AML & CFT Guidelines

For

Reporting Entities

Providing Services Related To

Virtual Digital Assets

Table of Contents

Contents

Acronyms

Term	Definition
AML	Anti-Money Laundering
CFT	Countering the Financing of Terrorism
CDD	Customer Due Diligence
CPF	Combating Proliferation Financing
CKYCR	Central Know Your Customer Registry
CRS	Common Reporting Standards
DApp	Decentralised or Distributed Application
DeFi	Decentralised Finance
DNFBP	Designated Non-Financial Business and Profession
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FI	Financial Institution (traditional financial institutions not defined as SPs)
FIU-IND	Financial Intelligence Unit – India
ICO / ITO	Initial Coin Offering / Initial Token Offering
Intermediary Service Provider	Refers to a Service Provider (SP) in a serial chain that receives and re-transmits a VDA transfer on behalf of the Originator SP and the Beneficiary SP or another intermediary SP.
KYC	Know Your Customer
ML/TF/PF	Money Laundering, Terrorism Financing and Proliferation Financing
NFT	Non-Fungible Token
NRA	National Risk Assessment

OFAC	Office of Foreign Assets Control (US)
OTC	Over-the-Counter
OVD	Officially Valid Document
P2P	Peer-to-Peer
PEPs	Politically Exposed Persons
PMLA	Prevention of Money Laundering Act 2002
PMLR	Prevention of Money-laundering (Maintenance of Records) Rules 2005
RBA	Risk-Based Approach
RE	Reporting Entities
SP	Service Provider providing services relating to Virtual Digital Assets
STR	Suspicious Transaction Reporting
UAPA	Unlawful Activities (Prevention) Act, 1967
UNSC	United Nations Security Council
VDA	Virtual Digital Assets
VC	Virtual Currencies
Wallet	Software or hardware that enables users to store and use Virtual Digital Assets. If hosted on an exchange or connected to the Internet, the same are referred to as Hot Wallets while offline wallets are referred to as Cold Wallets.

Introduction

1. Background

1.1 The Prevention of Money-Laundering Act, 2002 ('PMLA') forms the core of the legal framework put in place by India to combat Money Laundering. For the purpose of these guidelines, Money Laundering is defined in terms of Rule 3 of PMLA.

PMLA envisages certain record-keeping and reporting obligations for financial institutions and persons carrying on designated business or profession. Persons carrying on designated business or profession are defined in Clause (s) of sub-section (1) of Section 2 of the PMLA. Sub-clause (vi) of the said clause includes within the ambit of 'person carrying on designated business or profession' persons carrying on such other activities as the Central Government may, by notification, designate from time-to-time.

1.2 These guidelines shall be called AML & CFT Guidelines for Reporting Entities Providing Services Related To Virtual Digital Assets (hereinafter called "The Guidelines") and aim to provide a summary of the provisions of the applicable anti-money laundering, counter-terrorism financing and proliferation financing legislations in India, viz. the Prevention of Money Laundering Act, 2002 (hereinafter referred to as the "PMLA"), the Unlawful Activities (Prevention) Act, 1967 (hereinafter referred to as the "UAPA"), The Weapons of Mass Destruction and Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (hereinafter referred to as the "WMDA") and rules thereunder and their applicability to and implications for the providers of services related to Virtual Digital Assets hereinafter referred to as Service Providers (SPs) and their role in applying Anti-Money Laundering, Countering the Financing of Terrorism and Combating Proliferation Financing (AML/CFT/CPF) obligations.

a. These guidelines are intended to set out the steps that a SP shall implement to discourage and to identify any money laundering, terrorist financing or proliferation financing activities. It prescribes the procedures and obligations to be followed by the reporting entities to ensure compliance with AML/CFT/CPF guidelines.

b. The strategy would be to use deterrence (implementation of effective KYC, CDD and EDD measures), detection (e.g., monitoring and suspicious

transaction reporting), and record-keeping so as to facilitate investigations by the appropriate authorities wherever required.

1.3 Service Providers

The Central Government vide notification F.No. P-12011/12/2022-ES Cell-DOR dated March 07, 2023, has notified the following activities, when carried out for or on behalf of another natural or legal person in the course of business as an activity for the purposes of sub-clause (vi) of clause (sa) of sub-section (1) of section 2 of the Prevention of Money-laundering Act, 2002 (15 of 2003):

(i) exchange between virtual digital assets and fiat currencies;
(ii) exchange between one or more forms of virtual digital assets;
(iii) transfer of virtual digital assets;
(iv) safekeeping or administration of virtual digital assets or instruments enabling control over virtual digital assets; and
(v) participation in and provision of financial services related to an issuer's offer and sale of a virtual digital asset.

Explanation:- For the purposes of these guidelines 'virtual digital asset' shall have the same meaning assigned to it in clause (47A) of section 2 of the Income-tax Act 1961 (43 of 1961).

