ANTI MONEY LAUNDERING POLICY 2016-17

UNITED BANK OF INDIA

OPERATIONS & SERVICES DEPARTMENT

Annexure- I

Anti Money Laundering (AML) Policy of the Bank

Index

Preamble

World over, the fight against money laundering (ML) and financing of terrorism has become the topmost priority. ML poses, a risk to the soundness and stability of financial institutions and financial systems, increased volatility of international capital flows, and a dampening effect on foreign direct investment. It has not only shaken the world economy but also threatened the stability of human civilization. Protecting the integrity and stability of the international financial system, cutting off the resources available to terrorists, and making it more difficult for those engaged in crime to profit from their criminal activities are some of the measures taken in this regard.

In India, there had been Laws and Regulations for quite some time to address certain aspects of Prevention of Money Laundering (PML), like Criminal Law Amendment Ordinance, 1944 for attachment of proceeds of certain crimes or Reserve Bank of India instructions regarding identification requirements for opening of the bank accounts. However, consolidated Anti-money laundering specific legislation, Prevention of Money Laundering Act. (PMLA), 2002, came in to effect with the Government of India Gazette Notification on 1st July, 2005. The Financial Intelligence Unit-India (FIU-IND) constituted by Government of India on 18th November, 2004 as a Nodal Agency in India for the Anti-money Laundering (AML) measures got statutory recognition on and from 1st July**,** 2005.

It is to be noted that both KYC and AML are integrated and interrelated. Our AML Policy is based on the guidelines of the Controlling Authorities such as RBI Master circular on KYC norms/ Anti Money Laundering (AML) standards/Combating of Financing of Terrorism (CFT) obligation of banks, under PMLA, 2002, IBA Guidance Notes for Banks dated 9th January, 2012; Report of the IBA Working Group for Risk Based Transaction Monitoring dated 18th May, 2011; Circulars issued by Department of Financial Services (DFS), Ministry of Finance, including Bank's internal Circulars.

So far a number of developments took place in AML/CFT regime globally and in our country. We have already made AML policies time to time conforming to Amendments in PMLA. The last AML Policy was issued in 2015, as a unrevised continuation of the earlier Policy issued in 2014 was based on the Government of India notification on "PML (Maintenance of Records) Amendment Rules, 2013", aligned with RBI Master Circular DBOD.AML.BC.No.22/14.01.001/2014 – 15 dated July 1, 2014.

The objectives of the current revision are as under:

a) To include some amendments in PML Rules, issued after last Policy.
b) To exclude details of those parts (e.g. Customer Acceptance Policy) which are covered in detail in KYC Policy

c) To exclude some details which are academic in nature and considered to be not required in the Policy document, so that the user of the Policy does not lose track of the essentials.
d) To rearrange some parts to have a more natural flow
e) To have some minor corrections to have clarity of meaning.

1.1 Objectives

The major objectives of the policy are:

i) To prevent the bank accounts and banking services from being used intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities.

ii) To create awareness about legal and regulatory frame work for AML/CFT requirements and systems among our bank people,

iii) To interpret the obligations under the PMLA and other relevant regulations and how they may be implemented in practice,

iv) To align the banking operations with good international industry practice in AML/CFT procedures through a proportionate risk based approach, and

v) To implement the systems and controls necessary to mitigate the risks of the Bank being used in connection with money laundering and terrorist financing.

2. Understanding Money Laundering and other Financial Crimes

2.1 What is Money Laundering?

The offence of Money Laundering has been defined in Section 3 of the Prevention of Money Laundering Act (PMLA), 2002 as "whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime and projecting it as untainted property shall be guilty of offence of money laundering".

"Proceeds of crime" means any property derived or obtained, directly or indirectly, by any person as a result of criminal activity relating to a scheduled offence or the value of any such property.

Money laundering is the process by which criminals attempt to hide and disguise the true origin and ownership of the proceeds of their criminal activities, thereby avoiding prosecution, conviction and confiscation of the criminal funds.

There are three stages of money laundering during which there may be numerous transactions made by launderers that could alert an institution to criminal activity-

- **Placement**- the physical disposal of cash proceeds derived from illegal activity.
- **Layering**- separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity.

- **Integration**- placing the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing to be normal business

  Funds, if the previous layering process had succeeded

Prevention of Money Laundering, therefore, is not only a statutory or regulatory requirement but also a moral responsibility for all the bank employees as any facilitation of money laundering indirectly supports these criminal activities.

2.2 Terrorist Financing

Terrorists use similar methods as Money Launderers for moving their funds. Some of the terrorist groups also indulge in criminal activities for generating funds for their activities and some of them are even known to have strong relationships with criminal gangs. The two major differences between terrorist financing and money laundering are:

- Terrorist funding can happen from legitimately obtained income whereas the source of money in money laundering is always from illegal source, and
- More often terrorist activities require small amounts and hence it is increasingly difficult to identify terrorist funding transactions as against money laundering which is always with high value.

2.3 Other Financial Crimes

Other financial crimes such as Fraud and market abuse (insider trading) are closely related to money laundering and terrorist financing and most often the measures described in these guidelines for preventing money laundering and terrorist financing may help financial institutions in preventing fraud and other financial crimes, as well.

2.4 International Developments & Recommended Standards.

2.4.1 Financial Action Task Force (FATF)

One of the most important events to influence international money laundering prevention efforts was the establishment of FATF by the G-7 Summit in 1989 consisting of the G-7 member states, the European Union and Eight other countries. Over the years more members were admitted to the FATF and the current membership is 36, including 34 member states and 2 Regional Organizations, European Union and Gulf Development Council. India has been accorded membership status in June, 2010.

The objectives of the FATF are to set standards and promote 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.

FATF issued 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation' 1990. Subsequent revisions have been issued with the latest one issued in Feb 2012 to keep it relevant and up-to-date and make it universal in nature.

