

funds are co-mingled at the level of Bank, the Bank shall look for the beneficial owners.

e) Bank shall, at their discretion rely on the 'customer due diligence' (CDD) done by an intermediary, provided that the intermediary is a regulated and supervised entity and has adequate systems in place to comply with the KYC requirements of the customers.

f) The ultimate responsibility for knowing the customer lies with the Bank.

B. Simplified Due Diligence

37. Simplified norms for Self Help Groups (SHGs)

a) CDD of all the members of SHG shall not be required while opening savings bank account of SHG.

b) CDD all the office bearers shall suffice.

c) No separate CDD as per the CDD procedure mentioned in Section 15 of the members of office bearers shall be necessary at the time of credit linking of SHGs.

38. Procedure to be followed by banks while opening accounts of foreign students

a) Banks shall, at their option, open a Non Resident Ordinary (NRO) bank account of a foreign student on the basis of his/ her passport (with visa & immigration endorsement) bearing the proof of identity and address in the home country together with a photograph and a letter offering admission from the educational institution in India.

i. Provided that a declaration about the local address shall be obtained within a period of 30 days of opening the account and the said local address is verified.

ii. Provided further that pending the verification of address, the account shall be operated with a condition of allowing foreign remittances not exceeding USD 1,000 or equivalent into the account and a cap of rupees fifty thousand on aggregate in the same, during the 30-day period.

b) The account shall be treated as a normal NRO account, and shall be operated in terms of Reserve Bank of India's instructions on Non-Resident Ordinary Rupee (NRO) Account, and the provisions of PRMA. 1999.

c) Students with Pakistani nationality shall require prior approval of the

39. Simplified KYC norms for Foreign Portfolio investors) (FPLs)

Accounts of FPIs which are eligible / registered as per SEBI guidelines, for the purpose of investment under Portfolio Investment Scheme (PIS), shall be opened by accepting KYC documents as detailed in Annexure-I, subject to Income Tax (FATCA / CRS) Rules .

Provided that banks shall obtain undertaking from FPIs or the Global Custodian acting on behalf of the FPI that as and when required, the exempted documents as detailed in Annexure-I will be submitted.

Chapter VII Record Management

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

- 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 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 transaction;
 - 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;

g) Maintain records of the identity and address of their customer, and records in respect of transactions referred to in Rule 3 in hard or soft format.

Chapter VIII

Reporting Requirements to Financial Intelligence Unit – India

41. Bank 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.

42. The reporting formats and comprehensive reporting format guide, prescribed / released by FIU-IND and Report Generation Utility and Report Validation Utility developed to assist Bank in the preparation of prescribed reports shall be taken note of. The editable electronic utilities to file electronic Cash Transaction Reports (CTR) / Suspicious Transaction Reports (STR) which FIU-IND has placed on its website shall be made use of by Bank which are yet to install/adopt suitable technological tools for extracting CTR / STR from their live transaction data.

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

44. 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.

45. Reports to be furnished to Financial Intelligence Unit – India.

(1) Cash Transaction 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

taken place within a month and the aggregate value of such transaction exceeds Rupees ten lakh. However, individual entries below Rs. 50,000/- will not be reported in the Cash Transaction Report.

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

iii. A copy of monthly CTR submitted on its behalf to FIU-IND is available at the concerned branch (through MIS Report: Misc Reports Module under SENSRT – 5/7 & 5/7a) for production to auditors/Inspectors, when asked for.

(2) Suspicious Transaction Reports (STR)

i. While determining suspicious transactions, bank will be guided by the definition of – suspicious transaction II as contained in PMLA Rules as amended from time to time.

“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.

ii. It is likely that in some cases transactions are abandoned/ aborted by customers on being asked to give some details or to provide documents, Bank will report all such attempted transactions in STRs, even if not completed by the customers, irrespective of the amount of the transaction.

- iii. Bank to submit STRs if it has reasonable ground to believe that the transaction involves proceeds of crime irrespective of the amount of the transaction and/or the threshold limit envisaged for predicate offences in part B of Schedule of PMLA, 2002.
- iv. Bank will ensure furnishing of STR within seven days of arriving at a conclusion by the Principal Officer of the Bank that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature.
- v. Bank will ensure not to put any restrictions on operations in the accounts where an STR has been filed. The submission of STR will be kept strictly confidential, as required under PML Rules and it will be ensured that there is no tipping off to the customer at any level.
- vi. 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, 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.
- vii. For effective monitoring of transactions of the customers, Bank should implement an AML software – TCS Bancs Compliance (AML + version 6.0) for generation of AML alerts on day to day basis based on the pre-defined scenarios, as advised by Indian Banks Association (IBA) / Financial Intelligence Unit – India (FIU-IND) from time to time. These scenarios will be periodically reviewed to make them more effective based on the feedback received and experience gained. Further, an indicative list of behavioral/observation based scenarios has been circulated vide KYC AML Division Circular no. 10/2018 dated 04.06.2018. In case any suspicious transaction is detected, the same be reported to Centralized AML Cell for onward submission of Suspicious Transaction Report (STR) to Financial Intelligence Unit – India (FIU-IND) through FIN net Gateway after getting the approval of Principal Officer of the Bank.