2. Purpose of the guidelines

The purpose of these guidelines is to

a. Understand and apply the risk-based approach and indicate best practices in the design and implementation of an effective risk-based approach.
b. Identify the entities that conduct activities or operations relating to VDAs i.e., SPs.
c. Establish an efficient reporting mechanism to prevent money laundering, terrorist financing and proliferation financing.
d. To assist entities engaged in or seeking to engage in VDA activities or operations to better understand their AML/CFT/CPF obligations and how they can effectively comply with the AML/CFT/CPF requirements as notified under PMLA/PMLR.

3. Scope

a. The guidelines apply to SPs and explain how they should implement the AML/CFT/CPF obligations effectively.

b. Further, the guidelines focus on VDAs that are convertible to other funds or value, including both VDAs that are convertible to other VDAs and VDAs that are convertible to fiat or that intersect with the fiat financial system.

c. Central Bank issued Digital Currencies (CBDCs) are outside the scope of this guidance since they are digital representation of fiat currencies.

4. Effective Date

These guidelines shall take effect immediately i.e. from 10th March 2023.

The guidelines would be subject to regular amendments or updates with a view to reflect changes at the level of the domestic and international regulatory landscape, including the market dynamics of the VDA sector, in or from India.

5. General Obligations of Service Providers (SPs)

5.1. Registration of SPs as Reporting Entities with FIU-IND

In terms of Rule 2 (wa) read with Rule 2 (sa) of PMLA, all SPs are required to register as Reporting Entities with FIU-IND. As part of RE registration, SPs must disclose their account details with Banks/FIs where they hold accounts for transactions as well as for holding of Client Money.

5.2. Policies and Procedures to Combat Money Laundering, Counter Terrorist Financing and Combat Proliferation Financing: (AML/CFT/CPF Program)

In order to combat the menace of money-laundering, terror financing, proliferation financing and other related serious crimes, Rule 7(3) of the PMLR casts an obligation on every reporting entity to evolve an internal mechanism in respect of these guidelines to detect transactions as specified under Rule 3(1) and furnishing information about such transactions to FIU-IND.

The obligation of reporting entities to effectively serve to prevent and impede money laundering and terrorist financing and to observe such internal controls not only by them but also by their Designated Director, officers and employees is a legal requirement under Rule 7(4) of the PMLR.

In order to discharge the statutory responsibility to detect possible attempts of money laundering, financing of terrorism or proliferation financing, every SP must have a robust AML/CFT/CPF program in place.

The AML/CFT/ CPF program must include the following points.

5.3. Internal policies, procedures, and controls signed off by the Board and Senior Management

5.3.1 To comply with the obligations of Reporting Entities as specified under PMLA, PMLR, every reporting entity shall establish appropriate policies and procedures for the prevention of ML, TF, and PF, and ensure their effectiveness and compliance with all relevant legal and regulatory requirements. The reporting entities shall:

5.3.2 Issue a statement of policies and procedures for dealing with ML, TF and PF risks, reflecting the current statutory and regulatory requirements;

5.3.3 Ensure that the spirit of these guidelines and internal policies and procedures are understood by all staff members;

5.3.4 Regularly review the policies and procedures on the prevention of ML, TF, and PF to ensure their effectiveness. To ensure the effectiveness of policies and procedures, the person carrying out such a review shall, as far as possible, be different from the one who has framed them;

5.3.5 Adopt client acceptance policies and procedures and undertake Client Due Diligence (CDD) measures to the extent that is sensitive to the risk of ML, TF and PF depending on the type of client, business relationship or transaction**;**

5.3.6 Further, in terms of Rule (3A) of PMLR with regard to implementation of policies by groups (as per rule 2(1)(cba) of PMLR “group" shall have the same meaning assigned to it in clause (e) of sub-section (9) of section 286 of the Income-tax Act, 1961), Groups are required to implement group-wide policies for the purpose of discharging obligations under the provisions of Chapter IV of the PMLA.

5.4. Appointment of a Designated Director and a Principal Officer

5.4.1 **Appointment**:

a. A “Designated Director” (as defined under the PMLR as amended from time to time) to ensure overall implementation of the obligations imposed under chapter IV of the Act and the Rules shall be appointed.

b. A Principal Officer (PO) at a senior level and preferably not below the level of Head (Audit/Compliance)/Chief Risk Officer shall be appointed to ensure compliance with the obligations imposed under chapter IV of the Act and the Rules.

The Principal Officer and the Designated Director should be separate individuals. The contact details of the Designated Director and the Principal Officer for AML/CFT/CPF obligations shall be communicated to FIU-IND within 7 (seven) days of appointment/changes.

