficiencies in AML/CFT regime of the jurisdictions included in the FATF Statements. Special attention shall be given to business relationships and transactions with persons (including legal persons and other financial institutions) from or emanating in such countries/jurisdictions.

  Explanation: The process referred to above does not preclude KFINTECH from having legitimate trade and business transactions with the countries and jurisdictions mentioned in the FATF statements.

- KFINTECH shall examine the background and purpose of transactions with persons from such jurisdictions, and written findings, together with all documents, shall be retained and be made available to the Authority and other relevant authorities, on request.

7) SECRECY OBLIGATIONS AND SHARING OF INFORMATION

- KFINTECH shall maintain secrecy regarding the customer information that arises out of the contractual relationship between it and the customer. Information collected from customers for the purpose of opening of account shall be treated as confidential and details thereof shall not be divulged without the express consent of the customer.
- While considering the requests for data/information from Government and other agencies, KFINTECH shall satisfy itself that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy.
- Exceptions:
  (i) where disclosure is under compulsion of law;
  (ii) where there is a duty to the public to disclose;
  (iii) where the interest of KFINTECH requires disclosure; and
  (iv) where the disclosure is made with the express or implied consent of the customer.

8) REPORTING REQUIREMENTS UNDER FATCA AND CRS

- Under FATCA and CRS, KFINTECH shall adhere to Income Tax Rules 114F, 114G and 114H and determine whether it is a Reporting Financial Institution as defined in Rule 114F and, if so, shall:
  (a) Register on the e-filing portal of Income Tax Department as Reporting Financial Institution;
  (b) Submit online reports using the digital signature of the 'Designated Director' by either uploading the Form 61B or 'NIL' report, as per CBDT schema; (Explanation: refer to FEDAI spot reference rates for Rule 114H thresholds);
  (c) Develop IT framework for due diligence and record-keeping per Rule 114H;
  (d) Develop a system of audit for the IT framework and compliance with Rules 114F, 114G, 114H;
  (e) Constitute a "High Level Monitoring Committee" under the Designated Director (or equivalent) to ensure compliance;
  (f) Ensure compliance with updated instructions/rules/guidance notes/press releases issued by CBDT from time to time.