



hpsc
(Scheduled Bank)

हिमाचल प्रदेश राज्य सहकारी बैंक सीमित
H.P. State Co-operative Bank Ltd.

KNOW YOUR CUSTOMER (KYC) POLICY

www.hpsc.com

TABLE OF CONTENTS

Sr.No.	Topic	Page No.
1.	INTRODUCTION	1
1.1	ABOUT THE POLICY	1
1.2	SCOPE AND APPLICABILITY OF THE POLICY	2
1.3	POLICY CONTENTS	2
	I. CUSTOMER ACCEPTANCE POLICY	2
	II. RISK MANAGEMENT	3
	III. CUSTOMER IDENTIFICATION PROCEDURE	3
	IV. MONITORING OF TRANSACTIONS	4
	V. MONEY LAUNDERING AND TERRORIST FINANCING RISK ASSESSMENT BY BANK	4
2.	COMPLIANCE OF THE KYC POLICY	4
2.1	DESIGNATED DIRECTOR	5
2.2	PRINCIPAL OFFICER	5
2.3	COMPLIANCE MECHANISM	5
2.4	STATUTORY REPORTS TO BE FURNISHED TO FINANCIAL INTELLIGENCE UNIT-INDIA	6
3.	OTHER ASPECTS UNDER KYC	7
4.	OPERATIONAL GUIDELINES ON KYC	8
4.1	DEFINITIONS	8
4.2	SMALL ACCOUNT	14
5.	KEY ELEMENTS UNDER KYC	15
5.1	CUSTOMER DUE DILIGENCE (CDD)	15
5.2	RISK MANAGEMENT	20
5.2.1	RISK CATEGORIZATION	20
5.2.2	PERIODIC UPDATION OF ACCOUNTS	20
6.	REPORTING OBLIGATIONS	24
6.1	REPORTING REQUIREMENTS TO FIU	24
6.2	REPORTING FORMATS	24
6.3	FURNISHING OF INFORMATION	24
6.4	ROBUST SOFTWARE	24

6.5	REPORTS TO BE FURNISHED TO FIU-INDIA	24
	i) CASH TRANSACTION REPORT (CTR)	24
	ii) SUSPICIOUS TRANSACTION REPORT (STR)	25
	iii) COUNTERFIET CURRENCY REPORT (CCR)	26
	iv) NON-PROFIT ORGANIZATION TRANSACTION REPORT (NTR)	26
7.	INTERNAL KYC MECHANISM AND STRUCTURE (ROLES AND RESPONSIBILITIES OF THE STAFF)	27
8.	OBLIGATORY COMPLIANCES TO ACTS/LAWS	28
9.	OTHER INSTRUCTIONS	31
	ANNEXURES	35-69
	ANNEXURE I	35
	ANNEXURE II	47
	ANNEXURE III	49
	ANNEXURE IV	50
	ANNEXURE V	53
	ANNEXURE VI	65

1. INTRODUCTION

KYC is the mandatory process of identifying and verifying the client's identity while opening an account and it has to be updated periodically over time. In other words, banks must ensure that their clients are genuinely who they claim to be.

Know Your Customer (KYC) has gained significance over the years as it helps financial institutions verify the identity of their customers, assess potential risks, prevent fraud, and comply with legal and regulatory requirements.

KYC procedures defined by banks involve all the necessary actions to ensure their customers are real, assess, and monitor risks. These client-on boarding processes help prevent and identify money laundering, terrorism financing, and other illegal corruption schemes.

In order to prevent banks and other financial institutions from being used as a channel for Money Laundering (ML)/ Terrorist Financing (TF) and to ensure the integrity and stability of the financial system, efforts are continuously being made both internationally and nationally, by way of prescribing various rules and regulations. Internationally, the Financial Action Task Force (FATF) which is an inter-governmental body established in 1989 by the Ministers of its member jurisdictions, sets standards and promotes effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. India, being a member of FATF, is committed to upholding measures to protect the integrity of international financial system.

In India, the Prevention of Money-Laundering Act, 2002 and the Prevention of Money- Laundering (Maintenance of Records) Rules, 2005, form the legal framework on Anti- Money Laundering (AML) and Countering Financing of Terrorism (CFT). In terms of the provisions of the PML Act, 2002 and the PML Rules, 2005, as amended from time to time by the Government of India, Banks are required to follow certain customer identification procedures while undertaking a transaction either by establishing an account-based relationship or otherwise and monitor their transactions.

1.1 ABOUT THE POLICY

This KYC Policy is issued as per RBI's Master Direction on Know Your Customer (updated up to 04.05.2023) and GOI (MOF) Gazette Notification dated 03.05.2023 & 09.05.2023.

1.2 SCOPE AND APPLICABILITY OF THE KYC POLICY

Bank shall take all necessary steps to implement this KYC policy and provisions of Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, as amended from time to time, including operational instructions issued in pursuance of such amendment(s). The provisions of KYC Policy guidelines shall apply to all the branches / offices of the Bank.

Instructions in this regard should provide a protection against threats arising from money laundering, terrorist financing, proliferation financing and other related risks. While ensuring compliance of the legal/regulatory requirements as above, it shall also be considered to adopt best international practices taking into account the FATF standards and FATF guidance notes, for managing risks better.

1.3 POLICY CONTENTS

THE KYC POLICY INCLUDES FOLLOWING KEY ELEMENTS:

- I. CUSTOMER ACCEPTANCE POLICY
- II. RISK MANAGEMENT
- III. CUSTOMER IDENTIFICATION PROCEDURE (CIP)
- IV. MONITORING OF TRANSACTIONS
- V. MONEY LAUNDERING AND TERRORIST FINANCING RISK ASSESSMENT BY BANK

I. CUSTOMER ACCEPTANCE POLICY

Bank's Customer Acceptance Policy (CAP) lays down the guidelines for acceptance of customers. It is to be ensured as under:-

- (i) No account is opened in anonymous or fictitious / benami name.
- (ii) No account is opened where the Bank is unable to apply appropriate Customer Due Diligence (CDD) measures, either due to non-cooperation of the customer or non-reliability of the documents / information furnished by the customer.
- (iii) No transaction or account based relationship is undertaken without following the Customer Due Diligence procedure.
- (iv) The mandatory information sought for KYC purpose while opening an account and during the periodic updation, is specified.
- (v) Additional information, where such information requirement has not been specified in KYC Policy of the Bank, is obtained with the explicit consent of the customer.
- (vi) The CDD procedure is to be applied at the time of customer ID creation in the branch. Thus, if an existing KYC compliant customer of Bank desires to open another account with the same Bank, there shall be no need for a fresh CDD exercise.
- (vii) CDD Procedure is followed for all the joint account holders, while opening a

joint account.

(viii) Circumstances in which, a customer is permitted to act on behalf of another person / entity, are clearly spelt out.

(ix) No account is opened where identity of the customer matches with any person or entity, whose name appears in the sanctions lists indicated at Sr No. 8, Page No-28.

(x) Where Permanent Account Number (PAN) is obtained, the same shall be verified.

(xi) Where Goods & Services Tax (GST) details are available, the GST number shall be verified.

It is to be ensured that the Customer Acceptance Policy shall not result in denial of banking / financial facility to members of the general public, especially those, who are financially or socially disadvantaged.

- **Where a suspicion of money laundering or terrorist financing, is formed and reasonably believed that performing the CDD process will tip-off the customer, CDD process shall not be pursued, instead it shall be reported as suspicious transaction to Centralized AML Cell for onward reporting of STR to FIU –IND.**

II. RISK MANAGEMENT

For Risk Management, Bank has adopted risk based approach which includes the following:

(i) Customers shall be categorized as low, medium and high risk category, based on the assessment and risk perception of the Bank.

(ii) Risk categorization shall be undertaken based on parameters such as customer's identity, social / financial status, nature of business activity, and information about the clients' business and their location, geographical risk covering customers as well as transactions, type of products/services offered, delivery channel used for delivery of products/services, types of transaction undertaken—cash, cheque/ monetary instruments etc.

(iii) The risk categorization of a customer and the specific reasons for such categorization shall be kept confidential and shall not be revealed to the customer to avoid tipping off the customer.

III. CUSTOMER IDENTIFICATION PROCEDURE (CIP)

Customer Identification Procedure means undertaking client due diligence measures including identifying and verifying the customer and the beneficial owner. Bank to undertake identification of customers in the following cases:

(i) Commencement of an account-based relationship with the customer.

(ii) When there is a doubt about the authenticity or adequacy of the customer

identification data (CID) it has obtained.

(iii) Carrying out transactions for a non-account based customer, that is a walk-in customer, where the amount involved is equal to or exceeds rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected.

(iv) When Bank has reason to believe that a customer (account-based or walk-in) is intentionally structuring a transaction into a series of transactions below the threshold of rupees fifty thousand.

(v) It is to be ensured that introduction is not to be sought while opening accounts.

IV. MONITORING OF TRANSACTIONS

Bank shall undertake on-going due diligence of customers to ensure that their transactions are consistent with their knowledge about the customers, customers' business and risk profile; and the source of funds.

V. MONEY LAUNDERING AND TERRORIST FINANCING RISK ASSESSMENT BY BANK

(i) Bank shall carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment exercise periodically to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, products, services, transactions or delivery channels, etc. The assessment process should consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. While preparing the internal risk assessment, Bank shall take cognizance of the factors/deficiencies, if any, that the regulator (RBI/NABARD) may share with Bank from time to time.

(ii) The risk assessment by the Bank shall be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. of the Bank. Further, the periodicity of risk assessment exercised by the Section undertaking Risk Management and shall carry out the above said Risk Assessment exercise on annual basis. Bank shall apply a Risk Based Approach (RBA) for mitigation and management of the identified risk and should have Board approved policies, controls and procedures in this regard. Further, Bank shall monitor the implementation of the controls and enhance them if necessary.

2. COMPLIANCE OF KYC POLICY

Compliance of KYC Policy of the Bank, as advised in RBI's Master Directions on KYC will be ensured as under:-

2.1 DESIGNATED DIRECTOR:

(i) An Executive Director on the Board to be nominated as “**Designated Director**”, as per provisions of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, to ensure overall compliance with the obligations imposed under Chapter IV of the PML Act and the Rules. Designated Director shall be nominated by the Board. **The Managing Director Bank will be the Designated Director.**

(ii) The name, designation and address of the Designated Director shall be communicated to the FIU-IND.

(iii) Further, the name, designation, address and contact details of the Designated Director shall also be communicated to the RBI.

(iv) In no case, the Principal Officer be nominated as the 'Designated Director'.

2.2 PRINCIPAL OFFICER:

(i) The Board has nominated Dy. General Manager as Principal Officer of the Bank, who shall be responsible for ensuring compliance, monitoring transactions, sharing and reporting information as required under the law / regulations.

(ii) The name, designation and address of the Principal Officer shall be communicated to the FIU-IND.

(iii) Further, the name, designation, address and contact details of the Principal Officer shall also be communicated to the RBI.

(iv) The Principal Officer will report to Designated Director and will oversee the functioning of Centralized AML Cell as per PML Act/KYC Policy.

(v) The Principal Officer will maintain close liaison with enforcement agencies, banks and other institutions which are involved in the fight against money laundering and combating financing of terrorism.

2.3 COMPLIANCE MECHANISM

A. Compliance of KYC Policy will be ensured through: -

- A senior officer in the rank not below than the **Asstt General Manager** who will constitute as 'Senior Management' for the purpose of KYC compliance; **AGM (BRCTL cum Compliance Section)** will act as 'Senior Management' for the purpose.
- Allocation of responsibility through Office Order for effective implementation of policies and procedures at HO / District Office / Branch Office level.
- All HO Sections to ensure compliance of KYC guidelines in their respective areas of operation, products, services, activities etc.
- Independent evaluation of the compliance functions of Bank's policies and procedures, including legal and regulatory requirements be done by **BRCTL cum Compliance Section, HO.**
- Concurrent / internal audit system to verify the compliance with KYC / AML policies and procedures and submit quarterly audit notes and

compliance to their Controlling Office. Concurrent / internal audit to also ensure verification of compliance with KYC guidelines in system through system generated reports from CBS.

- At the end of every calendar quarter, implementation and compliance of guidelines at branches would be reviewed for apprising **Audit Committee of Board**.

B. It is to be ensured that decision-making functions of determining compliance with KYC norms are not outsourced by the bank.

C. PML Rules require the Bank to carry out Risk Assessment to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, and products, services, transactions or delivery channels. The risk assessment should-

- (i) be documented;
- (ii) consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied;
- (iii) be kept up to date; and
- (iv) be available to competent authorities and self-regulating bodies.

D. The implementation of KYC-AML guidelines by branches in letter and spirit has to be ensured by the District Managers/Internal Auditors and the same is to be checked during their visit to branches.

2.4 STATUTORY REPORTS TO BE FURNISHED TO FINANCIAL INTELLIGENCE UNIT –INDIA

In terms of Rule 3 of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 and in terms of Rule 7 thereof, the following reports shall be furnished to Financial Intelligence Unit-India as per guidelines prescribed by RBI / FIU as applicable and within the timelines specified.