Indicative list of various types of indicators i.e. customer behavior and risk based transaction monitoring,, high & medium risk: customers/ products & services / geographies/ locations /alerts for branches/ departments, are attached at

Annexure – II

(3) Counterfeit Currency Report (CCR)

Cash transactions were 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.

(4) Non profit Organizations Transaction report [NTR]

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

(5) Cross-border Wire Transfer (CWTR)

Bank will file Cross-Border Wire Transfer Report (CWTR) to the Director, Financial Intelligence Unit-India by 15th of succeeding month for all across border wire transfers of the value of more than Rs 5 lakh or its equivalent in foreign currency where either the origin or destination of fund is in India.

46. Internal Control System

i. At each Zonal Office, an Officer in the rank of Assistant General Manager / Chief Manager be designated as Nodal Officer for compliance of KYC Policy in all Circle Offices under its jurisdiction.

ii. Dy. Money Laundering Reporting Officer (DMLRO) cum Circle Compliance Officer (DMLRO cum CCO): At each Circle Office, an Officer, not below the rank of Chief Manager, shall be designated as DMLRO cum CCO, who would be responsible for compliance of KYC Policy in all the branches under the allotted Circle Office. He will prepare STRs pertaining to local adverse media reports, Law Enforcement Agency enquiries, public complaints, behavioral scenarios, attempted transactions etc. in all the branches under allotted Circle Office and will send STRs to Centralized AML Cell. Similarly, if during execution of his duties, DMLRO cum CCO observes any money laundering activity at BO/CO, he will escalate the same to Centralized AML Cell. DMLRO-cum-CCO to ensure that field functionaries are sensitized on KYC /AML guidelines and ensure that no money laundering activities take place in the branches under his/her jurisdiction. For this purpose he/she should also ensure on-site supervision by visiting the branches under his/her jurisdiction for random checking of compliance of KYC / AML guidelines of the Bank.

iii. Centralized AML Cell: Monitoring, analysis & closure of AML alerts, including Trade Based Money Laundering (TBML) alerts, shall be done at Centralized AML Cell on day to day basis. Makers/ Checkers at Centralized AML Cell will analyze alerts pertaining to their respective assigned Zones / Circles on day to day basis and will close the alerts after thorough analysis of the transactions / alerts and ensuring that all the transactions are genuine in nature & match with the business profile of customers. Post-closure scrutiny of closed alerts (@20%) shall be undertaken at Centralized AML cell by officers upto Scale-III. Further, Chief Managers at Centralized AML cell will also review / scrutinize at least 5% of the closed alerts, pertaining to their respective assigned Zones / Circles, on sample basis. They will also ensure that necessary corrective steps are initiated for the discrepancies observed during sample checking.

STRs on all suspicious transactions shall be put up to Principal Officer immediately for approval and onward submission to FIU-IND. Similarly, STRs on adverse media reports, Law Enforcement Agency enquiries etc. shall also be prepared and put up to Principal Officer.

During analysis of alerts, special attention shall be given to alerts pertaining to TBML, High Risk Customers, Politically Exposed Persons & High Value Transactions.

iv. Incumbent Incharge of branches will allocate duties and responsibilities for opening of accounts through an Office Order to the staff members, Senior Officers from the Zonal / Circle Offices, during their visits to the branches will ensure that KYC / AML guidelines are being strictly adhered to as per the laid down procedures, keeping in view the risk involved in a transaction, account or banking/business relationship.

v. For discharging the responsibilities effectively, the Principal Officer and other appropriate staff should have timely access to Customer Identification Data and other Customer Due Diligence information, transaction records and other relevant information.

vi. Any changes in KYC Policy may be implemented after approval of the Board.

Chapter IX

Requirements / Obligations under International Agreements
Communications from International Agencies

47. Bank shall ensure that in terms of Section 51A of the Unlawful Activities (Prevention) (UAPA) Act. 1967, they do not have any account in the name of

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:

a) The "ISIL (Da'esh) & Al-Qaida Sanctions List", which includes names of individuals and entities associated with the Al-Qaida. The updated ISIL & Al-Qaida Sanctions List is available at

<https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt=htdocs/resources/xsl/en/al-qaida-r.xsl>

b) The "1988 Sanctions List", consisting of individuals (Section A of the consolidated list) and entities (Section B) associated with the Taliban which is available at

<https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt=htdocs/resources/xsl/en/al-qaida-r.xsl>

48. 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 as required under UAPA notification dated August 27, 2009.