The FATF monitors the progress of its members in implementing necessary measures, reviews money laundering and terrorist financing techniques and counter-measures, and promotes the adoption and implementation of appropriate measures globally.

The FATF works to identify national-level vulnerabilities with the aim of protecting the international financial system from misuse.

3. Legislation & Regulation in India

3.1 Prevention of Money Laundering Act. (PMLA)

The first step in the AML legislation in India was the passage of PML bill by the Parliament in 2002 which received President's assent in January 2003 and PMLA, 2002 was enacted. This law came to effect on 1st July, 2005.

Subsequently amendments to this Act were made in 2009 and 2012 through **Prevention of Money Laundering (Amendment) ACT (PMLA), 2009 and Prevention of Money Laundering (Amendment) ACT (PMLA), 2012.**

The Act criminalizes money laundering and also provides for freezing and confiscation of assets concerned in money laundering. Appointment of various authorities including Financial Intelligence Unit (FIU) is also covered in its provisions. The Act also lays down obligations of banks in maintaining records of certain prescribed transactions and reporting such transactions to FIU-IND. This also lists out the prescriptive offences, which will come under the purview of the Act.

3.2 Rules under PMLA.

In terms of the section 73 of PMLA, the Central Government has been empowered to formulate rules for implementing the provisions of the Act. The rules are notified and published through Official Gazette. The first set of rules was notified on 1st July 2005.

Subsequently several modifications, additions to the Rules have been issued.

Consequent to the PMLA coming into effect and notification of the rules framed there under, detailed instructions have been issued by the Regulators regarding the responsibilities of regulated entities under the Act, especially on the following points:

- Nomination of Designated Director;
- Appointment of Principal Officers;

- Reporting of Cash Transactions (CTR) above INR ten lakh or its equivalent in foreign currency in a month;
- Reporting of Counterfeit Currency Notes and forged valuable securities detected in a month;
- Reporting of all transactions involving receipt by Non-profit organization (NPO) in a month, and
- Reporting of all Suspicious Transactions Report (STR) within 7 days of arriving at a conclusion that any transaction is of suspicious nature;
- Report of transactions of all Cross Border Wire Transfers of the value of more than five lakh rupees (or equivalent in foreign currency) where either the origin or destination of fund is in India.

3.2.1 Anti-Money Laundering (AML) Guidelines of RBI for related activities.

There are specific guidelines issued by RBI for complying with the requirements of PMLA related activities which commercial banks undertake, such as authorized money changers, payment system operators, etc. These guidelines also specify the standards for performing due diligence on their customers, maintenance records, monitoring and reporting of suspicious activities to FIU-IND, etc.

3.3 Guidelines for Anti-Money Laundering (AML) Measures issued by other regulators.

Other financial sector Regulators (SEBI, IRDA, NHB etc.) have been issuing guidelines under PMLA and Rules notified there under, for entities regulated by them, like CDD on customers, maintaining records of prescriptive transactions, reporting of suspicious activities, etc.

4. Obligation for establishing identity of clients and beneficial owners

Section 12 of the Prevention of Money Laundering Act, 2002 and rules thereunder require every reporting entity to verify and maintain the records of the identity of all its clients including beneficial owners, in such manner as may be prescribed.

Rules 9 and 10 of the Rules provide for verification and maintenance of the records of the identity of clients. Rule 10(2) prescribes that the records of the identity of clients shall be maintained in a manner specified by its regulators from time to time.

The KYC Policy issued by the Bank and being revised from time to time in conformity with RBI directions on the subject and PML Rules adequately covers this aspect.
The relevant provisions of the KYC Policy having the following key elements will be considered part of AML Policy also:

a) Customer Acceptance Policy
b) Risk Management
c) Customer Identification Procedure
d) Monitoring of Transactions.

KYC Policy is to be referred for details of the above key elements which are not being repeated here.

KYC Policy also covers guidelines on New Technology Products like pre-paid cards, UN Sanctions List, Bullion Traders, Money Mules, Multi Level Marketing (MLM) Firms, Politically Exposed Persons, **Remittance towards participation in lottery, money circulation schemes, other fictitious offers of chit funds/ponzy schemes etc. These will also be considered to be part of AML Policy and are not repeated here.**

5. Combating Financing of Terrorism

a) In terms of PML Rules, suspicious transaction should include, inter alia transactions which give rise to a reasonable ground of suspicion that it may involve the proceeds of an offence mentioned in the Schedule to the PMLA, regardless of the proceeds of an offence mentioned in the Schedule to the PMLA, regardless of the value involved.

Our bank has developed suitable mechanism through appropriate policy framework for enhanced monitoring of transactions suspected of having terrorist links and swift identification of the transactions and making suitable reports to the Financial Intelligence Unit-India (FIU-IND) on priority.

b) Our branches are advised to take into account risks arising from the list of individuals and entities approved by Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs) received form Govt. of India and circulated by RBI. The UN Security Council has adopted Resolutions 1988 (2011) and 1989 (2011) which have resulted in splitting of the 1267 Committee's Consolidated List into two separate lists, namely -

i) **"Al-Qaida Sanctions List",** which is maintained by the 1267/1989 Committee. This list shall include only the names of those individuals, groups, undertakings and entities associated with Al-Qaida. The updated AL-Qaida Sanctions List is available at **http://www.un.org/sc/committees/1267/aq_sanctions_list_shtml**.

ii) **"1988 Sanctions List",** which is maintained by the 1988 Committee. This list consists of names previously included in Sections A ("Individuals associated with the Taliban") and B ("Entities and other groups and undertakings associated with the Taliban") of the Consolidated List. The Updated 1988 Sanctions list is available at http://www.un.org/sc/committees /1988/list.shtml. The list is also published in our Bank's intranet as and when available.

iii) "Unlawful Activities Prevention ACT (UAPA) List",- List of individuals which is notified by Ministry of Home Affairs for exercising caution is published in our Intranet site as and when available. The list is to be referred before entering into a banking relationship and allowing transactions.