5.4.2 **Roles and Responsibilities of Designated Director and the Principal Officer**

The Designated Director and the Principal Officer shall be responsible for the following obligations to combat money laundering/ countering the financing of terrorism/ combat proliferation financing:

5.4.2.1 Furnishing of the information under Rule 8 (1) of the PMLR, as prescribed under sub rule (1) of Rule 3 of the said rules every month, by 15th day of the succeeding month, in prescribed format to the Director, FIU-IND. However, the information in respect of a suspicious transaction shall be furnished not later than seven working days on being satisfied that the transaction is suspicious as per Rule 8(2) of the PMLR. Such information shall include any attempted transactions, whether or not made in cash;

5.4.2.2 Evolving an internal mechanism with regard to any directions/ guidelines issued by the Director, FIU-IND and for furnishing information as prescribed under sub rule (1) of Rule 3 of the PMLR;

5.4.2.3 Communication of group policies relating to prevention of ML,TF and PF to all management and relevant staff that handle account information, money and client records, etc. within their organisation;

5.4.2.4 Client acceptance policy and client due diligence measures, including requirements for proper identification, such as:

- Maintenance of records;
- Compliance with relevant statutory and regulatory requirements;
- Cooperation with the relevant law enforcement authorities, including the timely disclosure of information;

- Role of internal audit or compliance function to ensure compliance with the policies, procedures and controls relating to the prevention of ML, TF and PF, including detection of suspected money laundering transactions

5.5. Training

Appropriate training to be provided to employees (compliance and others) based on their job profile.

- SPs should have adequate screening procedures when hiring employees.
- Instruction manuals on the procedures for client on boarding, KYC, CDD, Sanctions screening, customer identification, record-keeping and transaction processing and review should be set out.
- Training requirements must be customised to specific roles.

5.6. Internal Control/Audit

The internal audit/ inspection departments should verify on a regular basis, compliance with policies, procedures and controls relating to money laundering activities. The reports should specifically comment on the robustness of the internal policies and processes in this regard and make constructive suggestions where necessary, to strengthen the policy and implementation aspects.

Special attention should be paid to business relationships and transactions, especially those which do not have apparent economic or visible lawful purpose. In all such cases, the background and purpose of such transactions will as far as possible, have to be examined and written findings maintained for assisting competent authorities.

5.7. Know Your Customer (KYC) Norms

Keeping in view the anonymous and instantaneous nature of VDA transfers and the potential of services offered by SPs being misused by state and non-state actors for the purpose of money laundering, terror financing and proliferation financing, all SPs must have a robust mechanism in place for complying with KYC requirements prior to on boarding of clients/ wallets as well as for carrying out re-KYC of existing customers.

a. Effective procedures should be put in place to obtain requisite details for proper identification of new customers as well as existing customers (if such details

are not already in place). Special care has to be exercised to ensure that the wallets are not opened under anonymous, pseudonymous, or fictitious names.

b. SPs to take steps to identify the beneficial owner and take all reasonable measures to verify the identity to their satisfaction so as to establish the beneficial ownership. For the purpose of these guidelines, Beneficial Ownership shall be determined as defined in Rule 9(3) of PMLR, and detailed in Annexure I.

I. 'Beneficial owner' for this purpose means 'an individual who ultimately owns the wallet or controls a customer of the SP or the person on whose behalf a transaction is being conducted and includes a person who exercises ultimate effective control over a legal person.

II. For the purpose of KYC, the Permanent Account Number (PAN) as applicable to residents or National Identity Number and any of the Officially Valid Document (OVD) as prescribed below can be used as a measure of identification

- The passport,
- The driving license,
- Proof of possession of Aadhaar number,
- The Voter's Identity Card issued by the Election Commission of India,
- Job card issued by NREGA duly signed by an officer of the State Government and
- Letter issued by the National Population Register containing details of name and address.

Provided that,

a. Where the customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form as issued by the Unique Identification Authority of India (UIDAI).

b. Where the OVD furnished by the customer does not have the updated address, the following documents or the equivalent e-documents thereof shall be deemed to be OVDs for the limited purpose of proof of address:-

    - Utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
    - Property or Municipal tax receipt;

- Pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
- Letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and licence agreements with such employers allotting official accommodation;

c. The customer shall submit OVD with current address within a period of three months of submitting the documents specified at '**b**' above

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

   Explanation: For the purpose of this clause, a document shall be deemed to be an OVD even if there is a change in the name subsequent to its issuance provided it is supported by a marriage certificate issued by the State Government or Gazette notification, indicating such a change of name.

e. An additional requirement for service providers involved in VDA transactions is to report transactions in Form 26QF (Quarterly statement of tax deposited in relation to transfer of virtual digital asset to be furnished by intermediaries) of the Income tax department, as per provisions of Section 194S of Income Tax Act, 1961. This form captures data points such as name and PAN of the buyer and broker (for both transactions in which TDS was deducted, and transactions in which TDS was not deducted), value and number of VDA transferred, and date of transaction.

f. SPs are required to comply with the relevant record keeping and reporting requirements under Information Technology Act and Income Tax Act in addition to record keeping and reporting requirements under PMLR.

The officially valid documents (OVDs) must be verified by the SP at the time of accepting the risk for compliance with KYC requirement for individuals. No further documentation is necessary for proof of residence where the document of identity submitted also gives the proof of residence. It is mandatory to obtain any one of

the documents to clearly establish the customer identity in respect of all new wallets.