49. In addition to the above, other UNSCRs circulated by the Reserve Bank in respect of any other jurisdictions / entities from time to time shall also be taken note of.

50. Freezing of Assets under of Unlawful Activities (Prevention) Act, 1967

The procedure laid down in the UAPA Order dated August 27, 2009 (Annexure-III) of this KYC Policy shall be strictly followed and meticulous compliance with the Order issued by the Government shall be ensured.

51. 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 50 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.

Chapter X

Other Instructions

52. 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 banking 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

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

Bank shall capture the KYC information for sharing with the CKYCR in the

prepared for 'Individuals' and 'Legal Entities' as the case may be. 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 .

The KYC data / documents pertaining to all new individual accounts opened on or after January 1, 2017 have to be invariably uploaded with CERSAI in terms of the provisions of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 within ten days of opening the accounts.

54. Reporting requirement under Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS)

Under FATCA and CRS, Bank shall adhere to the provisions of Income Tax Rules 114F, 114G and 114H and determine whether they are a Reporting Financial Institution as defined in Income Tax Rule 114F and if so, shall take following steps for complying with the reporting requirements:

a) Register on the related e-filing portal of Income Tax Department as Reporting Financial Institutions at the link

<https://incometaxindiaefiling.gov.in/> post login → My Account

→ Register as Reporting Financial Institution,

b) Submit online reports by using the digital signature of the 'Designated Director' by either uploading the Form 61B or 'NIL' report, for which, the scheme prepared by Central Board of Direct Taxes (CBDT) shall be referred to.

Explanation: Bank shall refer to the spot reference rates published by Foreign Exchange Dealers' Association of India (FEDAI) on their website at <http://www.fedai.org.in/RevaluationRates.aspx> for carrying out the due diligence procedure for the purpose of identifying reportable accounts in terms of Rule 114H.

c) Develop Information Technology (IT) framework for carrying out due diligence procedure and for recording and maintain the same, as provided in Rule 114H.

d) Develop a system of audit for the IT framework and compliance with Rules 114F, 114G and 114H of Income Tax Rules.

e) Constitute a "High Level Monitoring Committee" under the Designated Director or any other equivalent functionary to ensure compliance.

f) Ensure compliance with updated instructions / rules / guidance notes / Press releases / issued on the subject by Central Board of Direct Taxes (CBDT) from time to time and available on the web site <http://www.incometaxindia.gov.in/Pages/default.aspx>. may take note of the following:

i. Updated Guidance Note on FATCA and CRS

ii. A press release on 'Closure of Financial Accounts' under Rule 114H (8).

55. 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.

56. Operation of Bank Accounts & Money Mules

The instructions on opening of accounts and monitoring of transactions shall be strictly adhered to, in order to minimize the operations of "Money Mules" which are used to launder the proceeds of fraud schemes (e.g., phishing and identity theft) by criminals who gain illegal access to deposit accounts by recruiting third parties which act as "money mules." If it is established that an account opened and operated is that of a Money Mule, it shall be deemed that the bank has not complied with these directions.

57. Collection of Accounts Payee Cheques

Account payee cheques for any person other than the payee constituent shall not be collected. Bank shall, at their option, collect account payee cheques drawn for an amount not exceeding rupees fifty thousand to the account of their customers who are co-operative credit societies, provided the payees of such cheques are the constituents of such co- operative credit societies.

58. (a) A Unique Customer Identification Code (UCIC) shall be allotted while entering into new relationships with individual customers as also the existing customers by bank.

(b) The bank shall not issue UCIC to all walk-in / occasional customers such as buyers of pre- paid instruments / purchasers of third party products. However, UCIC shall be allotted to such walk-in customers who have frequent transactions. 59. Introduction of New Technologies – Credit Cards / Debit Cards / Smart Cards / Gift Cards / Mobile Wallet / Net Banking / Mobile Banking / RTGS / NEFT / ECS / IMPS etc.

Adequate attention shall be paid by Bank to any money-laundering and financing of terrorism threats that may rise from new or developing technologies and it shall be ensured that appropriate KYC procedures issued from time to time are duly applied before introducing new products / services / technologies. Agents used for marketing of credit cards shall also be subjected to due diligence and KYC measures.

60. Correspondent Banks

Correspondent banking is the provision of banking services by one bank (the – correspondent I) to another bank (the – respondent bank II). These services include cash/funds management, international wire transfers, drawing arrangements for demand drafts and mail transfers, payable-through-accounts, cheques clearing etc.