1. Cash Transaction Report [CTR].
2. Suspicious Transactions Report [STR]
3. Counterfeit Currency Report [CCR]
4. Non Profit Organizations Transaction report [NTR]

Detailed Guidelines regarding reporting Requirements to FIU-India have been given in Operational Guidelines for KYC Policy.

3. OTHER ASPECTS UNDER KYC

Other KYC / AML Guidelines to be followed while on boarding of customers such as customer due diligence (CDD) procedure, identification of Beneficial Owner, periodic updation of KYC, transaction monitoring, etc., are given in Operational Guidelines of KYC Policy) such as: -

- (i) CDD Procedure for Individuals, Sole Proprietary firms, Legal Entities
- (ii) Identification of Beneficial Owner
- (iii) On-going Due Diligence
- (iv) Enhanced and Simplified Due Diligence Procedure
- (v) Record Management
- (vi) Internal Control System
- (vii) Requirements / Obligations under International Agreements
- (viii) Other Instructions

4. OPERATIONAL GUIDELINES ON KYC

4.1 DEFINITIONS

In terms of RBI's Master Direction on KYC, unless the context otherwise requires, the terms herein shall bear the meanings assigned to them below:

A. Terms bearing meaning assigned in terms of Prevention of Money Laundering Act, 2002 and the Prevention of Money Laundering (Maintenance of Records) Rules, 2005:

1. "Aadhaar number" as defined in the Aadhaar and Other Law (Amendment) Ordinance, 2019, means an identification number issued to an individual under sub-section (3) of section 3 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016), and includes any alternative virtual identity generated under sub-section (4) of that section.

2. "Act" and "Rules" means the Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, respectively and amendments thereto.

3. "Authentication", in the context of Aadhaar authentication, means the process as defined under sub-section (c) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

4. Beneficial Owner (BO)

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 persons, has / have 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 / entitlement to more than 10 per cent of the 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 / have ownership of / entitlement to more than 15 per cent of capital or profits of the partnership.

c. Where the customer 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 / have ownership of / entitlement to more than 15 per cent of the property or capital or profits of the

unincorporated association or body of individuals.

Explanation: Term 'body of individuals' includes societies. Where no natural person is identified under (a), (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official.

d. Where the customer is a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 10% 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.

5. "Certified Copy of OVD" - Obtaining a self attested copy by bank shall mean comparing the copy of officially valid document so produced by the customer with the original and recording the same on the copy by the authorized officer of the Branch and the concerned Branch Official will also attest the duly signed photograph of the customer.

6. "Central KYC Records Registry" (CKYCR) means an entity defined under Rule 2(1)(aa) of the Rules, to receive, store, safeguard and retrieve the KYC records in digital form of a customer.

7. "Designated Director" means a person designated by the Bank to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules.

8. "Digital Signature" shall have the same meaning as assigned to it in clause (p) of subsection (1) of section (2) of the Information Technology Act, 2000 (21 of 2000). [Presently, as per Information Technology Act, 2000, Digital Signature means authentication of any electronic record by a subscriber by means of an **electronic method or procedure in accordance with the provisions of section 3 of the Information Technology Act, 2000.**]

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

10. "Non-profit organizations" (NPO) means any entity or organization, constituted for religious or charitable purposes referred to in clause (15) of section 2 of the Income-Tax Act, 1961 (43 of 1961), that is registered as a trust or a society under the Societies Registration Act, 1860 or any similar State legislation or a company registered under Section 8 of the Companies Act, 2013 (18 of 2013).

11. "Officially valid document" (OVD) means 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 are issued by the Unique Identification Authority of India.

b. Where the OVD furnished by the customer does not have 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: -

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 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, failing which the operations in the account shall be restricted (**Debit-frozen**).

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.

12. "Offline verification" shall have the same meaning as assigned to it in clause (pa) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016).

13. "Person" has the same meaning assigned in the Act and includes

a. an individual,

b. a Hindu undivided family,

c. a company,

d. a firm,

e. an association of persons or a body of individuals, whether incorporated or not,

f. every artificial juridical person, not falling within any one of the above persons (a to e), and

g. any agency, office or branch owned or controlled by any of the above persons (a to f).

14. "Politically Exposed Persons" (PEPs) are individuals who are or have been entrusted with prominent public functions by the country, including the Heads of States/Governments, senior politicians, senior government or judicial and military officers, senior executives of state-owned corporations and important political party

officials.

15. "Principal Officer (PO)" means an officer nominated by the Bank, responsible for furnishing information as per rule 8 of the Rules.

16. "Suspicious transaction" means a "transaction" as defined below, 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 the Act, 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.

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

17. A 'Small Account' means a savings account which is opened in terms of sub-rule (5) of the PML Rules, 2005. Details of the operation of a small account and controls to be exercised for such account are specified in Section 5.

18. "Transaction" means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes:

- a. opening of an account;
- b. deposit, 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 non-physical means;
- c. the use of a safety deposit box or any other form of safe deposit;
- d. entering into any fiduciary relationship;
- e. any payment made or received, in whole or in part, for any contractual or other legal obligation; or
- f. establishing or creating a legal person or legal arrangement.

19. "UCIC" means **Unique Customer Identification Code**, i.e., unique customer-ID allotted to individual customers while entering into new relationships as well as to the existing customers. All the accounts of an individual customer will be opened under his / her UCIC.

B. Terms bearing meaning assigned in **RBI Master Directions on KYC**, unless the context otherwise requires, shall bear the meanings assigned to them below:

- 1. "Common Reporting Standards" (CRS)** means reporting standards set for implementation of multilateral agreement signed to automatically exchange information based on Article 6 of the Convention on Mutual Administrative Assistance in Tax Matters (MAAT).
- 2. Correspondent Banking:** Correspondent Banking is the provision of banking services by one bank (the "Correspondent Bank") to another bank (the "respondent bank). Respondent Banks may be provided with a wide range of services, including cash management (e.g interest bearing accounts in a variety of currencies), international wire transfers, cheque clearing, payable-through accounts and foreign exchange services.
- 3. "Customer"** means a person who is engaged in a financial transaction or activity with the Bank and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.
- 4. "Walk-in Customer"** means a person who does not have an account based relationship with the Bank, but undertakes transactions with the Bank.
- 5. "Customer Due Diligence (CDD)"** means identifying and verifying the customer and the beneficial owner.
- 6. "Customer identification"** means undertaking the process of CDD.
- 7. "KYC Templates"** means templates prepared to facilitate collating and reporting the KYC data to the CKYCR, for individuals and legal entities.
- 8. "Non-face-to-face customers"** means customers who open accounts without visiting the branch / offices of the Bank or meeting the officials of Bank.
- 9. "On-going Due Diligence"** means regular monitoring of transactions in accounts to ensure that they are consistent with the customers' profile and source of funds.
- 10. "Payable-through accounts":** The term payable-through accounts refers to correspondent accounts that are used directly by third parties to transact business on their own behalf.
- 11. "Periodic Updation"** means steps taken to ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records at periodicity prescribed by the Reserve Bank.
- 12. "Regulated Entities" (REs)** means
 - a.** all Scheduled Commercial Banks (SCBs)/ Regional Rural Banks (RRBs)/ Local Area Banks (LABs)/ All Primary (Urban) Co-operative Banks (UCBs)/State and

Central Co-operative Banks (StCBs / CCBs) and any other entity which has been licensed under Section 22 of Banking Regulation Act, 1949, which as a group shall be referred as 'banks'

- b.** All India Financial Institutions (AIFIs)
- c.** All Non-Banking Finance Companies (NBFCs), Miscellaneous Non-Banking Companies (MNBCs) and Residuary Non-Banking Companies (RNBCs)
- d.** All Payment System Providers (PSPs)/ System Participants (SPs) and Prepaid Payment Instrument Issuers (PPI Issuers)
- e.** All authorized persons (APs) including those who are agents of Money Transfer Service Scheme (MTSS), regulated by the Regulator.

C. All other expressions unless defined herein shall have the same meaning as have been assigned to them under the Banking Regulation Act, 1949, the Reserve Bank of India Act, 1935, the Prevention of Money Laundering Act, 2002, the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

4.2 Small Account

An individual who desires to open a bank account, bank shall open a 'Small Account', having the following **threshold limits**:

THRESHOLD LIMITS IN A SMALL ACCOUNT

- (i) the **aggregate of all credits in a financial year** does not exceed rupees **one lakh**;
- (ii) the **aggregate of all withdrawals and transfers in a month** does not exceed **rupees ten thousand**; and
- (iii) the **balance at any point of time** does not exceed rupees **fifty thousand**.

Provided, that this limit on balance shall not be considered while making deposits through Government grants, welfare benefits and payment against procurements.

Further, the following conditions are to be fulfilled for KYC compliance in small accounts:

- a. A self-attested photograph to be obtained from the customer.
- b. The designated officer of the bank certifies under his signature that the person opening the account has affixed his signature or thumb impression in his presence.

Provided that where the individual is a prisoner in a jail, the signature or thumbprint shall be affixed in presence of the officer in-charge of the jail and the said officer shall certify the same under his signature and the account shall remain operational on annual submission of certificate of proof of address issued by the officer in-charge of the jail.

- c. Such accounts are opened only at Core Banking Solution (CBS) linked branches or in a branch where it is possible to monitor the account.
- d. It is to be ensured that the stipulated monthly and annual limits on aggregate of transactions and balance requirements in such accounts are not breached, before a transaction is allowed to take place.
- e. The account shall remain operational initially for a **period of twelve months** which can be extended for a further period of twelve months, provided the account holder applies and furnishes evidence of having applied for any of the OVDs during the first twelve months of the opening of the said account.
- f. The entire relaxation provisions shall be reviewed after twenty four months.
- g. Notwithstanding anything contained in clauses (e) and (f) above, the small account shall remain operational between April 1, 2020 and June 30, 2020 and such other periods as may be notified by the Central Government.
- h. The account shall be monitored and when there is suspicion of money laundering or financing of terrorism activities or other high risk scenarios, due diligence must be carried out as per **Customer Due Diligence norms** elaborated separately in this policy.

5. KEY ELEMENTS UNDER KYC:

5.1 CUSTOMER DUE DILIGENCE (CDD)

5.2 RISK MANAGEMENT

5.2.1 Risk Categorization

5.2.2 Periodic Updation of Accounts

5.1 CUSTOMER DUE DILIGENCE (CDD)

Customer Due Diligence (CDD) is a process that financial institutions, businesses, and other organizations use to gather information about their customers and clients in order to identify and mitigate risks such as money laundering, financing terrorism, and other illicit activities.

CDD checks are designed to help organizations assess the risks posed by a customer and identify any red flags that may indicate an increased risk of illicit activity such as money laundering, financial terrorism. CDD procedures should be conducted at the time when a bank enters into the business relationship with the customer i.e the time customer opens his/her account with the Bank for the very first time.

1. CDD Procedure in case of Individuals

1. Banks shall obtain the following documents from an individual while opening an account:

- i) One certified copy of an OVD, containing details of identity and address;
- ii) One recent photograph; and
- iii) Such other documents pertaining to the nature of business or financial status specified by the Bank in their KYC policy.

Customers, at their option, shall submit one out of the six OVDs for proof of identity and proof of address.

"Officially valid document" (OVD) for KYC means the

- a) Passport
- b) PAN Card
- c) Driving license
- d) Proof of possession of Aadhaar number
- e) Voter`s Identity Card issued by the Election Commission of India
- f) Letter issued by the National Population Register containing details of name and address.

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

In case, the OVD furnished by the customer does not have 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**:-

1. **Utility bill** which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
2. **Property or Municipal tax receipt**;
3. **Pension or family pension payment orders (PPOs)** issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
4. **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 license agreements with such employers allotting official accommodation;
5. The customer **shall submit OVD with current address within a period of three months** of submitting the documents specified above.

2. CDD Measures for Sole Proprietary firms

1. For opening an account in the name of a sole proprietary firm, CDD of the individual/proprietor should be carried out first.
2. In addition to the above, any two of the following documents as a proof of business/ activity in the name of the proprietary firm shall also be obtained:

(a) Registration certificate

(b) Certificate/license issued by the municipal authorities under Shop and Establishment Act.

(c) Sales and income tax returns.

(d) CST/VAT certificate.

(e) Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities.

(f) Complete Income Tax Return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/acknowledged by the Income Tax authorities.

(g) Utility bills such as electricity, water, and landline telephone bills.

3. Business/ Activity proof for Sole Proprietary firms

In addition to the above, any two of the following documents or the equivalent e-document thereof as a proof of business / activity in the name of the proprietary firm shall also be obtained:

- (i) Registration certificate including Udyam Registration Certificate (URC) issued by the Government.
- (ii) Certificate / Licence issued by the municipal authorities under Shop and Establishment Act.
- (iii) Sales and income tax returns.
- (iv) CST / VAT / GST certificate.
- (v) Certificate / registration document issued by Sales Tax / Service Tax / Professional Tax authorities.
- (vi) Complete Income Tax Return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated / acknowledged by the Income Tax authorities.
- (vii) Utility bills such as electricity, water, and landline telephone bills.