III. In cases where e-KYC services of the Unique Identification Authority of India (UIDAI) are availed for KYC verification (which is acceptable subject to specific and express consent of the customer to access his/her data through UIDAI system), certification requirements under this clause shall be deemed to be complied with. The e-KYC should be based on biometric (finger/iris) authentication as the primary mode with One Time Password (OTP) based authentication as a second factor.

IV. While implementing the KYC norms on legal persons, SPs will have to identify and verify their legal status through various documents, to be collected in support of

- The name, legal form, proof of existence,
- Powers that regulate and bind the juridical persons,
- Address of the registered office/ main place of business
- For the purpose of KYC for business entities, documents mentioned in the Customer Due Diligence (CDD) measures prescribed by Reserve Bank of India Master Direction - Know Your Customer (KYC) Direction, 2016 as updated from time to time, shall be used and maintained.

V. At any point in time during the period, where the SP is no longer satisfied about the true identity of the customer, a Suspicious Transaction Report (STR) should be filed with FIU-IND.

5.7.1 **When should KYC be done?**

KYC shall be done by SPs prior to on boarding of customers as well as a one-time exercise in cases where such KYC is not already present as on the date of issuance of these guidelines. SPs may rely on the identification and verification steps that they have already undertaken in case of a customer, unless they have doubts about the veracity of the information with them.

Periodic KYC on existing customers may be done according to the RBA carried out by the SPs and at the very least every year owing to the high-risk nature of VDAs.

5.8. Client Due Diligence (CDD) Norms

5.8.1 SPs should maintain accurate and up-to-date customer information.

5.8.2 SPs have the obligation to identify their customers and their beneficial owners, which is essential for the prevention of ML/TF/PF.

5.8.3 In consonance with the basic principles of the KYC norms as prescribed in the PMLA or the rules made there under, all SPs shall frame their own internal directives based on their experience in dealing with their clients and legal requirements as per the established practices.

5.8.4 In accordance with Rule 9 of the PMLR, each SP shall adopt written procedures to implement the anti-money laundering provisions as envisaged under the PMLA, related to the 'Client Due Diligence Process'.

5.8.5 SPs would be expected to make use of relevant software to:

- Perform robust due diligence or KYC process on counterparty institutions;
- Identify counterparty wallet type (pre-transaction);
- Identify risk-related details about the beneficiary through Blockchain analytics and sanctions screening providers;
- Allow to safely send or receive encrypted customer KYC information through various messaging protocols;
- Store encrypted customer KYC information for up to five years; and
- Allow to generate reports to FIU-IND on a timely basis, upon request.
- All identification documents secured through the CDD measures should be retained by SPs for a period of at least five years as recommended under Chapter IV clause (3) of PMLA, 2002.
- The extent of the ongoing CDD measures applied by SPs should be determined on a risk-sensitive basis.
- However, SPs should be aware that as a business relationship develops, the associated ML/TF/PF risks may change.

5.9. Enhanced Due Diligence (EDD) Norms

SPs should examine, as far as reasonably possible, the background and purpose of all complex, unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose. Where the risks of money laundering, terrorist financing or proliferation financing are higher, SPs should be

required to conduct enhanced due diligence, consistent with the risks identified. In particular, they should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious.

5.9.1 Conducting enhanced due diligence should not be limited to merely documenting income proofs. It would mean having measures and procedures which are more rigorous and robust than normal KYC. These measures should be commensurate with the risk. While not intended to be exhaustive, the following are some of the reasonable measures in carrying out enhanced due diligence:

- More frequent review of the customers' profile/ transactions
- Application of additional measures like gathering information from publicly available sources or otherwise
- Reasonable measures to know the customer's source of funds commensurate with the assessed risk of customer and product profile which may include:
    - Conducting independent enquiries on the details collected on /provided by the customer where required,
    - Consulting a credible database, public or other, etc.,

5.9.2 EDD with respect to high-risk jurisdictions/ persons/ entities

Due to the potential for increased anonymity or obfuscation of VDA financial flows and the challenges associated with conducting effective supervision and CDD, including customer identification and verification, VDA activities are automatically regarded as posing higher ML/TF/PF risks that may potentially require the application of monitoring and EDD measures, where appropriate.

a. SPs may be required to apply EDD measures to business relationships and transactions with natural and legal persons from higher risk jurisdictions specifically with countries designated as tax-havens and those on the FATF grey and black lists.

SPs must implement EDD procedures when entering into business relationships with Politically Exposed Persons ("PEPs"). For the purposes of these guidelines 'PEP' shall have the same meaning assigned to it as per rule 2(1) (db) of PMLR.

b. In cases where an SP is not able to undertake the required EDD, the SP shall terminate the business relationship and file a suspicious transaction report (STR).