Bank will have a policy approved by the Board, or by a committee headed by the Chairman / CEO /MD to lay down parameters for approving correspondent banking relationships subject to the following conditions:

- a) Sufficient Information in relation to the nature of business of the bank including information on management, major business activities, level of AML / CFT compliance, purpose of opening the account, identity of any third party entities that will use the correspondent banking services, and regulatory / supervisory framework in the bank's home country shall be gathered.
- b) The accounts of the respondent banks will be opened with the prior approval of International Banking Division, Head Office, who would also be doing the due diligence in terms of the guidelines issued by RBI and Govt. of India. Similarly, IBD, HO will complete due diligence requirements in correspondent banking relationships where Bank is availing correspondent banking services from other banks.
- c) Post facto approval of the Board at its next meeting shall be obtained for the proposals approved by the Committee.
- d) The responsibilities of each bank with whom correspondent banking relationship is established shall be clearly documented.
- e) In the case of payable-through-accounts, the Bank shall satisfy that the respondent bank has verified the identity of the customers having direct access to the accounts and is undertaking on-going 'due diligence' on them.
- f) The Bank shall ensure that the respondent bank is able to provide the relevant customer identification data immediately on request.

g) Correspondent relationship shall not be entered into with a shell bank (i.e. a bank which is incorporated in a country where it has no physical presence and is not affiliated to any regulated financial group).

h) It shall be ensured that the respondent banks do not permit their accounts to be used by shell banks.

i) Bank will be cautious with respondent banks located in jurisdictions which have strategic deficiencies or have not made sufficient progress in implementation of FATF Recommendations.

j) Bank will ensure *that respondent banks have KYC / AML policies and procedures in place and apply enhanced 'due diligence' procedures for transactions carried out through the correspondent accounts.

61. Wire transfer

Bank shall ensure the following while effecting wire transfer:

a) All cross-border wire transfers including transactions using credit or debit card shall be accompanied by accurate and meaningful originator information such as name, address and account number or a unique reference number, as prevalent in the country concerned in the absence of account.

b) Exception. Interbank transfers and settlements where both the originator and beneficiary are banks or financial institutions shall be exempt from the above requirements.

c) Domestic wire transfers of rupees fifty thousand and above shall be accompanied by originator information such as name, address and account number.

d) Customer Identification shall be made if a customer is intentionally structuring wire transfer below rupees fifty thousand to avoid reporting or monitoring. In case of non-cooperation from the customer, efforts shall be made to establish his identity and STR shall be made to FIU-IND .

e) Complete originator information relating to qualifying wire transfers shall be preserved at least for a period of five years by the ordering bank.

f) A bank processing as an intermediary element of a chain of wire transfers shall ensure that all originator information accompanying a wire transfer is retained with the transfer.

g) The receiving intermediary bank shall transfer full originator information accompanying a cross-border wire transfer and preserve the same for at least

five years if the same cannot be sent with a related domestic wire transfer, due to technical limitations.

h) All the information on the originator of wire transfers shall be immediately made available to appropriate law enforcement and / or prosecutorial authorities on receiving such requests.

i) Effective risk-based procedures to identify wire transfers lacking complete originator information shall be in place at a beneficiary bank.

j) Beneficiary bank shall report transaction lacking complete originator information to FIU-IND as a suspicious transaction.

k) The beneficiary bank shall seek detailed information of the fund remitter with the ordering bank and if the ordering bank fails to furnish information on the remitter, the beneficiary shall consider restricting or terminating its business relationship with the ordering bank.

62. 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 issued of travellers' cheques for value of rupees fifty thousand and above shall be effected by debit to the customer's accounts 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.

63. Quoting of PAN

Permanent account number (PAN) 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.

64. Selling Third party products

Bank acting as agents while selling third party products as per regulations in force from time to time shall comply with the following aspects for the purpose of these directions:

a) The identity and address of the walk-in-customer shall be verified for transactions above rupees fifty thousand as required under Section 13(e) of this Directions.

b) Transaction details of sale of third party products and related records shall be maintained as prescribed in Chapter VII Section 39.

c) AML software capable of capturing, generating and analyzing alerts for the purpose of filing CTR / STR in respect of transactions relating to third party products with customers including walk-in customers shall be available.

d) Transactions involving rupees fifty thousand and above shall be undertaken only by:

i. Debit to customers' account or against cheques; and

ii. Obtaining and verifying the PAN given by the account based as well as walk-in customers.

e) Instruction at 'd' above shall also apply to sale of Bank's own products, payment of dues of credit cards / sale and reloading of prepaid / travel cards and any other product for rupees fifty thousand and above.

65. At-par cheque facility availed by co-operative banks

a) The 'at par' cheque facility offered by Bank to co-operative banks shall be monitored and such arrangements be reviewed to assess the risks including credit risk and reputational risk arising there from.

b) The right to verify the records maintained by the customer cooperative banks / societies for compliance with the extant instructions on KYC and AML under such arrangements shall be retained by Bank.