6. Internal Controls and Structures in the Bank.

6.1 Designated Director

Reserve Bank of India vide circular No. DBOD.AML.BC. No.80/14.01.001/2013-14 dated December 31, 2013, has advised banks to nominate a Designated Director for ensuring compliance with the obligations under the PMLA. Designated Director means a person designated by the Reporting entity to ensure overall compliance with the obligations imposed under chapter IV of the Act and the Rules. **Bank is required to nominate a Director on its Board as "Designated Director", as per the provisions of the PML (Maintenance of Records) Amendment Rules, 2013. The name, designation and address of the Designated Director are to be communicated to the Director, Financial Intelligence Unit – India (FIU-IND).**

6.2 Principal Officer

Bank is required to appoint a Senior Management officer to be designated as Principal Officer (PO). He should be located at the Head/corporate office of the bank and shall be responsible for monitoring and reporting of all transactions and sharing of information as required under the law. He will maintain close liaison with enforcement agencies, banks and any other institutions which are involved in the fight against Money Laundering and Combating Financing of Terrorism. He should have timely access to customer identification data and other Customer Due Diligence information, transaction records and other relevant information. He should also take reasonable steps to establish and maintain adequate arrangements for awareness creation and staff training. PO should take care for timely submission of CTR, STR, NTR, CWTR and Counterfeit Currency Report (CCR). He will also look after and ensure overall compliance with regulatory guidelines on KYC/AML/CFT issued from time to time and obligations under the Prevention of Money Laundering Act, 2002, rules and regulations made there under, as amended from time to time. He will also ensure that appropriate risk-based policies are in place across different aspects of the business to mitigate the risk of being used for the purpose of money laundering and terrorist financing. He should also provide sufficient guidance to staff to ensure that the customers are not informed (i.e. tipped off) that his/her accounts are under monitoring for suspicious activities and /or that a disclosure has been made to the FIU-IND.

6.3 AML Cell.

To meet the statutory requirements under PMLA, Bank has constituted an AML (Anti Money Laundering) Cell under the control and supervision of Principal Officer comprising

senior and trained officers including IT support officers. Bank has implemented AMLOCK software for alert generation. The functions of the AML Cell are as follows:

i) To import daily data of all branches through AMLOCK software from Finacle System.

ii) To analyze the alerts generated through AMLOCK System based on IBA recommended parameters for STRs, prepare notes and to get it approved by the Principal Officer.

iii) To generate monthly cash Transaction Report (CTR) and Non Profit Organization Report (NTR).

iv) To generate monthly Cross Border Transaction Report (CWTR).

v) To file the Counterfeit Currency Report (CCR) after receiving from Security Department within time schedule to FIU-IND.

vi) To adopt suitable steps to procure any information about the customers or transactions which the Regulatory Authorities require.

vii) To inform all the branch level functionaries about the day to day matters developed relating to national and international findings of the countries with inadequacies in their approach for prevention of money laundering.

6.4 Functions of Branches regarding KYC-AML.

Branch people play vital roles on compliance of KYC norms and assist to prevent money laundering. Their functions concerning with KYC-AML norms can be classified as follows:

i) Follow the KYC Policy of the Bank and circulars issued from time to time pertaining to KYC-AML, exercise of CDD (Customer Due Diligence) and EDD (Enhanced Due Diligence) while opening of new accounts.

ii) Making KYC updation of all old non KYC compliant accounts, observing all KYC norms within time schedule. Conducting Data Cleaning, it is to be ensured that the pertinent aspects of customer's identity like communication & permanent address, occupation, PAN etc. are properly incorporated in the CBS system under Menu option 'CUMM' as per Bank's circular No. IT/KYC/4/OM-0291/12-13 dated 8th August, 2012 and through a simplified web based Data Entry Package following Uniform Resource Locator (URL) in the browser address http:172.16.21.19:8084/kyc/

iii) While creating/modifying Customer Master, Customer Risk Parameters should be incorporated in the system following Bank's circular no. IT/CBS/16/OM-0605/12-13 dated 10th January, 2013 until the process of Automatic Risk Categorization is completed.

Detection and Impounding of Forged Indian Currency Notes (FICN) by the staff engaged in handling of cash in the branches/currency chests and reporting the same to the Security Department, Head office, **by 7th of the succeeding month** positively, so that the centralized AML Cell may report to FIU-IND by 15th of the same month.

Earlier branches were required to file FIR in case of each detection of counterfeit note irrespective of the number of pieces and bonafides of the tenderer. Now the matter has been reviewed by RBI and it has been decided that for detection of counterfeit notes up to 4 (four) pieces in a single transaction, a consolidated report per month to be sent but for detection of counterfeit notes of five or more pieces in a single transaction, FIR should be lodged with Nodal Police Station / Police Authorities as per jurisdiction.

iv) Identification of accounts of Non Profit Organization (NPO) in the branch level and rectification of specific field- customer type (code-171) through Menu Option -'CUMM', so that the Monthly Report of NPOR/NTR may be generated centrally by our centralized AML Cell.

v) Proper maintenance of records of all transactions and documents relating to KYC norms.

vi) Maintaining secrecy about the transactions of accounts under monitoring for suspicious activities.

vii) Reporting is an obligation of suspicious transactions relating to money laundering or terrorist financing activities. All branches are required to report any suspicious activities observed by them which is still under doubt after taking the due diligence, immediately to their Chief Regional Manager under 'confidential' cover which in turn will immediately be sent with observation to the Principal Officer for taking final decision and filing the Suspicious Transaction Report to FIU-IND based on 27 **'Indicative Alert Indicators for Branches /Department suggested by IBA'** circulated through circular no. INSP/AML/4/OM- /2011-12 dated 22nd July, 2011.