5.10. Sanctions screening for VDA transfers

For the purpose of enhanced monitoring, sanctions screening should be carried out both at the time of on boarding as well as when any VDA transfer is initiated.
SPs must ensure prompt application of the directives when issued by the competent authorities for implementing United Nations Security Council Resolutions relating to the suppression and combating of terrorism, terrorist financing and proliferation of weapons of mass destruction and its financing, and other related directives, as well as compliance with all other applicable laws, regulatory requirements and guidelines in relation to economic sanctions. SPs must also ensure prompt application of the directives when issued by the competent authorities relating to the individuals designated as 'terrorist' under Section 35(1)(a) of the UAPA, 1967 and directives when issued by the competent authorities under WMDA.

Since VDA transfers can currently be completed even without verification of sanctions screening, SPs may put in place the following safeguards.

a. Putting a wallet on hold until screening is completed and confirmed that no concern is raised.

b. Arranging to receive a VDA transfer with a provider's wallet that links to a customer's wallet and moving the transferred VDA to their customer's wallet only after the screening is completed and has confirmed that no concern is raised.

5.11. Counterparty Due Diligence

This would be applicable to VDA transfers from a customer holding a wallet with an SP or using its services to transfer VDAs to a wallet hosted by another SP. In this case the originating SP would need to carry out CDD on the counterparty SP before they transmit the required information to avoid dealing with illicit actors or sanctioned actors unknowingly.

Considering the concept of due diligence, SPs must refresh their counterparty due diligence information periodically and when faced with emergent risk in line with their defined RBA control structure stemming from suspicious transaction history or other information such as adverse media, published information about regulatory or criminal penalties.

5.12. Correspondent Relationship

A ‘correspondent relationship’ is the provision of VDA related services by one SP to another SP or FI. Like its banking sector equivalent, such a correspondent relationship is characterised by its **on-going, repetitive nature**. Such a relationship could also include, for example, one SP white-labelling its platform functionality to another SP and also providing nested services (providing accounts to smaller SPs for access to liquidity and trading pairs).

It should be incumbent on SPs providing services to another SP or financial institution as part of a cross-border correspondent relationship to:

5.12.1. Gather sufficient information about the other SP or FI with which it proposes to establish a correspondent relationship, to understand fully the nature of the other SP or financial institution’s business and its AML/CFT/CPF risk control framework, including: what types of customers the other SP or FI intends to provide services to through the correspondent relationship;

5.12.2. Gather sufficient information and determine from publicly available sources the reputation of the other SP or FI, the quality of supervision it is subject to and whether it has been subject to an ML/TF/PF investigation or regulatory action;

5.12.3. Assess the other SP’s or FI’s AML/CFT/CPF controls;

5.12.4. Obtain approval from senior management before establishing new correspondent relationships; and

5.12.5. With respect to accounts or custodial wallets able to be used directly by customers of the other SP or FI to transact business on the customer’s own behalf, be satisfied that the other SP or FI has conducted CDD on such customers and is able to provide relevant CDD information on request and transaction details pertaining to identified customer/s, to the extent permitted privacy and data protection regulations in both jurisdictions.

6. Reporting Obligations of Service Providers (SPs)

The AML/CFT/CPF program envisages submission of reports on certain transactions to Financial Intelligence Unit-India (FIU-IND) set up by the Government of India to coordinate and strengthen collection and sharing of financial intelligence through effective national, regional, and global network to combat money laundering and related crimes. FIU-IND is the central nodal agency responsible for receiving, processing, analysing, and disseminating information relating to suspect financial transactions.

All SPs are required to, where they have reasonable grounds to suspect that funds are the proceeds of crime or are related to ML, TF and PF, report their suspicions promptly to FIU-IND.

In addition, SPs may be required to report specific indicators that may be associated with VDA activity, such as device identifiers, IP addresses with associated time stamps, VDA wallet addresses, and transaction hashes.

6.1. Reporting to Financial Intelligence Unit-India

a. In terms of the PMLR, reporting entities are required to report information relating to cash and suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND) at the following address: Director, FIU-IND, Financial Intelligence Unit-India, 6th Floor, Tower 2, Jeevan Bharati Building, Connaught Place, New Delhi-110001. Website: http://fiuindia.gov.in

b. Format for reporting Transactions: The format for reporting transactions, including suspicious transactions made or attempted, as required under Rule 7(2) of PMLR, would be as prescribed by FIU-IND.

6.1.1. Suspicious Transactions Report (STR):

Rule 8(2) read with Rule 3(1)(D) of the PMLR provides for prompt reporting of a suspicious transaction, which includes an attempted suspicious transaction, to the Financial Intelligence Unit (FIU-IND), if a reporting entity suspects or has reasonable grounds to suspect that funds used by a client are the proceeds of a criminal activity, or are related to terrorist financing. As detailed in Rule 3(1) of PMLR, suspicious transactions shall be reported no later than seven working days from the date of forming of suspicion.

a. Suspicious activity monitoring program should be appropriate to the SP and the services it provides. Special attention should be paid to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose. Background of such transactions, including all documents/ office records/ memorandums pertaining to such transactions, as far as possible, should be examined by the Principal Officer for recording their findings.
b. Nothing in these Regulations is intended to limit any function or power conferred on another body or authority under the AML/CFT/CPF laws.