66. Issuance of Prepaid Payment Instruments (PPIs):

Bank shall ensure that the instructions issued by Department of Payment and Settlement System of Reserve Bank of India through their Master Direction are strictly adhered to.

67. Hiring of Employees and Employee training

a) Adequate screening mechanism as an integral part of their personnel recruitment/ hiring process shall be put in place.

b) 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.

KYC documents for eligible FPIs under PIS FPI Type

Document Type		Category I	Category II		Category III
Entity Level	Constitutive Documents (Memorandum and Articles of Association, Certificate of Incorporation etc.)	Mandatory	Mandatory	Mandatory	Mandatory
Proof of Address	Mandatory (Power of Attorney mentioning the address is acceptable address proof)	Mandatory (Power of Attorney the mentioning the address is acceptable as address proof)	Mandatory other than Power of Attorney		
PAN	Mandatory	Mandatory	Mandatory		
Financial Data	Exempted *	Exempted *	Mandatory		
SEBI Registration Certificate	Mandatory	Mandatory	Mandatory		
Board Resolution @@	Exempted *	Mandatory	Mandatory		
Senior Management (Whole Time Directors / Partners / Trustees /etc.)	List	Mandatory	Mandatory	Mandatory	
Proof of Identity	Exempted *	Exempted *	Entity declares* on letter head full name, nationality, date of birth or submits photo identity proof		
Proof of Address	Exempted*	Exempted*	Declaration on Letter Head *		
Photographs	Exempted	Exempted	Exempted*		

Authorized Signatories	List and Signatures	Mandatory – list of Global Custodian signatories can be given in case of PoA to global Custodian	Mandatory – list of Global Custodian signatories can be given in case of PoA to global Custodian	Mandatory
Proof of Identity	Exempted *	Exempted *	Mandatory	
Proof of Address	Exempted *	Exempted *	Declaration on Letter Head *	
Photographs	Exempted	Exempted	Exempted *	
Authorized Signatories	List and Signatures	Mandatory – list of Global Custodian signatories can be given in case of PoA to global Custodian	Mandatory – list of Global Custodian signatories can be given in case of PoA to global Custodian	Mandatory
Proof of Identity	Exempted *	Exempted *	Mandatory	
Proof of Address	Exempted *	Exempted *	Declaration on Letter Head *	
Photographs	Exempted	Exempted	Exempted *	
Ultimate Beneficial Owner (UBO)	List	Exempted *	Mandatory (can declare – no UBO over 25% II)	Mandatory
Proof of Identity	Exempted *	Exempted *	Mandatory	
Proof Address	Exempted *	Exempted *	Declaration on Letter Head *	
Photographs	Exempted	Exempted	Exempted *	
* Not required while opening the bank account. However, FPIs concerned may submit an undertaking that upon demand by Regulators / Law Enforcement Agencies the relative document/s would be submitted to the bank.				
@@ FPIs from certain jurisdictions where the practice of passing Board Resolution for the purpose of opening bank accounts etc. is not in vogue, may submit 'Power of Attorney granted to Global Custodian / Local Custodian in lieu of Board Resolution'				
Category		Eligible Foreign Investors		
I.		Government and Government related foreign investors such as Foreign Central Banks. Governmental		

	International / Multilateral Organizations / Agencies.
II.	a) Appropriately regulated broad based funds such as Mutual Funds, Investment Trusts, Insurance / Reinsurance Companies, Other Broad Based Funds etc. b) Appropriately regulated entities such as Banks, Asset Management Companies, Investment Managers/ Advisors, Portfolio Managers etc. c) Board based funds whose investment manager is appropriately regulated. d) University Funds and Pension Funds. e) University related Endowments already registered with SEBI as FII / Sub Account.
III.	All other eligible foreign investors investing in India under PIS route not eligible under Category I and II such as Endowments, Charitable Societies / Trust, Foundations, Corporate Bodies, Trusts, Individuals, Family Offices, etc.
III.	All other eligible foreign investors investing in India under PIS route not eligible under Category I and II such as Endowments, Charitable Societies / Trust, Foundations, Corporate Bodies, Trusts, Individuals, Family Offices, etc.