In cases where the concerned branch is satisfied that it is not possible to furnish two such documents, the Branch Manager may, at their discretion, accept only one of those documents as proof of business / activity.

Provided it undertakes contact point verification and collect such other information and clarification as would be required to establish the existence of such firm, and shall confirm and satisfy itself that the business activity has been verified from the address of the proprietary concern.

4. CDD Measures for Legal Entities

1. The following documents shall be obtained for opening an account of:

A. COMPANY:

- (a) Certificate of incorporation**
- (b) Memorandum and Articles of Association**
- (c) Permanent Account Number** of the company **(MANDATORY)**
- (d) A resolution from the Board of Directors** and **power of attorney** granted to its managers, officers or employees to transact on its behalf
- (e) Documents** relating to beneficial owner, the managers, officers or employees, as the case may be, holding an **attorney to transact** on the company's behalf
- (f) The names of the relevant persons** holding senior management position; and
- (g) The registered office** and the **principal place of its business**, if both are different.

B. PARTNERSHIP FIRM

- (a) Registration** certificate
- (b) Partnership deed**
- (c) Permanent Account Number** of the partnership firm **(MANDATORY)**
- (d) Documents**, relating to beneficial owner, managers, officers or employees, as the case may be, holding an **attorney** to transact on its behalf
- (e) The names** of all the partners and

(f) Address of the registered office, and the **principal place** of its business, if it is different.

C. TRUST:

(a) Registration certificate

(b) Trust deed

(c) Permanent Account Number or Form No.60 of the trust

(d) Documents, relating to beneficial owner, managers, officers or employees, as the case may be, holding an **attorney** to transact on its behalf

(e) The names of the beneficiaries, trustees, settlor and authors of the trust

(f) The address of the registered office of the trust; and

(g) List of trustees and documents, for those discharging the role as trustee and authorized to transact on behalf of the trust.

D. UNINCORPORATED ASSOCIATION OR A BODY OF INDIVIDUALS

Unregistered trusts/partnership firms shall be included under the term 'unincorporated association'.

Term 'body of individuals' includes societies.

(a) Resolution of the managing body of such association or body of individuals

(b) Permanent Account Number or Form No. 60 of the unincorporated association or a body of individuals

(c) Power of attorney granted to transact on its behalf

(d) Documents relating to beneficial owner, managers, officers or employees, as the case may be, holding an **attorney to transact** on its behalf and Documents, as specified in Section 16,

(e) Such information as may be required by the Bank to collectively establish the legal existence of such an association or body of individuals.

For opening accounts of **juridical persons** not specifically covered in the earlier part, such as Government or its Departments, societies, universities and local bodies like village panchayats, one certified copy of the following documents shall be obtained:

(i) Document showing name of the person authorized to act on behalf of the entity;

(ii) Officially valid documents for proof of identity and address in respect of the person holding an attorney to transact on its behalf and

(iii) Such documents as may be required by the Bank to establish the legal existence of such an entity/juridical person.

5. Identification of Beneficial Owner

For opening an account of a Legal Person who is not a natural person, the beneficial owner(s) shall be identified and all reasonable steps in terms of Rule 9(3) of the Rules to verify his / her identity shall be undertaken keeping in view

the following :

a. Where the customer or the owner of the controlling interest is (i) an entity listed on a stock exchange in India, or (ii) it is an entity resident in jurisdiction notified by the Central Government and listed on stock exchanges in such jurisdictions, or (iii) it is a subsidiary of such listed entities; it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such entities.

b. In cases of trust / nominee or fiduciary accounts whether the customer is acting on behalf of another person as trustee / nominee or any other intermediary is determined. In such cases, satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also details of the nature of the trust or other arrangements in place shall be obtained.

6. On-going Due Diligence

1. Banks shall undertake on-going due diligence of customers to ensure that **their transactions are consistent with their knowledge about the customers**, customers' business and risk profile; and the source of funds.

2. Without preconceiving personalized judgement the **following transactions need to be monitored mandatorily:**

(a) Large and complex transactions including RTGS transactions, and those with unusual patterns, inconsistent with the normal and expected activity of the customer, which have no apparent economic rationale or legitimate purpose.

(b) Transactions which exceed the thresholds prescribed for specific categories of accounts.

(c) High account turnover inconsistent with the size of the balance maintained.

(d) Deposit of third party cheques, drafts, etc. in the existing and newly opened accounts followed by cash withdrawals for large amounts.

3. The **extent of monitoring shall be aligned with the risk category of the customer.**

High risk accounts have to be subjected to more intensified monitoring.

Types of transactions for monitoring: Without prejudice to the generality of factors that call for close monitoring following types of transactions shall necessarily be monitored:

a. Large and complex transactions including RTGS transactions, and those with unusual patterns, inconsistent with the normal and expected activity of the customer, which have no apparent economic rationale or legitimate purpose.

b. Transactions which exceed the thresholds prescribed for specific categories of accounts.

- c. High account turnover inconsistent with the size of the balance maintained.
 - d. Deposit of third party cheques, drafts, etc. in the existing and newly opened accounts followed by cash withdrawals for large amounts.
- For ongoing due diligence, Bank may consider adopting appropriate innovations including artificial intelligence and machine learning (AI & ML) technologies to support effective monitoring.

7. Enhanced and Simplified Due Diligence Procedure

Simplified norms for Self Help Groups (SHGs)

- (a) CDD of all the members of SHG shall not be required while opening the savings bank account of the SHG.
- (b) CDD of all the office bearers shall suffice, which includes President, Secretary, Cashier.
- (c) CDD of all the members of SHG may be undertaken at the time of credit linking of SHGs

5.2 RISK MANAGEMENT

For Risk Management, Bank has adopted risk based approach in the following manner:

5.2.1 RISK CATEGORIZATION

As per RBI directions the accounts should be properly categorized according to their risk profile which leads to effective supervision and monitoring.

- (a) Customers shall be categorized as low, medium and high risk category, based on the assessment and risk perception of the Bank.
- (b) Risk categorization shall be undertaken based on parameters such as customer's identity, social / financial status, nature of business activity, and information about the client's business and their location, geographical risk covering customers as well as transactions, type of products/services offered, types of transaction undertaken—cash, cheque/ monetary instruments, etc.
- (c) The risk categorization of a customer and the specific reasons for such categorization shall be kept confidential and shall not be revealed to the customer to avoid tipping off the customer.

BRANCHES SHOULD REFER ANNEXURE IV FOR RISK CATEGORIZATION OF ACCOUNTS.

5.2.2 PERIODIC UPDATION OF ACCOUNTS

A risk-based approach is adopted by the Bank for periodic updation of KYC. Periodic updation shall be carried out:

- at least once in every **two years for high risk customers**,
- Once in every **eight years for medium risk customers** and
- Once in every **ten years for low risk customers** from the date of opening of the account / last KYC updation.

1. Individual Customers:

(i) No change in Customer Information:

a. For such cases, a customer can submit a self-declaration should be obtained from the customer stating that there is no change in his/her KYC information.

b. Branch on obtaining the request from the Customer shall ascertain that KYC documents as per the prescribed norms are available with them and shall update the account thereby performing CKYC in the account with that effective date. The account will be updated as and when the branch performs CKYC in the account.

c. If the available documents, are not as per KYC norms or the validity of KYC document has expired, the Branch shall inform the Customer to submit the requisite documents for KYC Updation.

d. The KYC documents/self-declaration obtained from customer shall be maintained alongwith Account Opening Form at the home branch.

(ii) Change in address: In case of a change only in the address details of the customer new address proof shall be obtained from the customer, and the declared address shall be verified through confirmation within two months, by means such as **Letter of Thanks** to be delivered on the new address.

(iii) Accounts of customers, who were minor at the time of opening the account, on their becoming major: In case of customers for whom account was opened when they were minor, **fresh photographs** and **latest signatures** shall be obtained on the Account Opening Form (AOF) in the branch as they become major.

Further, branch will obtain fresh KYC of the person becoming major and maintain the same with the AOF. If the current address is different from the address in Aadhaar, the current address proof be obtained and kept in record.

The branch will perform CKYC in such a account after completing all the above steps.

2. Customers other than individuals/in case of Legal Entities:

(i) No change in KYC information: In case of no change in the KYC information of the Legal Entity (LE) accounts, a self-declaration i.e letter from an official authorized or BOD resolution in this regard shall be obtained from the LE account holder.

(ii) Change in KYC information: In case of change in KYC information, Bank shall undertake the KYC process equivalent to that applicable for on-boarding a new LE customer.

After obtaining the requisite documents wherever there is change in the KYC information, the branch will perform its C-KYC with that effective date in order to complete KYC updation in the said account.

3. Additional measures: In addition to the above, it shall be ensured by the concerned branch that,

(i) The KYC documents of the customer as per the current Customer Due Diligence (CDD) standards are available with them. This is applicable even if there is no change in customer information but the documents available with the Bank are not as per the current CDD standards. Further, in case the validity of the CDD documents available with the Bank has expired at the time of periodic updation of KYC, Bank shall undertake the KYC process equivalent to that applicable for on-boarding of a new customer.

(ii) Customer's PAN details, if available with the Bank, is verified at the time of periodic updation of KYC.

4. Partial Freezing and closure of Non- KYC Compliance Accounts

In case of existing accounts, which are not KYC compliant, Bank shall ordinarily take steps to terminate this existing business relationship after giving due notice.

Although, Bank shall have an option to choose not to terminate business relationship straight away and instead opt for a phased closure of operations in this account **as explained below:**

i. Due **notice of three months to the customers** to comply with KYC requirements.

ii. Thereafter, a **reminder** giving a further period of **three months** shall also be given.

iii. Thereafter, '**partial freezing**' shall be imposed by allowing all credits and **putting debit hold in the Account.**

iv. All debits and credits from/to the accounts shall be disallowed, in case of the account being KYC non-compliant **after six months of imposing 'partial freezing'**.

v. When an account is closed whether without 'partial freezing' or after 'partial freezing', the reason for that shall be communicated to account holder.

vi. The account shall be closed in case of the account being KYC non-compliant even **after six months of issuing first notice.**

vii. The account holders shall have the option to revive their accounts by submitting the KYC documents.

Therefore, the branches are advised to adhere to the above instructions meticulously.

5. Record Management

The following steps shall be taken regarding maintenance, preservation and reporting of customer account information, with reference to provisions of PML Act and Rules. It is to be ensured to,

- a.** maintain all necessary records of transactions between the Bank and the customer, both domestic and international, for at least five years from the date of transaction;
- b.** preserve the records pertaining to the identification of the customers and their addresses obtained while opening the account and during the course of business relationship, for at least five years after the business relationship is ended;
- c.** make available swiftly, the identification records and transaction data to the competent authorities upon request;
- d.** introduce a system of maintaining proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005);
- e.** maintain all necessary information in respect of transactions prescribed under PML Rule 3 so as to permit reconstruction of individual transaction, including the following :
 - (i) the nature of the transactions;
 - (ii) the amount of the transaction and the currency in which it was denominated;
 - (iii) the date on which the transaction was conducted; and
 - (iv) the parties to the transaction.
- f.** evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities;

6. REPORTING OBLIGATIONS

6.1 Reporting Requirements to Financial Intelligence Unit – India

The AML Cell shall furnish to the Director, Financial Intelligence Unit-India (FIU-IND), information referred to in Rule 3 of the PML (Maintenance of Records) Rules, 2005 in terms of Rule 7 thereof.

Explanation: In terms of Third Amendment Rules notified September 22, 2015 regarding amendment to sub rule 3 and 4 of rule 7, Director, FIU-IND shall have powers to issue guidelines to the Bank for detecting transactions referred to in various clauses of sub-rule (1) of rule 3, to direct them about the form of furnishing information and to specify the procedure and the manner of furnishing information.

6.2 The Reporting Formats

FIU India has made its old version of reporting, i.e. FinNet dysfunctional since April 2022. As such the new reporting is required to be done on Fingate 2.0. The new reporting formats and comprehensive reporting format guide, prescribed/ released by FIU-IND shall be referred for the purpose of preparing reports as per new formats.

6.3 Furnishing of Information

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 specified in the Rule shall be constituted as a separate violation. Offices shall not put any restriction on operations in the accounts where an STR has been filed and shall keep the fact of furnishing of STR strictly confidential. It is to be ensured that there is no tipping off to the customer at any level.

6.4 Robust software.

Robust Software throwing alerts when the transactions are inconsistent with risk categorization and updated profile of the customers shall be put in to use as a part of effective identification and reporting of suspicious transactions.

6.5 Reports to be furnished to Financial Intelligence Unit-India

- (i) Cash Transaction Report [CTR].
- (ii) Suspicious Transactions Report [STR]
- (iii) Counterfeit Currency Report [CCR]
- (iv) Non Profit Organizations Transaction report [NTR]

(i). Cash Transactions Report [CTR]

- (i) Report of all cash transactions of the value of more than rupee ten lakhs or its equivalent in foreign currency and all series of cash transactions integrally

connected to each other which have been valued below rupees ten lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month and the aggregate value of such transaction exceeds Rupees ten lakh.