The **STR reporting** would be at multiple points as illustrated below, e.g., if an SP X is designated as an RE, then the STR reporting obligation would be on the following entities)

i. The FI from where the funds flow into X, if the funding of a user wallet is done through NEFT/RTGS/IMPS.
ii. The SP X, when the funds are moved on the exchange hot wallet for purchase of VDAs for further purchase of VDAs. E.g., X purchasing VDA from SP Y via an escrow account for a customer and then crediting the VDA to the customer hot wallet.
iii. X in cases where P2P transfer is done between customers of X since KYC data of both customers would be available with X.
iv. X in cases where P2P transfer is done between a customer of X and an unhosted wallet since KYC data of the customer holding a hosted wallet at X would be available with X along with the beneficiary wallet details of the beneficiary used at the time of VDA transfer.

6.1.2. Reporting of receipts by Non-Profit Organizations:

All transactions, involving receipts by non-profit organizations (i.e., wallets directly owned by NGOs/ NPOs or by persons known to be affiliated to them) of value more than ₹10,00,000/- or its equivalent in foreign currency, should be reported to FIU-IND. For the purposes of these guidelines 'non-profit organisation' shall have the same meaning assigned to it as per rule 2(1) (cf) of PMLR.

As prescribed under Rule 2(9A) of PMLR, every SP shall register the details of NPO accounts/ wallets held by it on the DARPAN Portal of NITI Aayog, if not

already registered, and maintain such registration records for a period of five years after the business relationship has ended or the account has been closed, whichever is later.

6.1.3. Transaction Monitoring

SPs would be required to monitor the transactions going through their systems (intermediary SPs and where at least one wallet (originator or beneficiary) is hosted by them.

SPs are required to develop, implement, and maintain effective transactional monitoring systems to determine the origin of a VDA and to monitor its destination, and to apply strong KYC measures that enable detection of possible ML/TF activities.

7. Prohibition of Tipping-off

Reporting entities and their directors, officers, and employees (permanent and temporary) shall be prohibited from disclosing ("tipping off") that an STR or related information is being reported or provided to the FIU-IND. 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. Thus, it shall be ensured that there is no tipping off to the client at any level. It is clarified that the reporting entities, irrespective of the amount of transaction and/or the threshold limit envisaged for reporting under PMLA, shall file an STR if they have reasonable grounds to believe that the transactions involve proceeds of crime.

8. Sharing of Information:

Sharing of information on customers as defined under Rule 66 of PMLA would be applicable.

8.1. Record Retention under Section 12(3) of PMLA

SPs are required to retain records as defined in Sections 12(1)(a) and 12(1)(e)of PMLA and for a period of five years after the business relationship between a client and the reporting entity has ended or the account has been closed, whichever is later as mentioned in Section 12(3) of PMLA , in order to ensure that such documents are not destroyed.

9. Access to Information under Section 12A of PMLA

Section 12A reads as under –

(1) The Director may call for from any SP, any of the records referred to in Section 11A, sub-section (1) of Section 12 and any additional information as he considers necessary for the purposes of this Act.

(2) Every SP shall furnish to the Director such information as may be required by him under sub-section (1) within such time and in such manner as he may specify.

(3) Save as otherwise provided under any law for the time being in force, every information sought by the Director under sub-section (1), shall be kept confidential.

9.1 The SPs must ensure that technology, systems, and measures are in place to safeguard the privacy of the data maintained and to prevent unauthorized access, alteration, destruction, disclosure or dissemination of records and data

9.2 The physical or electronic access to the premises, facilities, automatic data processing systems, data storage sites and facilities including back-up sites and facilities and to the electronic data communication network of the service provider is controlled, monitored, and recorded;

9.3 The SP must establish standard transmission and encryption formats and non-repudiation safeguards for electronic communication of data.

9.4 The SP must implement specific procedures for retaining internal records of transactions both domestic or international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of VDA/ fiat currency involved (if any) so as to provide, if necessary, evidence for prosecution of criminal activity.

9.5 Where the records relate to ongoing investigations, or transactions which have been the subject of a disclosure, they should be retained until it is confirmed that the case has been closed where practicable, SPs are required to seek and retain relevant identification documents for all such transactions and to report such transactions of suspicious funds.

9.6 In case of customer identification data obtained through the customer due diligence process, account files and business correspondence should be retained for at least five years after the business relationship is ended or the account has been closed, whichever is later.

10. Risk Based Assessment

Risk assessments must be designed and implemented to assist SPs to better understand their risk exposure and areas in which they should prioritise allocation of resources for appropriate control and oversight of their AML/CFT/CPF activities. SPs shall carry out risk assessment to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk, severally and together, for customers, countries or geographic areas, and products, services, transactions or delivery channels that are consistent with the national risk assessment duly notified by the Central Government.