ANNEXURE – II

➔ INDICATIVE LIST OF VARIOUS TYPES OF INDICATORS I.E. CUSTOMER BEHAVIOUR AND RISK BASED TRANSACTION MONITORING, HIGH & MEDIUM

**RISK: CUSTOMERS/ PRODUCTS & SERVICES/ GEOGRAPHIES/
LOCATIONS/ALERTS FOR BRANCHES/ OFFICES:**

**1. INDICATIVE LIST OF CUSTOMER BEHAVIOUR & RISK BASED TRANSACTION
MONITORING:**

- i. Customers who are reluctant in providing normal 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.
- ii. Customer expressing unusual curiosity about secrecy of information involved in the transaction.
- iii. Customers who decline to provide information that in normal circumstances would make the customer eligible for banking services.
- iv. Customer giving confusing details about a transaction.
- v. Customer 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.
- vi. Customers who use separate tellers to conduct cash transaction or foreign exchange transactions.
- vii. Customers who deposit cash / withdrawals by means of numerous deposit slips / cheques leaves so that the total of each deposits is unremarkable, but the total of all credits / debits is significant.
- viii. Customer's representatives avoiding contact with the branch.
- ix. Customers who repay the problem loans unexpectedly.
- x. Customers who appear to have accounts with several institutions within the same locality without any apparent logical reason.
- xi. Customers seeks 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.
- xii. Customer regularly issues large value cheques without balance and then deposits cash.
- xiii. Sudden transfer of funds from unrelated accounts through internet (or such other electronic channels) and subsequent quick withdrawal through ATM.

A. Transactions Involving Large Amounts of Cash:

- i. Exchanging an unusually large amount of small denomination notes for those of higher denomination;
- ii. Purchasing or selling of foreign currencies in substantial amounts by cash settlement despite the customer having an account with the bank;
- iii. Frequent withdrawal of large amounts by means of cheques, including traveller's cheques;
- iv. Frequent withdrawal of large cash amounts that do not appear to be justified by the customer's business activity;
- v. Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received an unexpected large credit from abroad;
- vi. Company transactions, both deposits and withdrawals, that are denominated by unusually large amounts of cash, rather than by way of debits and credits normally associated with the normal commercial operations of the company, e.g. cheques, letters of credit, bills of exchange etc;
- vii. Depositing cash by means of numerous credit slips by a customer such that the amount of each deposit is not substantial, but the total of which is substantial.

B. Transactions that do not make Economic Sense:

- i. A customer having a large number of accounts with the same bank, with frequent transfers between different accounts;
- ii. Transactions in which assets are withdrawn immediately after being deposited,

Unless the customer's business activities furnish a plausible reason for immediate withdrawal .

C. Activities not consistent with the Customer's Business:

- i. Corporate accounts where deposits or withdrawals are primarily in cash rather than cheques.

ii. Corporate accounts where deposits & withdrawals by cheque/telegraphic transfers/foreign inward remittances/any other means are received from/made to sources apparently unconnected with the corporate business activity/dealings.

iii. Unusual applications for DD/TT/PO against cash.

iv. Accounts with large volume of credits through DD/TT/PO whereas the nature of business does not justify such credits.

v. Retail deposit of many cheques but rare withdrawals for daily operations.

D. Attempts to avoid Reporting/Record-keeping Requirements:

i. A customer who is reluctant to provide information needed for a mandatory report, to have the report filed or to proceed with a transaction after being informed that the report must be filed.

ii. Any individual or group that coerces/induces or attempts to coerce/induce a bank employee not to file any reports or any other forms.

iii. An account where there are several cash deposits/withdrawals below a specified threshold level to avoid filling of reports that may be necessary in case of transactions above the threshold level, as the customer intentionally splits the transaction into smaller amounts for the purpose of avoiding the threshold limit.

E. Unusual Activities:

i. An account of a customer who does not reside/have office near the branch even though there are bank branches near his residence/office.

ii. A customer who often visits the safe deposit area immediately before making cash deposits, especially deposits just under the threshold level.

iii. Funds coming from the list of countries/centers, which are known for money laundering.

iii. Funds coming from the list of countries/centers, which are known for money laundering.

- i. A customer/company who is reluctant to provide complete information regarding the purpose of the business, prior banking relationships, officers or directors, or its locations.
- ii. A customer/company who is reluctant to reveal details about its activities or to provide financial statements.
- iii. A customer who has no record of past or present employment but makes frequent large transactions.

G. Certain Suspicious Funds Transfer Activities:

- i. Sending or receiving frequent or large volumes of remittances to/from countries outside India.
- ii. Receiving large TT/DD remittances from various centers and remitting the consolidated amount to a different account/center on the same day leaving minimum balance in the account.
- iii. Maintaining multiple accounts, transferring money among the accounts and using one account as a master account for wire/funds transfer.

H. Certain Bank Employees arousing Suspicion:

- i. An employee whose lavish lifestyle cannot be supported by his or her salary.
- ii. Negligence of employees/willful blindness is reported repeatedly.

I. Bank no longer knows the true identity:

When a bank believes that it would no longer be satisfied that it knows the true identity of the account holder .