7 Reporting Obligation under PMLA .

In terms of the Rules notified under Prevention of Money Laundering Act (PMLA), 2002, certain obligations were cast on banking companies with regard to reporting of certain transactions. The RBI has issued guidelines detailing the obligation of banks in term of the Rules notified under PMLA.

Accordingly, Bank is required to make the following reports to the FIU-IND.

1. Cash Transaction Reporting (CTR)
2. Counterfeit Currency Reporting (CCR)
3. Suspicious Transaction Reporting (STR)
4. Non Profit Organization Reporting (NPOR/NTR)
5. Cross-Border Wire Transfer Reporting (CWTR)

7.1 Cash Transaction Reporting (CTR).

As per the PMLA rules, Bank is required to submit the details of:

- All cash transactions of the value of more than rupees ten lakh or its equivalent in foreign currency.
- All series of cash transactions integrally connected to each other, which have been **individually** valued below rupees ten lakh or its equivalent in foreign currency, where such series of transactions have taken place within a month and the **monthly** aggregate exceeds rupees ten lakh or **its equivalent in foreign currency.**

For integrally connected cash transactions, total debit and total credit in a month should be considered separately. However, the bank should not separately report to FIU- IND which is less than Rs.50,000.00.

This report is required to be filed on a monthly basis by 15th of the succeeding month.

After migration to CBS system the Cash Transaction Report (CTR) are being compiled centrally at Head Office. However, the branches are to generate their monthly CTR at their end through Menu Option 'UNIRPT' and keep the report properly for production to Auditors/Inspectors as and when asked for.

7.2 Counterfeit Currency Reporting (CCR)

The PMLA Rule 3(1)(C) read with rule VIII requires the reporting of all cash transactions where forged or counterfeit Indian currency notes have been used as genuine. **The report is required to be filed by the 15th day of the succeeding month for centralized AML Cell.**

The consolidated monthly report of the branch should be sent to Security Department, HO **within the 7th day of the succeeding month and Security Department in turn send the consolidated monthly report immediately to centralized AML Cell for onward filing to FIU-IND.** While submitting the report of FICN to HO, they should specifically mention Date of detection and denomination wise currency Serial Nos.

7.3 Suspicious Transaction Reporting (STR)

As per PMLA Rule 2(g) Suspicious Transaction means a transaction whether or not made in cash which to a person acting in good faith –

a. gives rise to reasonable ground of suspicion that it may involve the proceeds of crime or
b. appears to be made in circumstances of unusual or unjustified complexity or
c. appears to have no economic rationale or bonafide purpose gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism .

7.3.1 Generation of Alerts

Alert generation involves application of scenarios and risk factor to detect potentially suspicious activity. Effective alert generation is very critical to the quantity and quality of the STRs generated by the bank. Indicators are circumstances that indicate suspicious nature of transactions. Suspicious transaction may be detected from one indicator or a set

of indicators.

In the new reporting format specifications, the bank are required to provide information about the source of alert and the alert indicator(s) for detection of suspicious transactions.

Our bank has adequate processes and systems for detection of transactions and reporting of suspicious transactions, identified by the employee at Branches/Departments and are using centralized Alert Generation Software-AMLOCK, based on IBA recommended parameters.

7.3.2 Identification of Suspicious transactions by Branches/Departments

There are certain types of transaction which can be identified at the branches/operations departments themselves. The identification of suspicious transaction at Branches/Departments is more likely to be related with the following sources:

- **Customer Verification (CV):** Detected during customer acceptance, identification or verification (excluding reasons mentioned on other codes e.g. use of forged ID, wrong address etc.)
- **Law Enforcement Agency Query (LQ):** Query or letter received from Law Enforcement Agency (LEA) or Intelligence Agency (blocking order received, transaction details sought etc.)
- **Media Reports (MR):** Adverse Media Reports about customer (e.g. news paper reports)
- **Employee Initiated (EI**): Employee raised alert (e.g. behavioural indicators such as customer had no information about transaction, attempted transaction etc.)
- **Public Complaint (PC):** Complaint received from public (e.g. abuse of account for committing fraud etc.)
- **Business Associates (BA):** Information received from other institutions, subsidiaries or business associates (e.g. cross-border referral, alert raised by agent etc.)

The list of commonly used alert indicators for detection of suspicious transaction at Branches/Departments is given in **Appendix A**. The first two characters in the alert indicator code denote the source of alert as mentioned above. Branch/Department is also encouraged to apply additional alert indicators to address specific risks faced by them.

7.3.3 Identification of suspicious transaction at Centralized AML Cell.

The identification of suspicious transactions at centralized AML cell using alert generation software is more likely to be related to following sources:

- **Watch List (WL):** The customer details matched with watched with watch lists (e.g. UN list, Interpol list etc.)
- **Typology (TY):** Common typologies of money laundering, financing of terrorism or other crimes (e.g. structuring of cash deposits etc.)
- **Transaction Monitoring (TM):** Transaction monitoring alert (e.g. unusually large

transaction, increase in transaction volumes etc.)

- **Risk Management System (RM**): Risk Management system based alert (e.g. high risk customer, country, location, source of funds, transaction type etc.)

The list of commonly used alert indicators for detection of suspicious transactions at centralized AML cell using alert generation software is given in **Appendix B.** The first two characters in the alert indicator code denote the source of alert as mentioned above.