A key component of their RBAs will entail that they should:

10.1 Identify areas where their products/services could be exposed to ML/TF/PF risks e.g.

a. Virtual Digital Assets [in particular, Anonymity-Enhanced Crypto currencies];
b. Virtual Digital Asset related products or services [in particular, methods in which Anonymity Enhanced Transactions can be conducted];
c. Virtual Digital Assets related business and professional practices; and
d. Technologies associated with VDA Activities.
e. Customers carrying out extremely complex or high value transactions.
f. Customers carrying out transactions with known high-risk jurisdictions.

10.2 Take appropriate steps to ensure that any identified risks are managed and mitigated through the establishment of appropriate and effective policies, procedures, and controls.

10.3 The risk assessment shall be documented and be kept up-to-date. The SP shall consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. It shall be made available to competent authorities and self-regulating bodies, as and when required.

10.4 SPs should carry out an effective RBA and not resort to wholesale termination or exclusion of business relationships within their sector or operations, without an appropriately targeted risk assessment.

10.5 Risk Assessments should be subject to regular review and updation to ensure an effective system for remedying any identified deficiencies.

10.6 A risk assessment should typically consider all of the risk factors that the SP considers relevant, including the types of services, products, transactions, or technologies involved; customer risks; geographical factors; types of VDAs traded, among other factors.

a. SPs must, inter alia, identify, assess, understand, and monitor ML/TF risks for its customers.
b. SPs shall also consider the findings of the National Risk Assessment for appropriate Direction in the adoption of its business risk assessment.

10.7 Certain clients may be of a higher or lower risk category depending on the client's background, type of business relationship or transaction, etc. In order to identify the types of clients that are likely to pose a higher-than-average risk of ML, TF or PF, the SP shall develop appropriate client acceptance policies and procedures.

10.8 The risk assessment shall be documented and shall be made available to the Director, FIU-IND, as and when required. The following safeguards are to be followed while accepting the clients:

a. No reporting entity shall allow the opening of or keep any anonymous account or account in fictitious names or accounts on behalf of other persons whose identity has not been disclosed or cannot be verified.
b. The clients should be categorised in two categories, viz. high risk and low risk.
c. Factors of risk perception for monitoring suspicious transactions of the clients are clearly defined having regard to clients' location, nature of business activity, trading turnover etc. and manner of making payment for transactions undertaken.

10.9 A risk assessment of clients who are non-residents, high net worth individuals, trusts, charities, NGOs, and organisations receiving donations, companies having close family shareholding or beneficial ownership, firms with sleeping partners etc. will determine their ML/TF/PF risk.

10.10 In cases where the appropriate CDD measures to identify the profile of a client cannot be applied or it is not possible to ascertain the identity of the client, or the information provided by the client is suspected to be false or non–genuine, the SP shall not enter into a transaction with such client. In such cases, a suspicious activity report shall be filed with FIU-IND.

10.11 In cases, where the identity of a client is ascertained as having a criminal background, a suspicious transaction report shall be filed with FIU-IND.

11. Specific Obligations

11.1. Initial Coin Offerings/ Initial Token Offerings (ICOs/ ITOs)

ICOs are generally a means to raise funds for new projects from early backers and function similar to IPOs for stock offerings. Persons offering services relating to issuance, offer, book building, underwriting, market making and placement agent activity, sale, distribution, ongoing market circulation and trading of a VDA would be considered as SPs

The use of an automated process such as a smart contract to carry out SP functions does not relieve the parties of responsibility for SP obligations. In such instances, controlling parties *(responsible for the execution of the contracts)* qualifying as SPs should undertake ML/TF/PF risk assessments prior to the launch or use of the platform and take appropriate measures to mitigate risks.

11.2. Virtual Digital Asset Transfers

All transactions related to transfer, exchange of VDAs for VDAs or fiat currencies would be construed to be on the lines of wire transfers since the same is defined as any transaction carried out on behalf of an originator through a FI by electronic means with a view to making an amount of funds available to a beneficiary person at a beneficiary FI, irrespective of whether the originator and the beneficiary are the same person.

Parties to a wire transfer for this purpose would mean (a) parties to a traditional wire transfer, (b) a VDA transfer between a SP and another obliged entity (e.g., between two SPs or between a SP and another obliged entity, such as a bank or other FI)

Exception: Transaction Fees, Blockchain rewards or Gas Fees are exempt from the definition of Wire Transfer and the travel rule since the recipient is not the originator or recipient of the VDA transfer itself.

11.2.1. VDA transfers to/from ‘intermediary SPs’

For VDA transfer to/ from intermediary SPs or FIs that facilitate VDA transfers as an intermediate element in a chain of VDA transfers, it is suggested that they may be treated as obliged entities and may be required to treat all VDA transfers as cross-border qualifying transfers.