J. Some examples of suspicious activities/transactions to be monitored by the operating staff:

- i. Multiple A
- ii. Large cash transactions
- iii. Frequently converting large amounts of currency from small to large denomination notes

- iv. Placing funds in term Deposits and using them as security for more loans.
- v. Large deposits immediately followed by wire transfers.
- vi. Sudden surge in activity level.
- vii. Same funds being moved repeatedly among several accounts.
- viii. Multiple deposits of money orders, Banker's cheques, drafts of third Parties
- ix. Multiple deposits of Banker's cheques, demand drafts, cross/bearer.
- x. Cheques of third parties onto the account followed by immediate cash withdrawals.
- xi. Transactions inconsistent with the purpose of the account.
- xii. Maintaining a low or overdrawn balance with high activity

➔ Check list for prevention money-laundering activity:

i. A customer maintains multiple accounts, transfer money among the accounts and used one account as a master account from which wire/funds transfer originates or

into which wire/funds transfer are received (a customer deposits funds in several accounts, usually in amounts below a specified threshold and the funds are then consolidated into one master account and wired outside the country).

ii. A customer regularly depositing or withdrawing large amounts by a wire transfer to, from, or through countries that are known sources of narcotics or where Bank secrecy laws facilitate laundering money.

iii. A customer sends and receives wire transfers (from financial haven countries) particularly if there is no apparent business reason for such transfers and is not consistent with the customer's business or history.

iv. A customer receiving many small incoming wire transfer of funds or deposits of cheques and money orders, then orders large outgoing wire transfers to another city or country.

v. A customer experiences increased wire activity when previously there has been no regular wire activity.

- vi. Loan proceeds unexpectedly are wired or mailed to an offshore Bank or third party.
- vii. A business customer uses or evidences or sudden increase in wire transfer to send and receive large amounts of money, internationally and/or domestically and such transfers are not consistent with the customer's history.
- viii. Deposits of currency or monetary instruments into the account of a domestic trade or business, which in turn are quickly wire transferred abroad or moved among other accounts for no particular business purpose.
- ix. Sending or receiving frequent or large volumes of wire transfers to and from offshore institutions.
- x. Instructing the Bank to transfer funds abroad and to expect an equal incoming wire transfer from other sources.
- xi. Wiring cash or proceeds of a cash deposit to another country without changing the form of the currency
- xii. Receiving wire transfers and immediately purchasing monetary instruments prepared for payment to a third party.
- xiii. Periodic wire transfers from a person's account/s to Bank haven countries.
- xiv. A customer pays for a large (international or domestic) wire transfers using multiple monetary instruments drawn on several financial institutions.
- xv. A customer or a non-customer receives incoming or makes outgoing wire transfers involving currency amounts just below a specified threshold, or that involve numerous Bank or travellers cheques.
- xvi. A customer or a non-customer receives incoming wire transfers from the Bank to 'Pay upon proper identification' or to convert the funds to banker's cheques and mail them to the customer or non-customer, when the amount is very large (say over Rs. 10 lakhs). The amounts is just under a specified threshold, the funds come from a foreign country or such transactions occur repeatedly.
- xvii. A customer or a non-customer arranges large wire transfers out of the country which are paid for by multiple Banker's cheques (just under a specified threshold)
- xviii. A Non-customer sends numerous wire transfers using currency amounts just below a specified threshold limit.

2. INDICATIVE LIST OF HIGH RISK CUSTOMERS:

- i. Individuals and entities in various United Nation' Security Council Resolutions (UNSCRs) such as UNSC 1267 & 1988 [2011] linked to Al Qaida & Taliban.
- ii. 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
- iii. Individuals and entities in watch lists issued by Interpol and other similar international organizations
- iv. Customer with dubious reputation as per public information locally available or commercially available.
- v. Individuals and entities specifically identified by regulators, FIU and other competent authorities as high-risk
- vi. Customers conducting their business relationship or transactions 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, frequent and unexplained movement of funds between institutions in various geographic locations etc.
- vii. Customers based in high risk countries/jurisdictions or locations as identified by FATF from time to time.
- viii. Politically exposed persons (PEPs) of foreign, customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner,
- ix. Non-resident customers and foreign nationals
- x. Accounts of Embassies / Consulates;
- xi. Off-shore (foreign) corporation/business
- xii. Non face-to-face customers
- xiii. High net worth individuals [HNIs]
- xiv. Firms with 'sleeping partners'
- xv. Companies having close family shareholding or beneficial ownership