Bank is empowered to select appropriate number and value thresholds before implementing the alert indicators using alert generation software. Bank is also encouraged to apply additional alert indicators to address specific risks faced by him. But out of recommended 61 parameters, 9 alert parameters related to credit and debit card, dealing in precious metal or stone etc. cannot be generated in the system due to non availability of records and not introduced some business criteria in our bank. Now IBA directed the member Banks to descope daily alerts to avoid duplication of alert generation in AMLOCK software. Based on the letters issued by IBA, the daily alerts have been descoped and 21 monthly scenarios and 10 other scenarios have been implemented as given in **Appendix B.The Suspicious Transaction Report (STR) should be furnished within 7 days of arriving at a conclusion that any transaction, is of suspicious nature.**

7.3.4. Offsite Surveillance

The generation of daily alerts for offsite surveillance through our internal web-based application has been started from 29.02.2016. At present, daily alerts are generated on 11 types of alert parameters which can be described as per **Appendix C.** Also Bank is in process of developing more alert Parameters which will be implemented in due course

The alerts are reported to respective Branches and ROs on daily basis for their awareness & scrutiny. The branches scrutinize the transactions and after being satisfied about their genuineness, report it to respective Regional office on the following day of receipt of the transaction report. Regional Office, in turn, submit consolidated report to the Centralised AMl Cell generally on the following day. The ROs have been reporting it through the respective Nodal officers and in case of any delay the Nodal officers are being followed up by the AML Department.

7.4 Non Profit Organization Reporting (NPOR/NTR)

'Non-Profit Organization' is an entity or organization that is registered as a trust or a society under the Societies Registration Act, 1860 (21 of 1860) or any similar State legislation or a company registered under section 25 of the Companies Act, 1956 (1 of 1956) (or under section 8 of the Companies Act,2013).

Bank is required to maintain proper record of all transactions involving receipts by non-profit organizations of value more than rupees ten lakh or its equivalent in foreign

currency and to forward a report to FIU-IND. **All such transactions in the prescribed format every month by the 15th of the succeeding month.**

To facilitate the generation of NTRs centrally, a flag to mark the accounts of Non Profit Organization (NPO) has been identified in CBS system. Accordingly Branches are asked to identify and mark the eligible accounts in CBS system as NPO. Non Profit Organization Transaction Reports (NTRs) are being generated by centralized **AML Cell** in desired format of FIU-IND.

7.5 Cross Border Wire Transfer Reporting (CWTR)

Banks use wire transfers as an expeditious method for transferring funds between bank accounts. Wire transfers include transactions occurring within the national boundaries of a country or from one country to another. As wire transfers do not involve actual movement of currency, they are considered as rapid and secure method for transferring value from one location to another.

Cross-border transfer means any wire transfer where the originator and the beneficiary bank or financial institutions are located in different countries. It may include any chain of wire transfers that has at least one cross-border element.

Cross-border wire transfers :

i. All cross-border wire transfers must be accompanied by accurate and meaningful originator information.
ii. Information accompanying cross-border wire transfers must contain the name and address of the originator and where an account exists, the number of that account. In the absence of an account, a unique reference number, as prevalent in the country concerned, must be included.
iii. Where several individual transfers from a single originator are bundled in a batch file for transmission to beneficiaries in another country, they may be exempted from including full originator information, provided they include the originator's account number or unique reference number as at (ii) above.

All cross Border wire transfers of the value of more than Rupees Five lakh or its equivalent in foreign currency where either the origin or destination of fund is in India; to be reported to FIU-IND.

7.6 Filing of Reports to FIU-IND

The Prevention of Money Laundering Act (PMLA) and the rules there under require every financial institution to furnish to FIU-IND the statutory reports i.e. CTR, STR, CCR, NTR and CWTR within time schedule. The earlier prescribed multiple data files reporting format is being replaced by a new single XML file format.

FIU-IND has developed Report Generation Utility and Report Validation Utility as per their version no. 2.6 developed from time to time and the said generated reports are sent to

FIU-IND by the Principal Officer through their own website https://finnet.gov.in.

7.7 Powers of the Director of FIU-IND

i) If the Director, in the course of any inquiry, finds that a banking company, financial institution or an intermediary or any of its officers has failed to comply with the provisions contained in section 12, then, without prejudice to any other action that may be taken under any other provisions of this Act, he may, by an order, levy a fine on such banking company or financial institution or intermediary which shall not be less than ten thousand rupees but may extend to one lakh rupees for each failure.

ii) While furnishing of information to the Director FIU-IND, delay of each day in not reporting a transaction or delay of each day in rectifying a misrepresented transaction beyond the time limit as specified in this rule shall constitute a separate violation.

8 Staff and Customer awareness

8.1 Staff Awareness

One of the most important controls over the prevention and detection of money laundering is to have staff members who are alert to the risks of money laundering/ terrorist financing and well trained in the identification of unusual activities and transactions, which may prove to be suspicious. The effective application of even the best designed control systems can be quickly compromised if the staff members applying the systems are not adequately trained. The effectiveness of the training will therefore be important to the success of the bank's AML/CFT strategy. Bank is required to take appropriate measures so that relevant employees are aware of -

a) Policies and procedures put in place to prevent money laundering.

b) The legal requirements contained in the PMLA and the rules and regulations framed there under.

c) KYC/AML guidelines issued by the RBI from time to time.

8.2 Customer awareness

In order to have an adequate control over AML, it is critical that key AML controls, such as KYC checks, have the support of Industry and customers. Customers should see the KYC checks process as a sensible contribution to the fight against crime and terrorism and not as a burdensome and deliberate barrier to the access to the banking. To promote this understanding, KYC checks should be done in a customer-friendly way and Bank's procedures and staff training should be designed accordingly.

9. Preservation of Records.

9.1 Purpose of maintaining records

The keeping of proper records is essential to enable the Bank to demonstrate that it has operated in conformity with local laws and regulations. This will in turn enable the Bank and individual staff members to defend themselves against any allegations of knowingly assisting a money launderer. Bank must retain records concerning customer identifications as evidence of the work they have undertaken in complying with their legal and regulatory obligations as well as for use as evidence in any investigation conducted by law enforcement.