(ii) The CTR for each month will be submitted to FIU-IND by **15th of the succeeding month**.

(ii) Suspicious Transaction Reports (STR)

"**Suspicious transaction**" means a "transaction" as defined below, 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 the Act, 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.

STR Detection and Reporting Mechanism:

1. The alerts generated by the **AML software of the Bank i.e. Cobasys** shall be examined thoroughly by the branch to decide whether the transaction is suspicious or is genuine.

2. The alerts comprise of:

a. some **system driven alerts** generated by Cobasys;

b. Rest are **offline** based on functional classification such as account monitoring, customer due diligence, shell company identification, terrorist financing, transaction due diligence, fake and mutilated Indian currency notes etc.

These **offline Scenario** alerts are enclosed as "**Annexure I**".

3. The branch incumbents are advised to monitor all the alerts generated by the system and simultaneously monitor the transactions on the basis of offline scenarios as well.

In addition to this, all the transactions taking place in the branch, must be analyzed based on various **grounds of suspicion** as per **Annexure II**.

4. The primary responsibility for monitoring and reporting of suspicious transaction shall be of the branch. The monitoring of the transactions will also be done by controlling offices after , who will also interact with the branches to facilitate monitoring and reporting of suspicious transactions. Controlling offices shall monitor transactions in customer accounts, in general, and high risk accounts/ high value transactions, in particular.

5. The list of various types of alerts for the branches is given in **Annexure III**, further an illustrative list for various grounds of suspicion is annexed as **Annexure II**, as specified above.

6. The branch on being satisfied with the genuineness of the transaction shall close the alert with appropriate reasons, if not; the branch shall immediately report the STR to the Principal Officer/BRCTL cum Compliance Cell with a copy to MLRO.

Further, the Principal Officer, MLRO and BRCTL cum KYC & AML Compliance Cell at HO, will also coordinate with branches to facilitate monitoring of alerts and reporting of suspicious transactions.

- **Principal Officer-** officer nominated by the Bank as Principal Officer, designated at Head Office, for the purpose of KYC/AML compliance.
- **Money Laundering Reporting Officer (MLRO):** The District Managers are designated as MLRO of each District. MLRO will also send his opinion to the committee within 10 days from receipt of any Suspicious Transaction.
- **AML Cell:** The Centralized AML Cell shall coordinate with branch, MLRO & Principal Officer for effective reporting of Suspicious Transactions.

7. A committee of AGM (**AML Cell/BRCTL**), **Sr Mgr/Mgr (Vigilance)**, will analyze the reported STR and send their recommendation to the Principal Officer.

8. The decision to report/file an STR finally rests with the Principal Officer.

9. The total time frame from the **review of an alert till the submission of an STR must not exceed 60 days.** The Branch Manager, MLRO and AML Cell must initiate the review promptly and complete it in a reasonable amount of time not exceeding 60 days.

10. The STR will be filed by the **Centralized AML Cell** to FIU India **within 7 working days** of arriving at the conclusion that a transaction is suspicious.

11. If an STR gets reported the record of STR along with relevant documents needs to be maintained for a period of ten years, in the safe custody of the branch, from the date of filing the STR.

12. Alerts/Red Flag Alerts indication (Online/Offline) are confidential, hence shall be kept confidential and not to be disclosed to the customer.

(iii) Counterfeit Currency Report (CCR)

Cash transactions where forged or counterfeit currency notes have been used as genuine or where any forgery of a valuable security or document has taken place facilitating the transactions will be reported to Financial Intelligence Unit-India in the specified format by 15th of the succeeding month.

(iv) Non Profit Organizations Transaction report [NTR]

All transactions involving receipts by non-profit organizations of value more than rupees ten lakh or its equivalent in foreign currency, to be reported to the Director, Financial Intelligence Unit-India by the 15th of the succeeding month.

7. INTERNAL KYC MECHANISM AND STRUCTURE (ROLES AND RESPONSIBILITIES OF THE STAFF)

The newly constituted AML/KYC Cell has been designated for compliance of KYC Policy and to monitor and strengthen the internal control system for prevention of money laundering and combating financing of terrorism.

AML Cell is responsible for compliance of all the directions/guidelines issued by the Regulating Agencies i.e. FIU India, RBI & NABARD in respect of AML/KYC/CFT. Further, the latest amendments/additions in this regard are to be implemented by the staff posted under AML Cell. The KYC Policy shall be updated from time to time as per guidelines of RBI, other law enforcing agencies with the Board's approval.

In addition to AML Cell the following Officers shall coordinate and oversee the position of the Bank with respect to KYC:

- **Designated Director** will ensure compliance of the KYC/AML/CFT directions issued by the regulating authorities like RBI, NABARD, FIU from time to time.
- **Principal Officer** shall mandatorily be designated by the Bank, who shall be the administrative head of Centralized AML Cell. The PO shall play a vital role in the compliance of AML/KYC/CFT guidelines.
- The District Manager of each District shall act as **Money Laundering Reporting Officer (MLRO); for the purpose of reporting of Suspicious Transactions to the Principal Officer.**
- The **Branch Managers** shall be responsible for ensuring KYC compliance, Risk categorization and Periodic updation of accounts and monitoring of transactions with a view to report/identify Suspicious Transactions.
- **Audit Committee** of Executives will allow amendment in operational matters related to KYC and AML. The position of the Bank w.r.t. KYC shall be placed before the Audit Committee in its every meeting.

8. OBLIGATORY COMPLIANCES TO ACTS/LAWS

1. Requirements / Obligations under International Agreements-Communications from International Agencies

Obligations under the Unlawful Activities (Prevention) (UAPA) Act, 1967:

Bank shall ensure that in terms of Section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967 and amendments thereto, they do not have any account 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). The details of the two lists are as under:

(i) The "**ISIL (Da'esh) & Al-Qaida Sanctions List**", established and maintained pursuant to Security Council resolutions 1267 / 1989 / 2253, which includes names of individuals and entities associated with the Al-Qaida is available at:

<https://scsanctions.un.org/ohz5jen-al-qaida.html>

(ii) The "**Taliban Sanctions List**", established and maintained pursuant to Security Council resolution 1988 (2011), which includes names of individuals and entities associated with the Taliban is available at:

<https://scsanctions.un.org/3ppp1en-taliban.htm>

It must also be ensured to refer to the lists as available in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as amended from time to time. The aforementioned lists, i.e., UNSC Sanctions Lists and lists as available in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as amended from time to time, shall be verified on daily basis and any modifications to the lists in terms of additions, deletions or other changes shall be taken into account by all the offices for meticulous compliance.

2. Procedure for implementation Section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967

Details of accounts resembling any of the individuals/entities in the lists shall be reported to FIU- IND apart from advising Ministry of Home Affairs (MHA) as required under UAPA notification dated February 2, 2021.

3. Freezing of Assets under Section 51A of Unlawful Activities (Prevention) Act, 1967.

The procedure laid down in the UAPA Order dated February 2, 2021 (**Annexure-IV**) shall be strictly followed and meticulous compliance with the Order issued by the Government shall be ensured.

The list of Nodal Officers for UAPA is annexed as **Annexure VI** and is also available on the website of Ministry of Home Affairs

4. Obligations under Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act, 2005):

(a) Bank shall ensure meticulous compliance with the "Procedure for Implementation of Section 12A of the Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005" laid down in terms of Section 12A of the WMD Act, 2005 vide Order dated January 30, 2023, by the Ministry of Finance, Government of India

(b) In accordance with paragraph 3 of the aforementioned Order, Bank shall ensure not to carry out transactions in case the particulars of the individual / entity match with the particulars in the designated list.

(c) Further, Bank shall run a check, on the given parameters, at the time of establishing a relation with a customer and on a periodic basis to verify whether individuals and entities in the designated list are holding any funds, financial asset, etc., in the form of bank account, etc.

(d) In case of match in the above cases, the transaction details with full particulars of the funds, financial assets or economic resources involved, be immediately reported Centralised AML (CAML) Cell for onward submission of same to the **Central Nodal Officer (CNO)**, designated as the authority to exercise powers under Section 12A of the WMD Act, 2005. A copy of the communication shall be sent by the CAML Cell to State Nodal Officer, where the account / transaction is held and to the RBI. The CAML Cell shall file an STR with FIU-IND covering all transactions in the accounts, covered above, carried through or attempted.

It may be noted that in terms of Paragraph 1 of the Order, Director, FIU-India has been designated as the CNO.

(e) Bank may refer to the designated list, as amended from time to time, available on the portal of FIU-India.

(f) In case there are reasons to believe beyond doubt that funds or assets held by a customer would fall under the purview of clause (a) or (b) of sub-section (2) of Section 12A of the WMD Act, 2005, the concerned office shall prevent such individual/entity from conducting financial transactions and immediately inform to CAML Cell for their onward intimating the same to the CNO by email, FAX and by post, without delay.

(g) In case an order to freeze assets under Section 12A is received by the Bank from the CNO, the Bank shall, without delay, take necessary action to comply with the Order.

(h) The process of unfreezing of funds, etc., shall be observed as per paragraph 7 of the Order. Accordingly, copy of application received from an individual/entity

regarding unfreezing shall immediately be forwarded by the concerned office to CAML Cell with full details of the asset frozen, as given by the applicant, for their onward submission of the same to the CNO by email, FAX and by post, within two working days.

Bank shall verify every day, the 'UNSCR 1718 Sanctions List of Designated Individuals and Entities', as available at **<https://www.mea.gov.in/Implementation-of-UNSC-Sanctions-DPRK.htm>**, to take into account any modifications to the list in terms of additions, deletions or other changes and also ensure compliance with the 'Implementation of Security Council Resolution on Democratic People's Republic of Korea Order, 2017', as amended from time to time by the Central Government.

In addition to the above, Bank shall take into account – **(a)** other UNSCRs and **(b)** lists in the first schedule and the fourth schedule of UAPA, 1967 and any amendments to the same for compliance with the Government orders on implementation of Section 51A of the UAPA and Section 12A of the WMD Act.

5. Jurisdictions that do not or insufficiently apply the FATF Recommendations

a. FATF Statements circulated by Reserve Bank of India from time to time, and publicly available information, for identifying countries, which do not or insufficiently apply the FATF Recommendations, shall be considered. Risks arising from the deficiencies in AML/CFT regime of the jurisdictions included in the FATF Statement shall be taken into account.

b. Special attention shall be given to business relationships and transactions with persons (including legal persons and other financial institutions) from or in countries that do not or insufficiently apply the FATF Recommendations and jurisdictions included in FATF Statements.

Explanation: The process referred to in Section 38 a & b do not preclude Bank from having legitimate trade and business transactions with the countries and jurisdictions mentioned in the FATF statement.

c. The background and purpose of transactions with persons (including legal persons and other financial institutions) from jurisdictions included in FATF Statements and countries that do not or insufficiently apply the FATF Recommendations shall be examined, and written findings together with all documents shall be retained and shall be made available to Reserve Bank/ other relevant authorities, on request.

Banks are encouraged to leverage latest technological innovations and tools for effective implementation of name screening to meet the sanction requirements.

9. OTHER INSTRUCTIONS

9.1 Secrecy Obligations and Sharing of Information:

- a. Bank shall maintain secrecy regarding the customer information which arises out of the contractual relationship between the banker and customer.
- b. While considering the requests for data / information from Government and other agencies, Bank shall satisfy themselves that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy in the transactions.
- c. The exceptions to the said rule shall be as under:-
 - i. Where disclosure is under compulsion of law,
 - ii. Where there is a duty to the public to disclose,
 - iii. the interest of bank requires disclosure and
 - iv. Where the disclosure is made with the express or implied consent of the customer.
- d. Information collected from customers for the purpose of opening of account shall be treated as confidential and details thereof shall not be divulged for the purpose of cross selling, or for any other purpose without the express permission of the customer

9.2 CDD Procedure and sharing KYC information with Central KYC Records Registry (CKYCR)

- a. Government of India has authorized the Central Registry of Securitization Asset Reconstruction and Security Interest of India (CERSAI), to act as, and to perform the functions of the CKYCR vide Gazette Notification No. S.O. 3183(E) dated November 26, 2015.
- b. In terms of provision of Rule 9(1A) of PML Rules, the Bank has to capture Customer's KYC records and upload onto CKYCR within 10 days of commencement of an account-based relationship with the customer.
- c. Operational Guidelines for uploading the KYC data have been released by CERSAI.
- d. Bank shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as per the KYC templates prepared for 'Individuals' and 'Legal Entities' (LEs), as the case may be. The templates may be revised from time to time, as may be required and released by CERSAI.
- e. The 'live run' of the CKYCR started from July 15, 2016 in phased manner beginning with new 'individual accounts'. Accordingly, staff posted at AML Cell shall invariably upload the KYC data pertaining to all new individual accounts opened on or after January 1, 2017, with CKYCR. Bank was initially allowed time up to February 1, 2017, for uploading data in respect of accounts opened during January 2017.
- f. KYC records pertaining to accounts of LEs opened on or after April 1, 2021 have to be uploaded, with CKYCR in terms of the provisions of the Rules *ibid*. The KYC records have to be uploaded as per the LE Template released by CERSAI.
- g. Once KYC Identifier is generated by CKYCR, it is to be ensured that the same is

communicated to the individual/LE as the case may be.

h. In order to ensure that all KYC records are incrementally uploaded on to CKYCR, the branches shall upload/update the KYC data pertaining to accounts of individual customers and LEs opened prior to the above mentioned dates as per (e) and (f) respectively at the time of periodic updation as specified in Section 19 of this KYC Policy, or earlier, when the updated KYC information is obtained/received from the customer.

i. it is to be ensured that during periodic updation, the customers are migrated to the current CDD standard.

j. Where a customer, for the purposes of establishing an account based relationship, submits a KYC Identifier to the Bank, with an explicit consent to download records from CKYCR, then AML Cell shall retrieve the KYC records online from the CKYCR using the KYC Identifier and the customer shall not be required to submit the same KYC records or information or any other additional identification documents or details, unless —

(i) there is a change in the information of the customer as existing in the records of CKYCR;

(ii) the current address of the customer is required to be verified;

(iii) the Bank considers it necessary in order to verify the identity or address of the customer, or to perform Enhanced Due Diligence (EDD) or to build an appropriate risk profile of the client;

(iv) the validity period of documents downloaded from CKYCR has lapsed.