- xvi. Complex business ownership structures, which can make it easier to conceal underlying beneficiaries, where there is no legitimate commercial rationale
- xvii. 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
- xviii. Investment Management/ Money Management Company/Personal Investment Company
- xix. 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.
- xx. Client Accounts managed by professional service providers such as law firms, accountants, agents, brokers, fund managers, trustees, custodians, etc
- xxi. Trusts, charities, NGOs/NPOs (especially those operating on a – cross-border II basis) unregulated clubs and organizations receiving donations (excluding NPOs/NGOs promoted by United Nations or its agencies)
- xxii. Money Service Business: including seller of: Money Orders / Travelers" Checks / Money Transmission / Check Cashing / Currency Dealing or Exchange
- xxiii. Business accepting third party checks (except supermarkets or retail stores that accept payroll checks/cash payroll checks)
- xxiv. Gambling/gaming including – Junket Operators II arranging gambling tours
- xxv. 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).
- xxvi. Customers engaged in a business which is associated with higher levels of corruption (e.g. arms manufacturers, dealers and intermediaries.
- xxvii. Customers engaged in industries that might relate to nuclear proliferation activities or explosives.
- xxviii. Customers that may appear to be Multi-level marketing companies etc.

3. INDICATIVE LIST OF MEDIUM RISK CUSTOMERS:

- ii. Import/ Export
- iii. Stock Brokerage
- iv. Gas Station
- v. Car/Boat/ Plane Dealership
- vi. Electronics (wholesale)
- vii. Travel agency
- viii. Used car sales
- ix. Telemarketers
- x. Providers of telecommunications service, internet café, IDD call service ,
phone cards, phone center
- xi. Dot-com company or internet business
- xii. Venture Capital Companies
- xiii. Auctioneers
- xiv. Cash-Intensive Businesses such as restaurants, retail shops, parking
garages, fast food stores, movie theaters, etc.
- xv. Sole Practitioners or Law Firms (small, little known)
- xvi. Notaries (small, little known)
- xvii. Secretarial Firms (small, little known)
- xviii. Accountants (small, little known firms)
- xix. Pawnshops

4. LIST OF HIGH / MEDIUM RISK PRODUCTS & SERVICES:

- i. Electronic funds payment services such as Electronic cash (e.g., stored value
and payroll cards), funds transfers (domestic and international), etc
- ii. Electronic banking
- iii. Private banking (domestic and international)
- iv. Trust and asset management services

- vi. Foreign correspondent accounts
- vii. Trade finance (such as letters of credit)
- viii. Special use or concentration accounts
- ix. Lending activities, particularly loans secured by cash collateral and marketable securities
- x. Non-deposit account services such as Non-deposit investment products and Insurance
- xi. Transactions undertaken for non-account holders (occasional customers)
- xii. Provision of safe custody and safety deposit boxes
- xiii. Currency exchange transactions
- xiv. Project financing of sensitive industries in high-risk jurisdictions
- xv. Trade finance services and transactions involving high-risk jurisdictions
- xvi. Services offering anonymity or involving third parties
- xvii. Services involving banknote and precious metal trading and delivery
- xviii. Services offering cash, monetary or bearer instruments; cross-border transactions,

5. INDICATIVE LIST OF HIGH / MEDIUM RISK GEOGRAPHIES/ LOCATIONS/ COUNTRIES :

Countries/ jurisdictions

- i. Countries subject to sanctions, embargoes or similar measures in the United Nations Security Council Resolutions (-UNSCR II).
- ii. Jurisdictions identified in FATF public statement as having substantial money laundering and terrorist financing (ML/FT) risks (www.fatf-gafi.org)
- iii. Jurisdictions identified in FATF public statement with strategic AML/CFT deficiencies (www.fatf-gafi.org)
- iv. Tax havens or countries that are known for highly secretive banking and corporate law practices
- v. Countries identified by credible sources 1 as lacking appropriate AML/CFT laws, regulations and other measures.

vi. Countries identified by credible sources as providing funding or support for terrorist activities that have designated terrorist organizations operating within them.

vii. Countries identified by credible sources as having significant levels of criminal activity.

viii. Countries identified by the bank as high-risk because of its prior experiences, transaction history, or factors (e.g. legal considerations, or allegations of official corruption).

Locations

i. Locations within the country known as high risk for terrorist incidents or terrorist financing activities (e.g. sensitive locations in Jammu and Kashmir, North east, Naxal affected districts)

ii. Locations identified by credible sources as having significant levels of criminal, terrorist, terrorist financing activity.

iii. Locations identified by the bank as high-risk because of its prior experiences, transaction history, or other factors.

6. Indicative List of High Risk Countries:

The countries identified by Financial Action Task Force [FATF] as high risk countries which continue to show deficiencies in their Anti Money Laundering and Combating of Financing of Terrorism framework will be circulated from time to time.

Annexure III

File No. 14014/01/2019/CFT

Government of India

Ministry of Home Affairs

CTCR Division

New Delhi, dated 14 March 2019

ORDER

Subject: - Procedure for implementation of Section 51A of the Unlawful