Bank may maintain records of the identity of the clients **and records of transactions in hard and soft format.**

Rule 10(2) refers the records of the identity of clients shall be maintained in a manner as may be specified by its regulators from time to time. Regulator has to specify the procedure and manner of maintaining the records of the identity of the clients.

9.2 Records to be preserved

Bank introduced a system of maintaining proper record of transactions prescribed under Rule 3, of Prevention of Money Laundering Act, 2005 (PML Rules, 2005), as under:

- All cash transactions of the value of more than rupees ten lakhs or its equivalent in foreign currency;
- All series of cash transactions integrally connected to each other which have been individually valued below rupees ten lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds Rs.10 lakh;
- All transactions involving receipts by non-profit organizations of value more than Rs.10 lakh or its equivalent in foreign currency;
- All cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine or where any forgery of a valuable security or a document has taken place facilitating the transactions;
- All suspicious transactions whether or not made in cash;
- All cross border wire transfers of the value exceeding Rs.5 lakh or its equivalent in foreign currency where either the origin or destination of fund is in India;

Bank is required to maintain the following information in respect of transactions referred

to Rule 3 of Prevention of Money Laundering Act 2002.

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.

9.3 Period of retention of records

As per the PMLA, the account opening records including identification documents should be kept for 5 years from the date of cessation of the transactions/relationship between the customer and the bank and transaction records including credit/debit slips, cheques and other forms of Records relating to investigations and transactions, which have been the subject of a disclosure, should be kept for 5 years from the time the STR is filed with FIU-IND. Such records and related documents should be made available to help auditors in their work relating to scrutiny of transactions and also RBI/other relevant authorities. The term 'cessation' would broadly mean the time of closure of account. But there should have some exceptions:

a) In the matter related to a suspicious transaction is pending in a court, the relevant record should retained for 10 years from the date of final verdict of the court.

b) In specific cases, where RBI/FIU-IND or any other regulatory body requests for the retention of records for a period more than 10 years , the bank should be guided

by such specific request.

Any further development regarding AML-KYC should be communicated to all concerned through circulars.

Appendix- A

Area of Suspicious Transaction Reports to be submitted by the branch:

Branches can effectively control and reduce their risk only if they have an understanding of the normal and reasonable activity of the customer. Branches should pay special attention to all complex, unusually large transactions and all unusual patterns of business which have no apparent economic rationale or so. Branch people may raise alert on behavioral ground of Walk-in-customers such as attempted transaction etc. and submit STR to Principal Officer (PO) through respective CRM of the Region. IBA has recommended 27 Alert indicators for Branches/Departments of the Bank as indicated below:

:Indicative Alert Indicators for Branches/Departments:

Sl. No.	Alert Indicator	Indicative Rule/Scenario
1	CV1.1-Customer left without opening account.	Customer did not open account after being informed about KYC requirements.
2	CV2.1-Customer offered false of forged identification document.	Customer given false identification documents or documents that appears to be counterfeited, altered or inaccurate.
3	CV2.2-Identity documents are not verifiable	Identity documents presented are not verifiable i.e. Foreign documents etc.
4	CV3.1 – Address found to be non existent	Address provided by the customer is found to be nonexistent.
5	CV3.2- Address found to be wrong	Customer not staying at address provided during account opening.
6	CV4.1 – Difficult to Identify beneficial owner.	Customer uses complex legal structures or where it is difficult to identify the beneficial owner.
7	LQ1.1- Customer is being investigated for criminal offences.	Customer has been the subject to inquiry from any law enforcement agency relating to criminal offences.
8	LQ2.1 Customer is being	Customer has been the subject of

	investigated for TF offences	inquiry from any law enforcement agency relating to TF or terrorist activities.
9	MR1.1 – Adverse media report about criminal activities of customer	Match of customer details with persons reported in local media/open source for criminal offences.
10	MR2.1 – 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.
11	EI1.1 – Customer did not complete transaction	Customer did not complete transaction after queries such source of funds etc.
12	EI2.2- Customer is nervous.	Customer is hurried or nervous.
13	EI2.2 – Customer is over cautious	Customer over cautious in explaining genuineness of the transaction.
14	EI2.3 – 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.
15	EI3.1 – Customer acting on behalf of a third party	Customer has vague knowledge about amount of money involved in the transaction. Customer taking instructions for conducting transactions. Customer is accompanied by unrelated individuals.

16	EI3.2 – Multiple customers working as a group	Multiple customers arrive together but pretend to ignore each other.
17	EI4.1 – Customer avoiding nearer branches	Customer travels unexplained distances to conduct transactions.
18	EI3.2 – Customer offers different identifications on different occasions	Customer offers different identifications on different occasions with an apparent attempt to avoid linkage of multiple transactions.
19	EI4.3 – Customer wants to avoid reporting	Customer makes inquiries tries to convince staff to avoid reporting.
20	EI4.4 – Customer could not explain source of funds.	Customer could not explain source of funds satisfactorily.
21	EI5.1 – Transaction is unnecessarily complex	Transaction is unnecessarily complex for its stated purpose.
22	E15.2- Transaction has no economic rationale	The amounts or frequency or the stated reason of the transaction does not make sense for the particular customer.
23	EI5.3- Transaction inconsistent with business	Transaction involving movement of which is inconsistent with the customer's business.
24	EI6.1 – Unapproved inward remittance in NPO	Foreign remittance received by NPO not approved by FCRA.
25	PC1.1- Complaint received from public.	Complaint received from public for abuse of account for committing fraud etc.
26	BA1.1 – Alert raised by agent	Alert raised by agents about suspicion
27	BA1.2 – Alert raised by other institution	Alert raised by other institutions, subsidiaries or business associates including cross-border referral.