9.3. Period for presenting payment instruments

Payment of cheques / drafts / pay orders / banker's cheques, if they are presented beyond the period of three months from the date of such instruments, shall not be made.

9.4. Introduction of New Technologies

Identification and assessment of ML/FT risk shall be done by the Bank 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 pre-existing products.

Further, Bank shall ensure:

a. to undertake the ML/TF risk assessments prior to the launch or use of such products, practices, services, technologies; and

b. adoption of a risk-based approach to manage and mitigate the risks through appropriate EDD measures and transaction monitoring, etc.

9.5. Issue and Payment of Demand Drafts, etc.

Any remittance of funds by way of demand draft, mail / telegraphic transfer / NEFT/

IMPS or any other mode and issue of travelers' cheques for value of rupees fifty thousand and above shall be effected by debit to the customer's account or against cheques and not against cash payment.

Further, the name of the purchaser shall be incorporated on the face of the demand draft, pay order, banker's cheque, etc., by the issuing bank. These instructions shall take effect for such instruments issued on or after September 15, 2018.

9.6 Quoting of PAN

Permanent account number (PAN) or equivalent e-document thereof of customers shall be obtained and verified while undertaking transactions as per the provisions of Income Tax Rule 114B applicable to banks, as amended from time to time. Form 60 shall be obtained from persons who do not have PAN or equivalent e-document thereof.

9.7 Issuance of Prepaid Payment Instruments (PPIs):

It is to be ensured that the instructions issued by Department of Payment and Settlement System of Reserve Bank of India through their Master Direction are strictly adhered to.

9.8 Hiring of Employees and Employee training

a. Adequate screening mechanism, including Know Your Employee / Staff Policy, as an integral part of their personnel recruitment/ hiring process shall be put in place.

b. Bank shall ensure that the staff dealing with / being deployed for KYC/AML/CFT matters have: high integrity and ethical standards, good understanding of extant KYC/AML/CFT standards, effective communication skills and ability to keep up with the changing KYC/AML/CFT landscape, nationally and internationally. Bank shall also strive to develop an environment which fosters open communication and high integrity amongst the staff.

c. On-going employee training programme shall be put in place so that the members of staff are adequately trained in AML / CFT policy. The focus of the training shall be different for frontline staff, compliance staff and staff dealing with new customers. The front desk staff shall be specially trained to handle issues arising from lack of customer education. Proper staffing of the audit function with persons adequately trained and well-versed in AML/ CFT policies of the Bank, regulation and related issues shall be ensured.

9.9 Account Number Portability: The customers have the option to transfer their account from one branch to another without changing their account number.

The following procedure shall be followed in case of Account Number Portability:

1. Customer would visit in person either in the parent branch or the branch where account is to be transferred to request for account transfer and submit the written application to the branch.
2. Customer ID would remain with the parent branch; only account number would be transferred. Only operative accounts would be eligible for portability and the account must be c-KYC compliant.
3. The branch where account had been transferred would obtain the fresh KYC documents only in case of change of address or other demographic details along with the account opening form.
4. Only saving/current account would be transferred.

9.10 E-KYC: It is the process of verifying a customer's identity and address digitally via Aadhaar authentication. In other words, E-KYC verification is done through a digital mode, and there is no need for physical documentation. E-KYC is backed by biometric verification, making it very safe and secure.

The Bank envisages implementing E-KYC in the Bank and is in the process of obtaining membership from UIDAI, being a pre-requisite for starting E-KYC. The detailed procedure in respect of E-KYC shall be separately shared with all concerned as and when the same is implemented.

ANNEXURE I

LIST OF OFFLINE ALERTS

Sr. No.	Functional Classification	Alert Indicator	Indicative Rule/Scenario	Source of Alert	Guidance/Directi ons
1		Routing of funds through multiple accounts	Transactions greater than INR [1,00,000] between more than [20] accounts in the same bank aggregating to more than [20,00,000] on the same day	Typology	Branches shall monitor closely the transaction greater than abnormal and high value between multiple accounts on same day in individual accounts.
2	Account Monitoring	Reg. NGOs	<p>a) Any person receiving foreign contribution in its account [not designated as FCRA (foreign contribution regulation act) account] or without obtaining prior permission from MHA. [Banks to update this list as per Orders issued by RBI (as advised by MHA) from time to time].</p> <p>b) Transfers from a FCRA-designated account of a registered person to a Non-FCRA designated account of another person;</p> <p>c) Receipt of</p>	Typology	Note: Any breach of these RFIs should be reported as STRs by banks. Further instructions given from time to time in this regard in the bank be strictly followed by branches.

			foreign contribution for credit to any person in India, sent by donor agencies mentioned under 'Prior Reference Category' without prior permission from MHA. [Banks to update this list as per Orders issued by RBI (as advised by MHA) from time to time]		
3	Account Monitoring	Reg. NGOs	Receipt of funds in account of an NGO or payments from account of an NGO which is not in line with stated activity or purpose of NGO.	Typology	Self-explanatory
4	Afghan Drug Business	Students from other countries (having Afghan nationality) staying in India, maintaining more than one account and generating cash more than INR 10 lakh in a year	Students from other countries (having Afghan nationality) staying in India, maintaining more than one account and generating cash more than INR 10 lakh in a year	Typology	Self explanatory
5		Customer left without opening account	Customer did not open account after being informed about KYC	Customer Verification	Self explanatory

			requirements		
6	Customer Due Diligence	Customer offered false or forged identification/address documents	Customer gives false identification/address documents or documents that appear to be counterfeited, altered and inaccurate	Customer Verification	Self explanatory
7		Address found to be nonexistent or wrong	Address provided by the customer is found to be nonexistent or wrong	Customer Verification	Self explanatory
8		Difficult to identify beneficial owner	Customer uses complex legal structures or where it is difficult to identify the beneficial owner	Customer Verification	Self explanatory
9		Multiple accounts by individual customer/company under various heads in a single branch	Same Directors/authorized signatories/partners of a company, LLP or partnership open multiple accounts in the same branch without proper rationale	Customer Verification	Self explanatory
10		Customer is being investigated for criminal offences	Customer has been the subject of inquiry from any law enforcement agency relating to criminal offences	Law Enforcement Agency Query	Self explanatory
11		Customer is being investigated for TF	Customer has been the subject of inquiry from any law enforcement	Law Enforcement Agency Query	Self explanatory

	Customer Due Diligence	offences	agency relating to TF or terrorist activities		
12		Adverse media report about criminal activities of customer	Match of customer details with persons reported in local media/open source for criminal offences	Media Reports	Self explanatory
13		Adverse media report about TF or terrorist activities of customer	Match of customer details with persons reported in local media/open source for terrorism or terrorist financing related activities	Media Reports	Self explanatory
14		Customer did not complete transaction	Customer did not complete transaction after queries such as source of funds etc.	Employee Initiated	Self explanatory
15		Customer is nervous or over cautious	Customer is hurried or nervous/over cautious in explaining genuineness of the transaction	Employee Initiated	Self explanatory
16		Customer provides inconsistent information	Customer changes the information provided after more detailed information is requested. Customer provides information that seems minimal, possibly false or inconsistent.	Employee Initiated	Self explanatory
17		Customer acting on behalf of a third party	Customer has vague or no knowledge about the transaction(s) in his/her account; or, customer is	Employee Initiated	Self explanatory

	Customer Due Diligence		taking instructions from a third party for conducting transactions of which he/she is not aware of		
18		Multiple customers working as a group	Multiple customers arrive together but pretend to ignore each other	Employee Initiated	Self explanatory
19		Customer avoiding nearer branches	Customer travels unexplained distances to open account or conduct transactions	Employee Initiated	Self explanatory
20		Customer wants to avoid reporting	Customer makes inquiries or tries to convince staff to avoid reporting	Employee Initiated	Self explanatory
21		Customer could not explain source of funds	Customer could not explain source of funds satisfactorily	Employee Initiated	Self explanatory
22		Complaint received from public	Complaint received from public for abuse of account for committing fraud etc.	Public Complaint	Self explanatory
23		Alert raised by other agents/subsidiaries/as sociates/other institutions	Alert raised against the customer by employed agents, business associates, overseas branches, subsidiaries, other institutions or correspondent banks	Business Associates	Complaint, Adverse news or Referral against a Customer of the member bank
24		Availing loan facility/ OD (Overdraft) facility against	Fraudsters hand over counterfeit FDR to investor and subsequently within span of few days avail loan/OD	Typology	This scenario is applicable for all customers and constitutions types.

		FDR (Fixed Deposit Receipt) within few days of creation	facility against original FDR and other forged documents		
25	Customer Due Diligence	Customer providing different details to avoid linkage	Customer provided different IDs or Email id, mobile number or Date of Birth at different instances	Typology	Self explanatory
26		Multiple customers working together	Accounts opened by multiple unrelated customers linked by a common PAN, address, mobile number or email address	Typology	Self explanatory
27		Transacting parties appear to be affiliated, conduct business out of a residential address or provide only a registered agent's address	Transacting parties appear to be affiliated, conduct business out of a residential address or provide only a registered agent's address	Typology	Self explanatory
28	Locker Operations Monitoring	Frequent Locker operations	Number of locker operations greater than [10] times in [30] days	Employee Initiated	Branches shall closely monitor frequent locker operations done by individual more than normal.
29	Shell Company Identification	Generally no physical presence	Generally no physical presence (other than a	Typology	Self explanatory

		(other than a mailing address)	mailing address)		
30		Directors are persons of very low means - individually they have nil or low net worth and do not have any substantial source of income	Directors are persons of very low means - individually they have nil or low net worth and do not have any substantial source of income	Typology	Self explanatory
31		Payments have no stated purpose, do not have reference to goods or services, or identify only a contract or invoice number	Payments have no stated purpose, do not have reference to goods or services, or identify only a contract or invoice number	Typology	The examination of the Invoice be done properly.
32		Transacting businesses i.e. entities doing business with the company share the same address or there are address	Transacting businesses i.e. entities doing business with the company share the same address or there are address related inconsistencies	Typology	Self explanatory

		related inconsistencies			
33		Funds are transferred from the company to an unusually large number and different kind of beneficiaries (from different sectors/businesses)	Funds are transferred from the company to an unusually large number and different kind of beneficiaries (from different sectors/businesses)	Typology	Such type of transactions be closely monitored and reported accordingly by branches.
34	Shell Company Identification	Little or no withdrawal from account for business purposes/ no recurrent business expenses	Little or no withdrawal from account of a company for business purposes/ no recurrent business expenses	Typology	Self-explanatory
35	Sell Company Identification	Rotation of funds between account of companies having same authorized signatory	Transfer of funds between account of companies having nominal authorized share capital and having same authorized signatory	Typology	Self-explanatory
36	Terrorist Financing	Transaction involving a location with terrorist incident	Transaction involving a location prior to or immediately after a terrorist incident	Typology	Note: 1) Proactive monitoring to be conducted by banks in the wake of major terrorist

					<p>incidents ("incidents") in locations where they operate.</p> <p>2) Banks to review all transaction monitoring alerts generated on transactions involving their branches in the specific location, especially alerts which were earlier closed as 'non-suspicious'. This due diligence exercise should be undertaken for a period commencing one month immediately preceding the date of the incident, upto the date of conducting such due diligence.</p>
37	Trade Based Money Laundering	Booking of ticket abroad and subsequent cancelling and payment made to third party.	High value remittances for frequent ticket/tour packages booked by tour operators	Typology	Note: Trigger relevant for the transactions by Tours and Travel operators. To be considered as part of the checklist during transaction monitoring due diligence.
38		A customer deviates significantly from its historical pattern of	A customer deviates significantly from its historical pattern of trade activity (i.e. in terms of markets,	Typology	Self explanatory

		trade activity (i.e. in terms of markets, monetary value, frequency of transactions, volume, or merchandise type)	monetary value, frequency of transactions, volume, or merchandise type)		
39	Transaction Due Diligence	Transaction is unnecessarily complex	Transaction is unnecessarily complex for its stated purpose	Employee Initiated	Self explanatory
40		Transaction has no economic rationale	The amounts or frequency or the stated reason of the transaction does not make sense for the particular customer	Employee Initiated	Self explanatory
41		Transaction inconsistent with business	Transaction involving movement of funds which is inconsistent with the customer's business	Employee Initiated	Self explanatory
42	FICN	Transaction(s) involving Fake Indian Currency Notes (FICN)	FICNs attempted to be deposited in single/multiple accounts of the customer, greater than [5] FICN notes in a month	Transaction monitoring	In implementing this RFI, banks need to consider only the number of FICN notes which have been detected in a month for the same customer. Note: Details of FICN to be provided by banks in the transaction

					file of the STR.
43	FICN	Transaction(s) involving Fake Indian Currency Notes (FICN)	FICNs attempted to be deposited in single/multiple accounts of the customer, aggregating to greater than INR [25000] value in a month	Transaction monitoring	Note: Details of Fake Indian Currency Notes (FICN) to be provided by banks in the transaction file of the STR.