Just as a traditional intermediary FI processing a traditional fiat cross-border wire transfer must ensure that all required originator and beneficiary information that accompanies a wire transfer is retained with it, so too must an intermediary SP or other comparable intermediary institution that facilitates VDA transfers ensure that the required information is transmitted along the chain of VDA transfers, as well as maintaining necessary records and making the information available to appropriate authorities upon request.

Similarly, where technical limitations prevent the required originator or beneficiary information from remaining with a required data submission, a record should be kept, for at least five years, by the receiving intermediary SP of all the information received from the ordering SP or another intermediary SP. Intermediary institutions involved in VDA transfers also have general obligations to identify suspicious transactions, take freezing actions, and prohibit transactions with designated persons and entities—just like ordering and beneficiary SPs (or other ordering or beneficiary obliged entities that facilitate VDA transfers).

11.2.2. VDA transfers to/from unhosted wallets

VDA transfers to / from unhosted wallets are categorised as high risk since either the originating or beneficiary wallet may not be hosted at an SP that is an obliged entity. This also covers P2P transfers where one of the wallets is not hosted.

In case where the VDA transfer is between two wallets where at least one of them is a hosted wallet, the onus of compliance would be on the obliged entity where the wallet is hosted.

In addition, additional limitations or controls may be put in place on such transfers with unhosted wallets.

11.3. Travel Rule

In terms of Rule 12(1) (a) of PMLA, SPs should ensure to include *required and accurate originator information*, and *required beneficiary information*, on wire transfers and related messages. SPs should also monitor wire transfers to detect those which lack the required originator and/or beneficiary information and screen the transactions to comply with relevant UNSCR resolutions.

The originating SPs must obtain and hold required and accurate originator information and required beneficiary information on VDA transfers, submit the above information to the beneficiary SP or financial institution (if any) immediately and securely, and

make it available on request to appropriate authorities. Beneficiary SPs must obtain and hold required originator information and accurate beneficiary information on VDA transfers and make it available on request to appropriate authorities.

This applied regardless of whether the value of the VDA transfer is denominated in fiat currency or another VDA.

The required information, **which the *ordering* SP must *obtain* and *hold*,** includes:

a. Originator's Permanent Account Number (PAN) or National Identity Number

b. Originator's name (*i.e.*, the sending person's accurate (i.e., verified) full name);

b. Originator's account number used to process the transaction. In the VDA context, this would mean the "wallet address" of the originator;

c. Originator's physical (geographical) address that uniquely identifies the originator to the ordering institution, or date and place of birth. Provided that such an address has been verified for accuracy by the originator SP as part of its KYC process.

d. Beneficiary's name (*i.e.*, the name of the person who is identified by the originator as the receiver of the VDA transfer). This is not required to be verified by the ordering institution for accuracy, but should be reviewed for the purpose of STR monitoring and sanction screening; and

e. Beneficiary account number used to process the transaction. In the VDA context, this could mean the "wallet address" of the beneficiary.

The required information **which the *beneficiary* SP must *obtain* from the originator SP and *hold*,** includes:

b. Originator's Permanent Account Number (PAN) or National Identity Number

c. Originator's name (i.e., the sending person's name). The beneficiary institution does not need to be verify the originator's name for accuracy, but should review it for the purpose of STR monitoring and sanction screening.

d. Originator's account number used to process the transaction. In the VDA context, this could mean the "wallet address" of the originator.

e. Originator's physical (geographical) address that uniquely identifies the originator to the ordering institution, or date and place of birth.

f. Beneficiary's name (i*.e.,* the name of the person who is identified by the originator as the receiver of the VDA transfer). The beneficiary institution must verify the beneficiary's name for accuracy, if the name of their customer has not been previously verified. Thus, the beneficiary institution can confirm if the beneficiary's name and account number they obtain from the ordering institution match with the beneficiary institution's verified customer data.

g. Beneficiary's account number used to process the transaction. In the VDA context, this could mean the "wallet address" of the beneficiary.

Annexure I

Procedures for determination of Beneficial Ownership of VDA Wallet

In order to have a uniform approach across the financial sector, the following procedures for determination of Beneficial Ownership as mentioned in Rule 9(3) of PMLR as amended from time to time are prescribed:

a. Where the customer is a company, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has a controlling ownership interest or who exercises control through other means.

Explanation - For the purpose of this sub-clause-

i. "Controlling ownership interest" means ownership of or entitlement to more than ten percent of shares or capital or profits of the company;

ii. "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements;

b. Where the customer is a partnership firm, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has ownership of/entitlement to more than fifteen percent of capital or profits of the partnership;

c. Where the client is an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has ownership of or entitlement to more than fifteen percent of the property or capital or profits of such association or body of individuals;

d. Where no natural person is identified under (a) or (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official;

e. Where the client is a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with ten percent or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership; and

f. Where the client or the owner of the controlling interest is a company listed on a stock exchange, or is a subsidiary of such a company, it is not necessary to identify

and verify the identity of any shareholder or beneficial owner of such companies, since it may be assumed that such due-diligence has been carried out at the time of listing on the exchange.