Appendix- B

Alert Indicators for Centralized AML Cell

IBA Parameters	Logical Description on threshold limit of the Bank
1. High value cash deposits (Monthly)	➔ Account (Individual and non-individual) wise aggregate transaction amount (Deposit) for the period of one month. ➔ Each and every Transaction amount (Deposit) for **Individual** account must be >= INR 2.00 lac & for Non-individual account must be >= INR 50.00 lac. ➔ Individual customers identified by constitution code '01', 11, and 16 and all others considered as non-Individual customers. ➔ It processes only cash transactions
2. High value cash WITHDRAWLS (MONTHLY)	➔ Account (Individual and non-individual) wise aggregate transaction amount (Withdrawal) for the period of one month. ➔ Each and every Transaction amount (Withdrawal) for Individual account must be >= INR 2.00 lac & for non-individual account must be >= INR 50.00 lac. ➔ Individual customers identified by constitution code '01', 11, and 16 and all others considered as non-Individual customers. ➔ It processes only cash transactions
3. High Value Non-Cash Deposits in a Month	➔ Account (Individual & non-individual) wise aggregate transaction amount (Deposit) for the period of one month. ➔ Each and every Transaction amount (Deposit) for Individual account must be >= INR 5.00 lac & for non-individual account must be >= INR 10.00 crore. ➔ Individual customers identified by constitution code '01', 11, and 16 and all others considered as non-Individual customers. ➔ It processes only non-cash transactions
4. High Value Non-Cash Withdrawal in a Month	➔ Account (Individual & non-individual) wise aggregate transaction amount (Withdrawals) for the period of one month. ➔ Each and every Transaction amount (Withdrawal) for Individual account must be >= INR 5.00 lac & for non-individual account must be >= INR 10.00 crore.

	➔ Individual customers identified by customer type code '01', 11, and 16 and all others considered as Non-Individual customers. ➔ It processes only non-cash transactions
5. Sudden High Value Transaction **for the Client** (MONTHLY)	➔ The Alert based on high value transactions done by the bank on behalf of its client/customer (as per instruction of the client) e.g., NEFT, RTGS, DD, PO etc. ➔ It's a comparative study of **non-cash transactions** (**Debit** only) done by the bank on behalf of the customer. ➔ First take account wise maximum high value transaction in a particular date of last SIX months (Threshold: 6 months). ➔ Let's say for an account the average transactions of previous **SIX** months' (Month wise) x, 2x, 3x, 4x, 5x or 6x where the highest value of last six months transaction is **6x**. ➔ If the value of the current month is **[6x plus 25% of 6x],** then the ALERT will come. ➔ Whereas, the Threshold limit of customer type code '01', 11, and 16 is >=2.00 lac. ➔ And, Threshold limit of non-individual is >=10.00 lac. ➔ Then alerts will be generated for that account. ➔ **BI is to be considered only.** ➔ **Govt. and Collection accounts are not to be considered.**
6. Sudden Increase in **Value of Transactions** in a Month for the Client	Below are the logical steps for the alert: ➔ It is the comparison between two different conditions of value of transactions (of total value), **debit and credit** separately. ➔ It's a comparative study of transactions of the account. ➔ The value of transactions increases suddenly in the current month with the average value of transactions of **previous SIX months**. ➔ Let's say for an account the average transactions of previous **SIX** months' (excluding the considerate month) is 'X'. ➔ Then account wise average transactions amount for current month/ considerate month should be ['X' plus 25% of current month's value], then the alert will come. ➔ Only such accounts are to be considered where date of opening minimum of SIX months' leaving the current month/considerate month for the generation of alert (threshold: 6 months). ➔ Taking the Threshold limit of customer type code '01', 11, and 16 >=2.00 lac. ➔ And, Threshold limit of non-individual >=10.00 lac.

	➔ **Non-cash transactions are to be considered only.**
7. High Value Transactions in Newly opened Account (monthly):	➔ It takes all the accounts of Savings Bank Account (SBA) and Current Deposit Account (CAA) whose account opening date is in between last SIX months. ➔ Transactions should be in **CASH and in NON-CASH** ➔ If high value **CASH** transactions happened in last month for the newly opened Individual (customer Type 141 or 142) >= INR 2.00 lac (threshold limit). ➔ For Non-Individual A/c it is >=10.00 lac, then alerts are to be generated. ➔ If any conjugate **(CASH plus NON-CASH)** transactions happened in last month for the newly opened accounts where the threshold limit for code '01', 11, and 16 >=10.00 lac and for non-individual it is >=20.00 lac, then alerts are to be generated for that transactions.
8. Number of Transactions in Newly opened Accounts, monthly:	➔ The alert is generated for the account whose age of opening is 6 months. ➔ The total number of transactions happened for that account during the last SIX months' time period is >=40 (threshold limit for SBA). ➔ The total number of transactions happened for that account during the last SIX months' time period is >=100 (threshold limit for CAA).
9. High value cash transactions inconsistent with profile (Monthly)	➔ The alerts are generated for the cash transactions whose transaction amount is >= INR 5.00 lac (threshold limit) and their occupation code must be 41, 42, 43, 45, 46, 54, 61 or 62. (41-teacher, 42-Judge, 43- bank employees, 45-state/central Govt. Emp, 46-othrs salary earners, 54-Pensioners, 61-student, 62- House wife).
10. Cash Deposits Between 09 to 10 lakh in a Month (Monthly)	➔ Alerts generated for the accounts whose cash transactions amount in between INR 9.00 lac and INR 9,99,999.00 and number of such transactions must be >= 5 (threshold) in a month.
11. Cash Deposits Between 40 to 50 thousands (Monthly)	➔ Alerts generated for the accounts whose transaction amount in between INR 40,000 and INR 49,999. ➔ Alerts generated for all such accounts transaction wise for a month. ➔ Number of such transactions must be >=8 (threshold) in a