44	Mutilated Indian Currency Notes	Transaction(s) involving mutilated Indian Currency Notes	Customer/non-account holder attempts to deposit, exchange or adjudicate mutilated Indian Currency Notes at a Bank's branch or currency chest, aggregating to greater than INR [5000] value in a month	Transaction monitoring	As per RBI, a mutilated note is a note of which a portion is missing or which is composed of more than two pieces. Such notes may be presented at any of the bank branches and shall be accepted, exchanged and adjudicated in accordance with the Reserve Bank of India (Note Refund) Rules, 2009 as circulated in bank vide H.O.G.C no. 27/2021-22 dated 16 th June 2021.
----	---------------------------------	--	---	------------------------	--

ANNEXURE II

ILLUSTRATIVE LIST OF GROUNDS OF SUSPICION REPORTED IN STRS

Sr. No.	Suspicion	Summary of detection and review
1	False identity	Identification documents were found to be forged during customer verification process. The accountholder was not traceable.
2	Wrong address	Welcome pack was received back as the person had furnished incorrect or false details or was not staying at the given address. or address details given by the accountholder were found to be false. The accountholder was not traceable.
3	Doubts over the real beneficiary of the account	The customer not aware of the transactions in his/her account. Transactions were inconsistent with the customer's profile.
4	Account of persons under investigation	The customer was reported in media for being under investigation
5	Account of wanted criminal	Name of the accountholder and additional criteria (date of birth/ father's name/ nationality) were same as a person on the watch list of UN, Interpol, etc
6	Account used for cyber crime	Complaints of cybercrime were received against the customer. No valid explanation for the transactions was furnished by the accountholder.
7	Account used for lottery fraud	Complaints were received against a particular bank account that was used for receiving money from the victims. Deposits at multiple locations followed by immediate withdrawals using ATMs. No valid explanation provided by the accountholder.
8	Doubtful activity of a customer from high risk country	Cash deposited in a bank account at different cities on the same day. The accountholder is a citizen of a high risk country with known cases of drug trafficking.
9	Unexplained transfers between multiple accounts	Large number of related accounts with substantial inter- account transactions without any economic rationale.
10	Unexplained activity in dormant accounts	Sudden spurt of activity in a dormant account. The customer could not provide satisfactory explanation for the transactions.
11	Unexplained activity in account inconsistent with the declared business	Transactions in an account inconsistent with what would be expected from declared business. The customer could not provide valid explanation.

12	Unexplained large value transaction inconsistent with client's apparent financial standing	Large value transactions in an account which usually has small value transactions. No valid explanation provided by the account holder.
13	Suspicious use of ATM Card	Frequent cash deposits in the account followed by ATM withdrawals at different locations. No valid explanation.
14	Doubtful use of safe deposit locker	Safe deposit locker operated frequently though the financial status of client did not match.
15	Doubtful source of cash deposited in bank account	Frequent cash transactions of value just under the reporting threshold. Cash transactions split across accounts to avoid reporting. No valid explanation provided.
16	Suspicious cash withdrawal from bank account	Large value cheques deposits followed by immediate cash withdrawals.
17	Misappropriation of funds	Reports of misappropriation of funds. Substantial cash withdrawals in account of charitable organizations.

ANNEXURE III**LIST OF VARIOUS TYPES OF ALERTS FOR BRANCHES****I. Customer Behavior Indicators**

- ❖ Customers who are reluctant to provide basic information while opening an account; providing minimal or fictitious information or when applying to open an account; providing information that is difficult or expensive for the institution to verify.
- ❖ Customer expressing unusual curiosity to maintain secrecy of the transaction.
- ❖ Customers who decline to provide information that in normal circumstances would make the customer eligible for banking services.
- ❖ Customers who are reluctant or refuses to state a purpose of a particular large/complex transaction/source of funds involved or provides a questionable purpose and/or source.
- ❖ Customers who use separate tellers to conduct cash transaction or foreign exchange transactions.
- ❖ Customers who deposit cash/withdrawals by means of numerous deposit slips/cheque leaves so that the total of each deposit is unremarkable, but the total of all credits / debits is significant.
- ❖ Customer representatives avoiding contact with the branch.
- ❖ Customers who repay the problem loans unexpectedly.
- ❖ Customers who appear to have accounts with several institutions within the samelocality without any apparent logical reason.
- ❖ Customers seek to change or cancel a transaction after the customer is informed of currency transaction reporting/information verification or record keeping requirements relevant to the transaction.
- ❖ Customers who regularly issue large value cheques without balance and then deposit cash.

ANNEXURE IV

INDICATIVE RISK CATEGORISATION OF CUSTOMERS

High Risk Customers

1. Individuals and entities in various United Nations Security Council Resolutions (UNSCRs), such as UN 1267 etc.
2. Individuals or entities listed in the schedule to the order under section 51A of the Unlawful Activities (Prevention) Act, 1967 relating to the purposes of prevention of and for coping with terrorist activities.
3. Individuals and entities in watch lists issued by Interpol and other similar international organizations.
4. Customers with dubious reputation as per public information available or commercially available watch lists.
5. Individuals and entities specifically identified by regulators, FIU and other competent authorities as high-risk.
6. Customers conducting their business relationship or transaction in unusual circumstances, such as significant and unexplained geographic distance between the institution and the location of the customer, frequent and unexplained movement of accounts to different institutions in various geographic locations, etc.
7. Customers based in high risk countries/jurisdictions or locations.
8. Politically Exposed Persons (PEPs) of foreign origin, customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner;
9. Non-resident customers and foreign nationals
10. Embassies/Consulates
11. Off-shore (foreign) corporation/business
12. Non face-to-face customers
13. High net worth individuals
14. Partnership Firms
15. Firms with 'sleeping partners'
16. Walk-in Customers
17. Companies having close family share-holding or beneficial ownership
18. Complex business ownership structures, which can make it easier to conceal underlying beneficiaries, where there is no legitimate commercial rationale
19. Shell companies which have no physical presence in the country in which it is incorporated. The existence simply of a local agent or low level staff does not constitute physical presence.
20. Investment Management/Money Management Company/ Personal Investment Company

21. Accounts for “gatekeepers’ such as accountants, lawyers, or other professionals for their clients where the identity of the underlying client is not disclosed to the financial institution.
22. Client Accounts managed by professional service providers such as law firms, accountants, agents, brokers, fund managers, trustees, custodians, etc.
23. Trusts, charities, NGOs/NPOs (those operating on a “cross-border’ basis) unregulated clubs and organizations receiving donations (excluding NPOs/NGOs promoted by United Nations or its agencies)
24. Money service Business, including seller of Orders/ Travellers Checks/ Money Transmission/ Check Cashing/ Dealing or Exchange
25. Business accepting third party cheque (except supermarkets or retail stores that accept payroll cheque/ cash payroll cheque)
26. Gambling/gaming, including “junket Operators” arranging gambling tours
27. Dealers in high value or precious goods (e.g. jewel, gem and precious metals dealers, art and antique dealers and auction houses, estate agents and real estate brokers).
28. Customers engaged in a business which is associated with higher levels of corruption (e.g. arms manufacturers, dealers and intermediaries)
29. Customers engaged in industries that might relate to nuclear proliferation activities or explosives.
30. Customers that may appear to be Multi-level marketing companies etc.
31. Accounts of Jewelers.

Medium Risk Customers

1. Non-Bank Financial Institution
2. Stockbrokerage
3. Import/Export
4. Gas Station
5. Car/Boat/Plane Dealership
6. Electronics (wholesale)
7. Travel agency
8. Used car sales
9. Telemarketers
10. Providers of telecommunications service, internet café, IDD call service, phone cards, phone centre
11. Dot-com company or internet business
12. Pawnshops
13. Auctioneers
14. Cash-intensive Businesses such as restaurants, retail shops, parking garages, fast food stores, movie theatres, etc.
15. Sole Practitioners or Law firms (small, little known)

16. Notaries (small, little known)
17. Secretarial (small, little known)
18. Accountants (small, little known)
19. Venture capital companies.

Low Risk Customers

1. Individuals (Other than included in High and Medium Risk categories above)
2. Government departments and Government owned Companies, regulatory and statutory bodies
3. Non-Profit Organisations/Non-Government Organisations promoted by United Nations or its agencies
4. All other categories of accounts/customers not falling under the above indicated High and Medium Risk classifications

ANNEXURE V

Procedure for Implementation of Sec 12A of “The Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005

Attention is drawn to Section 12A of Weapons of Mass Destruction and Their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005

1. In this regard, it is conveyed that Department of Revenue has issued an order (F. No. P-12011/14/2022-ES Cell-DOR) dated September 1, 2023, in respect of implementation of the provisions of said section. The order may be found enclosed with the present alert. The order may also be found on the FIU-INDIA website at the URL below,

https://fiuindia.gov.in/pdfs/AML_legislation/DoR_Section_12A_WMD.pdf

2. Reporting entities are advised to take note and ensure strict adherence to the provisions of section 12A of WMD Act, 2005 and Department of Revenue Order No. F. No. P-12011/14/2022-ES Cell-DOR dated September 01, 2023.

F.No.P-12011/14/2022-ES Cell-DOR
Government of India
Ministry of Finance
Department of Revenue

New Delhi, dated the 1st September, 2023.

ORDER

Subject: - Procedure for implementation of Section 12A of "The Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005".

Section 12A of The Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 [hereinafter referred to as 'the Act'] reads as under: -

"12A. (1) No person shall finance any activity which is prohibited under this Act, or under the United Nations (Security Council) Act, 1947 or any other relevant Act for the time being in force, or by an order issued under any such Act, in relation to weapons of mass destruction and their delivery systems.

(2) For prevention of financing by any person of any activity which is prohibited under this Act, or under the United Nations (Security Council) Act, 1947 or any other relevant Act for the time being in force, or by an order issued under any such Act, in relation to weapons of mass destruction and their delivery systems, the Central Government shall have power to—

- a) 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;

prohibit any person from making funds, financial assets or economic resources or related services available for the benefit of persons related to any activity which is prohibited under this Act, or under the United Nations (Security Council) Act, 1947 or any other relevant Act for the time being in force, or by an order issued under any such Act, in relation to weapons of mass destruction and their delivery systems

(3) The Central Government may exercise its powers under this section through any authority who has been assigned the power under sub-section (1) of section 7."

II. In order to ensure expeditious and effective implementation of the provisions of Section 12A of the Act, the procedure is outlined below.

1. Appointment and communication details of Section 12A Nodal Officers:

1.1 In exercise of the powers conferred under Section 7(1) of the Act, the Central Government assigns Director, FIU-India, Department of Revenue, Ministry of Finance, as the authority to exercise powers under Section 12A of the Act. The Director, FIU-India shall be hereby referred to as the Central Nodal Officer (CNO) for

the purpose of this order. [Telephone Number: 01123314458, 011- 23314435, 011-23314459 (FAX), email address: dir@fiuindia.gov.in].

1.2 **Regulator** under this order shall have the same meaning as defined in Rule 2(fa) of Prevention of Money-Laundering (Maintenance of Records) Rules, 2005. **Reporting Entity (RE)** shall have the same meaning as defined in Section 2 (1) (wa) of Prevention of Money- Laundering Act, 2002. DNFPBs is as defined in section 2(1) (sa) of Prevention of Money-Laundering Act, 2002.

1.3 The Regulators, Ministry of Corporate Affairs and Foreigners Division of MHA shall notify a Nodal Officer for implementation of provisions of Section 12A of the Act. The Regulator may notify the Nodal Officer appointed for implementation of provisions of Section 51A of UAPA, also, as the Nodal Officer for implementation of Section 12A of the Act. All the States and UTs shall notify a State Nodal officer for implementation of Section 12A of the Act. A State/UT may notify the State Nodal Officer appointed for implementation of provisions of Section 51A of UAPA, also, as the Nodal Officer for implementation of Section 12A of the Act.