	MONTH.
12. Frequent Low Cash Deposits in a month:	➔ Alerts generated for the accounts, if it satisfies the below conditions ➔ The deposit amount of transaction should be = Min. deposit Amount (threshold: INR 5000.00) and <40,000.00 Max. deposit Amount (threshold: INR 39,999.99). ➔ Total number of deposit in cash for an account must be >= Deposit Count (threshold:10).
13. Frequent Low Cash Withdrawals (Monthly)	➔ Alerts generated for the accounts, if it satisfies the below conditions: ➔ The Withdrawal in cash should be = Min. withdrawal Amount in cash (threshold: INR 5000.00) and <40,000.00 Max. withdrawal Amount in cash (threshold: INR 39,999.99). ➔ Total number of withdrawal in cash transactions for an account must be >= Deposit Count (threshold: 10).
14. One to Many Fund Transfer (Monthly):	➔ All transactions must be are in non-cash. ➔ Single account transfer proceeds to multiple accounts of the bank. ➔ The accounts may be related or may not be related. ➔ Alert is generated on the basis of number of transfers between accounts. ➔ As for e.g., account of A to B,C,D,E,F,G,H …… . ➔ Non-cash transfer/withdrawals are >= INR 10,00,000.00 (threshold) and ➔ Number of such transactions should be >= 10 (threshold) in a month.
15. Many to One Fund Transfer (MonthlyONTHLY):	➔ All transactions must be are in non-cash. ➔ Multiple accounts of the bank transfer proceeds to SINGLE A/cs of the bank. ➔ The accounts may be related or may not be related. ➔ Alert is generated on the basis of number of transfers between accounts. ➔ As for e.g., accounts of B,C,D,E,F,G,H etc. to A. ➔ Non-cash transfers/Credits are >= INR10,000.00 (threshold) and ➔ Number of such transactions/ credits should be >= 10 (threshold) in a month.

16. Repayment of loan in cash (Monthly)	➔ The alert is generated on the basis of repayment of Loans/Advances by cash. ➔ Repayment of loan in cash is in a monthly basis. ➔ If its flow code is 'COLST' and transaction amount is >= INR10.00 lac (threshold) then the alert will generate. [COLST= Collection of standard accounts]
17. Frequent Locker Operations (Monthly)	➔ It is an existing IBA alert ➔ It is an off-line Alert, maintained by the cell. ➔ Alert is generated on the basis of locker numbers put manually. ➔ As for e.g. if a single locker number is operated >= 15 times (putting manually) in a month, then alert will be generated for that locker number. ➔ Presently number of Locker operations are chosen manually as per requirement (as existing).
18. High value cash transactions in NPO (Monthly)	➔ An alert will be generated on cash transactions of accounts whose customer type in '09', '26' or '171' and the transaction amount >=INR 5.00 lac (09- Trust, 26- NGO, 171-N P Institution).
19. High Value Inward Remittance (Monthly)	➔ The alert is generated on individual deposit transactions, mostly is in non-cash. ➔ If a deposit transaction whose narration is starting with 'By DD' or it contains text like 'PAY ORDER' or 'RTGS' or 'NEFT' or Transaction Instrument Code is 'CHQ' and the transaction amount is >= INR 10.00 lac then the alert will generate.
20. Inward Remittance in a Newly opened Account	➔ The alert is generated on individual deposit/trfd. transactions, mostly are in non-cash deposits ➔ The age of the account must be <= 6 months. ➔ If a deposit transaction whose narration is starting with 'By DD' or it contains text like 'PAY ORDER' or 'RTGS' or 'NEFT' or transaction instrument code is 'CHQ' and the transaction amount is >= INR 5.00 lac then the alert will generate. ➔ Pensioners are not to be considered for the alert.
21. Inward Remittance Inconsistent with Client Profile (Monthly)	➔ The alert is generated on individual deposit transactions, if it satisfies the following conditions: ➔ The alert is generated on individual deposit/trfd. transactions, mostly are in non-cash deposits ➔ If a deposit transaction whose narration is starting with 'By DD' or it contains text like 'PAY ORDER' or 'RTGS' or 'NEFT' or

	transaction instrument code is 'CHQ' etc. and the transaction amount is >= INR 5.00 lac then the alert will generate. ➔ The occupation code should be 41, 42, 43, 44, 45, 46, 47, 54, 61 or 62.

Appendix- C

Sl No.	Type of Parameter for Alert Generation	Threshold Fixed by HO
1	Daily Cash Holding Report of the Branches	Cash Retention Limit of the Branch
2.	High Value Transactions in Savings A/Cs other than those under Product Code 'SBSTF	All types of transactions in which individual transaction amount is more than or equal to Rs. 5 Lacs.
3.	High Value Transaction in Savings/Current A/Cs opened within six months from the date to which the report pertains.	All types of transactions in whichindividual transaction amount is more than or equal to Rs. 5 Lacs (for CAA)and Rs. 2 Lacs (for SBA).
4.	High Value Transactions in staff A/Cs under Scheme Code, 'SBSTF' and 'ODSTF	Cash Deposit/Withdrawal transactions in which individual transaction amount is more than or equal to Rs. 20000.00 and Transfer & Clearing transactions in which individual transaction amount is more than or equal to Rs. 125000.00
5.	High Value Transactions in Current A/Cs	All types of transactions in which individual transaction amount is more than or equal to Rs. 25 Lacs.
6.	Term Deposit Accounts opened with Preferential Rate of Interest	All type of TD accounts in which Preferential Rate of Interest has been allowed
7.	TOD given in Savings Account	All type of Savings Accounts in which Overdraft facility has been allowed
8.	TOD given in Current Account	All type of Current Accounts in which Overdraft facility has been allowed
9.	Conversion of Inoperative/Dormant Account to Operative Account	All type of Savings & Current Accounts which have been converted into Operative/Active Status.
10.	Transaction in Marginal Deposit Account	All transactions of the account occurred in a day
11.	Transactions in deposit suspense including sundry collection –in –transit Account	All transactions of the account occurred in a day