1.4 The CNO shall maintain an updated list of all Nodal Officers, and share the updated list with all Nodal Officers periodically. The CNO shall forward the updated list of all Nodal Officers to all REs.

Communication of the lists of designated individuals/entities:

2.1 The Ministry of External Affairs will electronically communicate, without delay, the changes made in the list of designated individuals and entities (hereinafter referred to as 'designated list') in line with Section 12A (1) to the CNO and Nodal officers.

2.1.1 Further, the CNO shall maintain the Designated list on the portal of FIU- India. The list would be updated by the CNO, as and when it is

updated, as per para 2.1 above, without delay. It shall make available for all Nodal officers, the State Nodal Officers, and to the Registrars performing the work of registration of immovable properties, either directly or through State Nodal Officers, without delay.

2.1.2 The Ministry of External Affairs may also share other information relating to prohibition / prevention of financing of prohibited activity under Section 12A (after its initial assessment of the relevant factors in the case) with the CNO and other organizations concerned, for initiating verification and suitable action.

2.1.3 The Regulators shall make available the updated designated list, without delay, to their REs. The REs will maintain the designated list and update it, without delay, whenever changes are made as per para 2.1 above.

2.2 The Nodal Officer for Section 12A in Foreigners Division of MHA shall forward the updated designated list to the immigration authorities and security agencies, without delay.

3. Regarding funds, financial assets or economic resources or related services held in the form of bank accounts, stocks or insurance policies, etc.

3.1 All Financial Institutions shall —

i. Verify if the particulars of the entities/individual, party to the financial transactions, match with the particulars of designated list and in case of match, REs shall not carry out such transaction and shall immediately inform the transaction details with full particulars of the funds, financial assets or economic resources involved to the CNO by email, FAX and by post, without delay.

ii. Run a check, on the given parameters, at the time of establishing a relation with a customer and on a periodic basis to verify whether individuals and entities in the designated list are holding any funds, financial assets or economic resources or related services, in the form of bank accounts, stocks, Insurance policies etc. In case, the particulars of any of their customers match with the particulars of designated list, REs shall immediately inform full particulars of the funds, financial assets or economic resources or related services held in the form of bank accounts, stocks or insurance policies etc., held on their books to the CNO by email, FAX and by post, without delay.

iii. The REs shall also send a copy of the communication, mentioned in 3.1 (i) and (ii) above, to State Nodal Officer, where the account/transaction is held, and to their Regulator, as the case may be, without delay.

iv. In case there are reasons to believe beyond doubt that funds or assets held by a customer would fall under the purview of clause (a) or (b) of sub-section (2) of Section 12A, REs shall prevent such individual/entity from conducting financial transactions, under intimation to the CNO by email, FAX and by post, without delay.

3.2 On receipt of the particulars, as referred to in Paragraph 3.1 above, the CNO would cause a verification to be conducted by the State Police and/or the Central Agencies so as to ensure that the individuals/entities identified by the REs are the ones in designated list and the funds, financial assets or economic resources or related services, reported by REs are in respect of the designated individuals/entities. This verification would be completed expeditiously from the date of receipt of such particulars.

3.3 In case, the results of the verification indicate that the assets are owned by, or are held for the benefit of, the designated individuals/entities, an order to freeze these assets under Section 12A would be issued by the CNO without delay and be conveyed electronically to the concerned RE under intimation to respective Regulators. The CNO shall also forward a copy thereof to all the Principal Secretaries/Secretaries, Home Department of the States/UTs and All Nodal officers in the country, so that any individual or entity may be prohibited from making any funds, financial assets or economic resources or related services available for the benefit of the designated individuals / entities. The CNO shall also forward a copy of the order to all Directors General of Police/ Commissioners of Police of all States/UTs for initiating suitable action.

3.4 The order shall be issued without prior notice to the designated individual/entity.

4. Regarding financial assets or economic resources of the nature of immovable properties:

- 4.1 The Registrars performing work of registration of immovable properties shall --
- i. Verify if the particulars of the entities/individual, party to the transactions, match with the particulars of the designated list, and, in case of match, shall not carry out such transaction and immediately inform the details with full particulars of the assets or economic resources involved to the State Nodal Officer, without delay.
 - ii. Verify from the records in their respective jurisdiction, without delay, on given parameters, if the details match with the details of the individuals and entities in the designated list. In case, the designated individuals/entities are holding financial assets or economic resources of the nature of immovable property, and if any match with the designated individuals/entities is found, the Registrar shall immediately inform the details with full particulars of the assets or economic resources involved to the State Nodal Officer, without delay.
 - iii. In case there are reasons to believe beyond doubt that assets that are held by an individual/entity would fall under the purview of clause (a) or (b) of sub-section (2) of Section 12A, Registrar shall prevent such individual/entity from conducting transactions, under intimation to the State Nodal Officer by email, FAX and by post, without delay.
- 4.2 The State Nodal Officer would cause communication of the complete particulars of such individual/entity along with complete details of the financial assets or economic resources to the CNO without delay by email, FAX and by post.
- 4.3 The State Nodal Officer may cause such inquiry to be conducted by the State Police so as to ensure that the particulars sent are indeed of these designated individuals/entities. This verification shall be completed without delay and shall be conveyed, within 24 hours of the verification, if it matches, with the particulars of the designated individual/entity, to the CNO without delay by email, FAX and by post.
- 4.4 The CNO may also have the verification conducted by the Central Agencies. This verification would be completed expeditiously.
- 4.5 In case, the results of the verification indicate that the assets are owned by, or are held for the benefit of, the designated individuals/entities, an order to freeze these assets under Section 12A would be issued by the CNO without delay and be conveyed electronically to the concerned Registrar performing the work of registering immovable properties, and to FIU under intimation to the concerned State Nodal Officer. The CNO shall also forward a copy thereof to all the Principal Secretaries/Secretaries, Home Department of the States/UTs and All Nodal officers in the country, so that any individual or entity may be prohibited from making any funds, financial assets or economic resources or related services available for the benefit of the designated individuals / entities. The CNO shall also forward a copy of the order to all Directors General of Police/ Commissioners of Police of all States/UTs for initiating suitable action.
- 4.6 The order shall be issued without prior notice to the designated individual/entity.
5. Regarding the real-estate agents, dealers of precious metals/stones

(DPMS), Registrar of Societies/ Firms/ non-profit organizations, The Ministry of Corporate Affairs and Designated Non-Financial Businesses and Professions (DNFBPs):

(i) The dealers of precious metals/stones (DPMS) as notified under PML (Maintenance of Records) Rules, 2005 and Real Estate Agents, as notified under clause (vi) of Section 2(1) (sa) of Prevention of Money-Laundering Act, 2002, are required to ensure that if any designated individual/entity approaches them for sale/purchase of precious metals/stones/Real Estate Assets or attempts to undertake such transactions, the dealer should not carry out such transaction and, without delay, inform the Section 12A Nodal officer in the Central Board of Indirect Taxes and Customs (CBIC). Also, If the dealers hold any assets or funds of the designated individual/entity, they shall freeze the same without delay and inform the Section 12A Nodal officer in the CBIC, who will, in turn, follow procedure similar to as laid down for State Nodal Officer in the paragraphs 4.2 to 4.6.

ii. Registrar of Societies/ Firms/ non-profit organizations are required to ensure that if any designated individual/ entity is a shareholder/ member/ partner/ director/ settler/ trustee/ beneficiary/ beneficial owner of any society/ partnership firm/ trust/ non-profit organization, then the Registrar shall freeze any transaction for such designated individual/ entity and shall inform the State Nodal Officer, without delay, and, if such society/ partnership firm/ trust/ non-profit organization holds funds or assets of designated individual/ entity, follow the procedure as laid down for State Nodal Officer in the paragraphs 4.2 to 4.6 above. The Registrar should also ensure that no societies/ firms/ non-profit organizations should be allowed to be registered if any of the designated individual/ entity is a director/ partner/ office bearer/ trustee/ settler/ beneficiary or beneficial owner of such juridical person and, in case, such request is received, then the Registrar shall inform the State Nodal Officer, without delay.

iii. The State Nodal Officer shall also advise appropriate department of the State/UT, administering the operations relating to Casinos, to ensure that the designated individuals/ entities should not be allowed to own or have beneficial ownership in any Casino operation. Further, if any designated individual/ entity visits or participates in any game in the Casino or if any assets of such designated individual/ entity are with the Casino operator, or if the particulars of any client match with the particulars of designated individuals/ entities, the Casino owner shall inform the State Nodal Officer, without delay, and shall freeze any such transaction.

iv. The Ministry of Corporate Affairs shall issue an appropriate order to the Institute of Chartered Accountants of India, Institute of Cost and Works Accountants of India and Institute of Company Secretaries of India (ICSI), requesting them to sensitize their respective members to the provisions of Section 12A, so that, if any designated individual/entity approaches them, for entering/ investing in the financial sector and/or immovable property, or they are holding or managing any assets/ resources of designated individual/ entities, then the member shall convey the complete details of such designated individual/ entity to Section 12A Nodal Officer in the Ministry of Corporate Affairs, who shall in turn follow the similar procedure as laid down for State Nodal Officer in paragraph 4.2 to 4.6 above.

v. The members of these institutes should also be sensitized by the Institute of

Chartered Accountants of India, Institute of Cost and Works Accountants of India and Institute of Company Secretaries of India (ICSI) that if they have arranged for or have been approached for incorporation/ formation/ registration of any company, limited liability firm, partnership firm, society, trust, association where any designated individual/ entity is a director/ shareholder/ member of a company/ society/ association or partner in a firm or settler/ trustee or beneficiary of a trust or a beneficial owner of a juridical person, then the member of the institute should not incorporate/ form/ register such juridical person and should convey the complete details of such designated individual/ entity to Section 12A Nodal Officer in the Ministry of Corporate Affairs.

vi. In addition, a member of the ICSI shall, if he/she is Company Secretary or is holding any managerial position where any of designated individual/ entity is a Director and/or Shareholder or having beneficial ownership of any such juridical person, convey the complete details of such designated individual/ entity to Section 12A Nodal Officer in the Ministry of Corporate Affairs, who shall follow the similar procedure as laid down in paragraph 4.2 to 4.6 above for State Nodal Officer, if such company, limited liability firm, partnership firm, society, trust, or association holds funds or assets of the designated individual/entity.

vii. In case any designated individual/ entity is a shareholder/ director/ whole time director in any company registered with the Registrar of Companies (ROC) or beneficial owner of such company or partner in a Limited Liabilities Partnership Firm registered with ROC or beneficial owner of such firm, the ROC should convey the complete details of such designated individual/ entity to section 12A Nodal officer of Ministry of Corporate Affairs. If such company or LLP holds funds or assets of the designated individual/ entity, he shall follow the similar procedure as laid down in paragraph 4.2 to 4.6 above for State Nodal Officer. Further the ROCs are required to ensure that no company or limited liability Partnership firm shall be allowed to be registered if any of the designated individual/ entity is the Director/ Promoter/ Partner or beneficial owner of such company or firm, and in case such a request is received, the ROC should inform the Section 12A Nodal Officer in the Ministry of Corporate Affairs.

viii. All communications to Nodal officer as enunciated in subclauses (i) to (vii) above should, inter alia, include the details of funds and assets held and the details of transaction.

ix. The Other DNFBPs are required to ensure that if any designated individual/entity approaches them for a transaction or relationship or attempts to undertake such transactions, the dealer should not carry out such transaction and, without delay, inform the Section 12A Central Nodal officer. The communication to the Central Nodal Officer would include the details of funds and assets held and the details of the transaction. Also, If the dealers hold any assets or funds of the designated individual/entity, they shall freeze the same without delay and inform the Section 12A Central Nodal officer.

(DNFBPs shall have the same meaning as the definition in Section 2(1) (sa) of Prevention of Money-Laundering Act, 2002.)

5.1. All Natural and legal persons holding any funds or other assets of designated persons and entities, shall, without delay and without prior notice, freeze any

transaction in relation to such funds or assets and shall immediately inform the State Nodal officer along with details of the funds/assets held, who in turn would follow the same procedure as in para 4.2 to 4.6 above for State Nodal Officer. This obligation should extend to all funds or other assets that are owned or controlled by the designated person or entity, and not just those that can be tied to a particular act, plot or threat of proliferation; those funds or other assets that are wholly or jointly owned or controlled, directly or indirectly, by designated persons or entities; and the funds or other assets derived or generated from funds or other assets owned or controlled directly or indirectly by designated persons or entities, as well as funds or other assets of persons and entities acting on behalf of, or at the direction of designated persons or entities.

5.2 No person shall finance any activity related to the 'designated list' referred to in Para 2.1, except in cases where exemption has been granted as per Para 6 of this Order.

5.3. Further, the State Nodal Officer shall cause to monitor the transactions / accounts of the designated individual/entity so as to prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities in the designated list. The State Nodal Officer shall, upon becoming aware of any transactions and attempts by third party, without delay, bring the incidence to the notice of the CNO and the DGP/Commissioner of Police of the State/UT for initiating suitable action.

5.4. Where the CNO has reasons to believe that any funds or assets are violative of Section 12A (1) or Section 12A (2)(b) of the Act, he shall, by order, freeze such funds or Assets, without any delay, and make such order available to authorities, Financial Institutions, DNFBPs and other entities concerned.

5.5 The CNO shall also have the power to issue advisories and guidance to all persons, including FIs and DNFBPs obligated to carry out sanctions screening. The concerned Regulators shall take suitable action under their relevant laws, rules or regulations for each violation of sanction screening obligations under section 12A of the WMD Act.

6. Regarding exemption, to be granted to the above orders

6.1. The above provisions shall not apply to funds and other financial assets or economic resources that have been determined by the CNO to be: -

a. necessary for basic expenses, including payments for foodstuff, rent or mortgage, medicines and medical treatment, taxes, insurance premiums and public utility charges, or exclusively for payment of reasonable professional fees and reimbursement of incurred expenses associated with the provision of legal services or fees or service charges for routine holding or maintenance of frozen funds or other financial assets or economic resources, consequent to notification by the MEA authorizing access to such funds, assets or resources.

This shall be consequent to notification by the MEA to the UNSC or its Committee, of the intention to authorize access to such funds, assets or resources, and in the absence of a negative decision by the UNSC or its Committee within 5 working days of such notification.

- b. necessary for extraordinary expenses, provided that such determination has been notified by the MEA to the UNSC or its Committee, and has been approved by the UNSC or its Committee;

6.2. The accounts of the designated individuals/ entities may be allowed to be credited with:

- a. interest or other earnings due on those accounts, or
- b. payments due under contracts, agreements or obligations that arose prior to the date on which those accounts became subject to the provisions of section 12A of the Act.

Provided that any such interest, other earnings and payments continue to be subject to those provisions under para 3.3;

6.3 Any freezing action taken related to the designated list under this Order should not prevent a designated individual or entity from making any payment due under a contract entered into prior to the listing of such individual or entity, provided that:

- (i) the CNO has determined that the contract is not related to any of the prohibited goods, services, technologies, or activities, under this Act, or under the United Nations (Security Council) Act, 1947 or any other relevant Act for the time being in force, or by an order issued under any such Act, in relation to weapons of mass destruction and their delivery systems;
- (ii) the CNO has determined that the payment is not directly or indirectly received by an individual or entity in the designated list under this Order; and
- (iii) the MEA has submitted prior notification to the UNSC or its Committee, of the intention to make or receive such payments or to authorise, where appropriate, the unfreezing of funds, other financial assets or economic resources for this purpose, ten working days prior to such authorization

7. Regarding procedure for unfreezing of funds, financial assets or economic resources or related services of individuals/entities inadvertently affected by the freezing mechanism upon verification that the individual or entity is not a designated person or no longer meet the criteria for designation:

7.1 Any individual/entity, if it has evidence to prove that the freezing of funds, financial assets or economic resources or related services, owned/held has been inadvertently frozen, an application may be moved giving the requisite evidence, in writing, to the relevant RE/Registrar of Immovable Properties/ ROC/Regulators and the State.

7.2 The RE/Registrar of Immovable Properties/ROC/Regulator and the State Nodal Officer shall inform, and forward a copy of the application, together with full details of the asset frozen, as given by applicant to the CNO by email, FAX and by Post, within two working days. Also, listed persons and entities may petition a request for delisting at the Focal Point Mechanism established under UNSC Resolution.

7.3 The CNO shall cause such verification, as may be required on the basis of the evidence furnished by the individual/entity, and, if satisfied, it shall pass an order, without delay, unfreezing the funds, financial assets or economic resources or related services, owned/held by such applicant, under intimation to all RE/Registrar of Immovable Properties/ROC/Regulators and the State Nodal Officer. However, if it is not possible, for any reason, to pass an Order unfreezing the assets within 5 working days, the CNO shall inform the applicant expeditiously.

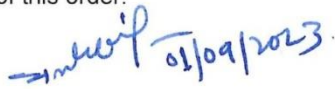
7.4 The CNO shall, based on de-listing of individual and entity under UN Security Council Resolutions, shall pass an order, if not required to be designated in any other order, without delay, unfreezing the funds, financial assets or economic resources or related services, owned/held by such applicant, under intimation to all RE/Registrar of Immovable Properties/ROC/Regulators and the State Nodal Officer.

8. Procedure for communication of compliance of action taken under Section 12A: The CNO and the Nodal Officer in the Foreigners Division, MHA shall furnish the details of funds, financial assets or economic resources or related services of designated individuals/entities, frozen by an order, and details of the individuals whose entry into India or transit through India was prevented, respectively, to the Ministry of External Affairs, for onward communication to the United Nations.

9. Communication of the Order issued under Section 12A: The Order issued under Section 12A of the Act by the CNO relating to funds, financial assets or economic resources or related services, shall be communicated to all nodal officers in the country.

10. This order is issued in suppression of F.No.P-12011/14/2022-ES Cell-DOR, dated 30th January 2023.

11. All concerned are requested to ensure strict compliance of this order.


(Manoj Kumar Singh)
Director(HQ)

To,

1. Governor, Reserve Bank of India, Mumbai
2. Chairman, Securities & Exchange Board of India, Mumbai
3. Chairman, Insurance Regulatory and Development Authority, Hyderabad.
4. Foreign Secretary, Ministry of External Affairs, New Delhi.
5. Finance Secretary, Ministry of Finance, New Delhi.
6. Revenue Secretary, Department of Revenue, Ministry of Finance, New Delhi.
7. Secretary, Ministry of Corporate Affairs, New Delhi
8. Chairman, Central Board of Indirect Taxes & Customs, New Delhi.
9. Director, Intelligence Bureau, New Delhi.
10. Additional Secretary, Department of Financial Services, Ministry of Finance, New Delhi.
11. Chief Secretaries of all States/Union Territories

12. Principal Secretary (Home)/Secretary (Home) of all States/ Union Territories
13. Directors General of Police of all States & Union Territories
14. Director, General of Police, National Investigation Agency, New Delhi.
15. Commissioner of Police, Delhi.
16. Joint Secretary (Foreigners), Ministry of Home Affairs, New Delhi.
17. Joint Secretary (Capital Markets), Department of Economic Affairs, Ministry of Finance, New Delhi.
18. Joint Secretary (Revenue), Department of Revenue, Ministry of Finance, New Delhi.
19. Director (FIU-IND), New Delhi. Copy for information to: -
 1. Sr. PPS to HS
 2. PS to SS (IS)

List of Nodal Officers for the implementation of Section 12A of WMD Act, 2005

Attention is drawn to Section 12A of Weapons of Mass Destruction and Their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005.

1. Further attention is drawn to Department of Revenue Order No. F. No. P-12011/14/2022-ES Cell-DOR dated September 01, 2023, vide which Director, FIU-INDIA has been designated as the Central Nodal Officer (CNO) for the purpose of implementation section 12A of said Act.
2. Further, para 1.4 of the order requires the CNO to maintain an updated list of all nodal officers and share the same with reporting entities.
3. In pursuance of the same, the list of Nodal Officers for the implementation of Section 12A of the WMD Act, 2005, may be found enclosed with the present alert.
4. Reporting entities are to take note of the list of Nodal Officers (**Annexure VI**) and ensure strict adherence to the provisions of section 12A of WMD Act, 2005 and Department of Revenue Order No. F. No. P-12011/14/2022-ES Cell-DOR dated September 01, 2023.

Annexure VI

LIST OF NODAL OFFICERS

Regulators						
Sr.No.	Agency	Name of Nodal Officer	Designation	Email ID	Contact Number	FAX Number
1	CBIC	Dr. Amandeep Singh	ADG	aman@gov.in		
2	IRDAI	Ms. Nimisha Srivastava	GM	nimisha@irdai.gov.in	852726 9188	
3	MCA	Shri Inder Deep Singh Dhariwal	Joint Secretary, Policy Section, MCA	dhariwalids@cag.gov.in	011-23383345	
4	PFRDA	Shri Ashish Bharati	GM	ashish.bharati@pfrda.org.in	851005 5510	
5	RBI	Shri Santosh Kumar Panigrahy	CGM	skpanigrahy@rbi.org.in cgmaml@rbi.org.in	916779 2059	
6	SEBI	Ms. Sapna Sinha	DGM	sapnas@sebi.gov.in	947100 3518	
States and Union Territories						
1	Andhra Pradesh	Shri Ravindranath Babu	AIG(Law & Order), O/o, DGP	aigloappolice@gmail.com	912105 8158	0863-2340255

2	Arunachal Pradesh	Shri Rohit Rajbir Singh	SP Crime/SIT	sit@arunpol.nic.in		
3	Bihar	Shri Chaitanya Prasad	Additional Chief Secretary, Home Department	secy-home-bih@nic.in	947319 1464	
4	Goa	Shri Edwin M. S. Colaco	Superintendent of Police (ATS)	sp.ats@goapolice.gov.in	787575 6019	
5	Haryana	Shri Saurabh Singh	Inspector General of Police, Security, CID, Haryana	igp.security@hry.nic.in		
6	Himachal Pradesh	Shri Sandeep Kumar Bhardwaj	SP	sp-sb-hp@nic.in		
7	Kerala		Additional Director General of Police (Intelligence)	adgpint.pol@kerala.gov.in		
8	Maharashtra	Shri Praveen Salunke	Addl DGP	adg.sops@mahapolice.gov.in	777606 0781	
9	Manipur	Dr. Th Charanjeet Singh	Joint Secretary, Home Department	charanluwang@gmail.com	897447 5406	

10	Meghalaya	Shri R Rapthap, IAS	Secretary, Home (Police) Department	r_rapthap@yahoo.in	943610 7574	0364- 25065 06
11	Mizoram	Shri Lalthiamsanga Sailo	Joint Secretary, Home Department	ltsailo61@gmail.com home-mz@mizoram.gov.in	943637 9659	
12	Odisha	Dr. Santosh Bala, IPS	Special Secretary, Home Department	splsecyhome@gmail.com	943708 5200	
13	Punjab	Smt. Jaswinder Kaur Sidhu	Secretary, Home	home@punjab.gov.in	981420 5583	
14	Rajasthan	Shri Anshuman Bhomia	Deputy Inspector General of Police, ATS, Rajasthan, Jaipur	digp.ats-rj@gov.in	941400 5888	0141- 26015 83
15	Sikkim	Shri Sudhakar Rao, IPS	Additional Chief Secretary, Home Department	attilisudhakar@gmail.com	943404 4452	
16	Tamil Nadu	Shri Ara Arularasu, IPS	SP, Special Division, SB CID, Chennai, Tamil Nadu	spsdsbcid.tnpol@nic.in	949812 2422	

17	Telangana	Shri. Mahesh M. Bhagwat, IPS	DG of Police, 3rd Floor, DGP Complex, Lakdika Pool, Hyderabad 04	adg-cidts@gov.in	9440700105	040-23242424
18	Tripura	Shri. Sudipta Das, IPS	SP(Economic Offences)	speo-tpcb@tripurapolicenice.in	9836466414	
19	Uttar Pradesh	Shri. Vivek	Special Secretary, Home Department	vivek.09@ias.gov.in	9919219190	
20	Jammu and Kashmir	Shri. Sandeep Gupta	SSP(Tech), CID Hqrs, J&K	sptechcidhqrs@jkpolice.gov.in	9419130411	0191-2580811
21	Dadra & Nagar Haveli	Shri Fulzele Piyush Nirakar, IPS	SP (HQ), Dadra & Nagar Haveli and Daman & Diu. Police HQ, Dunetha, Nani Daman, Daman - 396210	sp-hq-dnhdd@ddd.gov.in	0260-2220180	
22	Lakshadweep	Shri. Ajay Kumar	Deputy Superintendent of Police, [HQ UTL], Kavaratti	dysp.hq.lkpol@gov.in	9188129890	04896-262740
		Shri Rajiv				011-

23	NCT of Delhi	Ranjan Singh, IPS	DCP/NDR/Special Cell	dcp-ops-splcell-dl@nic.in	981809 8587	24633 291
24	Pondicherry	Shri Brijendra Kumar Yadav, IPS	Senior Superintendent of Police, Crime and Intelligence	sspci@py.gov.in	704271 5304	
25	Ladakh	Shri Sheikh Junaid Mahmood, IPS	DIG, Leh-Kargil Range	dig-ladakh@police.ladakh.gov.in	941903 3207	
26	Andaman & Nicobar	Shri Sanjay Tyagi, IPS	Deputy Inspector General of Police, (Intl./CID) Police HQ, Atlanta Point Port Blair-744104	digpint-anp@gov.in		03192 - 23230 5
27	Chandigarh		Deputy Superintendent of Police, CID,	pdspcid-chd@nic.in	977958 0991	



hpsc

(Scheduled Bank)

हिमाचल प्रदेश राज्य सहकारी बैंक सीमित
H.P. State Co-operative Bank Ltd.

Follow us on



@hpscblofficial