

**RBI/ 2008-2009/72
DBOD. AML. BC. No. 12 /14 .01.001/2008-09**

July 1, 2008

The Chairman/CEOs of all Scheduled Commercial Banks (Excluding RRBs) /
all Financial Institutions

Dear Sir,

**Master Circular – Know Your Customer (KYC) norms /
Anti-Money Laundering (AML) standards/
Combating of Financing of Terrorism (CFT)/Obligation of banks under
PMLA, 2002**

Reserve Bank of India has issued regulatory guidelines on Know Your Customer (KYC) norms / Anti Money Laundering (AML) Standards / Combating of Financing of Terrorism (CFT) from time to time. This Master Circular consolidates all the guidelines issued by Reserve Bank of India on KYC/AML/CFT norms up to June 30, 2008.

2. This Master Circular has been placed on the RBI website
(<http://www.rbi.org.in>).

Yours faithfully,

(Vinay Baijal)
Chief General Manager

**MASTER
CIRCULAR**

Know Your Customer(KYC) norms/Anti Money Laundering (AML) Standards/Combating of Financing of Terrorism/Obligations of Banks under Prevention of Money Laundering Act, (PMLA), 2002



(Updated upto June 30, 2008)

**Department of Banking Operations and
Development**

RESERVE BANK OF INDIA

Central Office

Mumbai

The Master Circular can also be viewed and be downloaded from RBI

Website

www.rbi.org.in

Master Circular on Know Your Customer (KYC) norms/Anti-Money Laundering (AML) standards/Combating of Financing of Terrorism (CFT)/Obligation of banks under Prevention of Money Laundering Act, (PMLA), 2002

Purpose

Banks were advised to follow certain customer identification procedure for opening of accounts and monitoring transactions of a suspicious nature for the purpose of reporting it to appropriate authority. These 'Know Your Customer' guidelines have been revisited in the context of the Recommendations made by the Financial Action Task Force (FATF) on Anti Money Laundering (AML) standards and on Combating Financing of Terrorism (CFT). Detailed guidelines based on the Recommendations of the Financial Action Task Force and the paper issued on Customer Due Diligence (CDD) for banks by the Basel Committee on Banking Supervision, with indicative suggestions wherever considered necessary, have been issued. Banks have been advised to ensure that a proper policy framework on 'Know Your Customer' and Anti-Money Laundering measures with the approval of the Board is formulated and put in place.

2. This Master Circular aims at consolidating all the instructions/guidelines issued by RBI on Know Your Customer (KYC) norms/Anti-Money Laundering (AML) standards. The Master Circular has been placed on the RBI website (<http://www.rbi.org.in>).

Previous instructions

A list of circulars issued in this regard is given in Annex – III.

Application

i) The instructions, contained in the master circular, are applicable to all Financial Institutions and all the scheduled commercial banks excluding RRBs. The said guidelines shall also apply to the branches and majority owned subsidiaries located abroad, especially, in countries which do not or insufficiently apply the FATF Recommendations, to the extent local laws permit. When local applicable laws and regulations prohibit implementation of these guidelines, the same should be brought to the notice of Reserve Bank. In case there is a variance in KYC/AML standards prescribed by the Reserve Bank and the host country regulators, branches/overseas subsidiaries of banks are required to adopt the more stringent regulation of the two.

ii) These guidelines are issued under Section 35A of the Banking Regulation Act, 1949 and Rule 7 of Prevention of Money-Laundering (Maintenance of Records of the Nature and Value of Transactions, the Procedure and Manner of Maintaining and Time for Furnishing Information and Verification and Maintenance of Records of the Identity of the Clients of the Banking Companies, Financial Institutions and Intermediaries) Rules, 2005. Any contravention thereof or non-compliance shall attract penalties under Banking Regulation Act.

iii) This Master Circular consolidates all the circulars issued on the subject up to June 30, 2008.

Structure

1. Introduction

1.1 KYC/AML/CFT

1.2 Definition of Customer

2. Guidelines

2.1 General

2.2 KYC Policy

2.3 Customer Acceptance Policy

2.4 Customer Identification Procedure

2.5 Customer Identification Requirements – Indicative guidelines

2.6 KYC guidelines for small deposit accounts

2.7 Monitoring of transactions

2.8 Closure of Accounts

2.9 Risk Management

2.10 Introduction of new technology – credit/debit/smart/gift cards

2.11 Combating Financing of Terrorism

2.12 Correspondent Banking

2.13 Wire Transfers

2.14 Principal Officer

2.15 Maintenance of records of transactions/Information to be preserved/
Maintenance and preservation of records/Cash and Suspicious
transactions reporting to Financial Intelligence Unit-India (FIU-IND)

2.16 Cash and Suspicious Transaction Report

2.17 Customer Education/ Training of Employees /Hiring of Employees

3. Annex

3.1 Annex - I - Indicative List of documents required for opening of
accounts

3.2 Annex – II – List of reporting formats

3.3. Annex – III – List of circulars superseded by the Master Circular

1 Introduction

1.1 Know Your Customer (KYC)/Anti-Money Laundering (AML) / Combating of Financing of Terrorism (CFT)

The objective of KYC/AML/CFT guidelines is to prevent banks from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities. KYC procedures also enable banks to know/understand their customers and their financial dealings better which in turn help them manage their risks prudently.

1.2 Definition of Customer

For the purpose of KYC policy, a 'Customer' is defined as :

- a person or entity that maintains an account and/or has a business relationship with the bank;
- one on whose behalf the account is maintained (i.e. the beneficial owner);
- beneficiaries of transactions conducted by professional intermediaries, such as Stock Brokers, Chartered Accountants, Solicitors etc. as permitted under the law, and
- any person or entity connected with a financial transaction which can pose significant reputational or other risks to the bank, say, a wire transfer or issue of a high value demand draft as a single transaction.

2. Guidelines

2.1 General

i) Banks should keep in mind that the information collected from the customer for the purpose of opening of account is to be treated as confidential and details thereof are not to be divulged for cross selling or any other like purposes. Banks should, therefore, ensure that information sought from the customer is relevant to the perceived risk, is not intrusive, and is in conformity with the guidelines issued in this regard. Any other information from the customer should be sought separately with his/her consent and after opening the account.

ii) Banks should ensure that any remittance of funds by way of demand draft, mail/telegraphic transfer or any other mode and issue of travellers' cheques for value of Rupees fifty thousand and above is effected by debit to the customer's account or against cheques and not against cash payment.

iii) Banks should ensure that the provisions of Foreign Contribution (Regulation) Act, 1976, as amended from time to time, wherever applicable are strictly adhered to.

2.2 KYC Policy

Banks should frame their KYC policies incorporating the following four key elements:

- a) Customer Acceptance Policy;
- b) Customer Identification Procedures;
- c) Monitoring of Transactions; and
- d) Risk Management.

2.3 Customer Acceptance Policy (CAP)

a) Every bank should develop a clear Customer Acceptance Policy laying down explicit criteria for acceptance of customers. The Customer Acceptance Policy must ensure that explicit guidelines are in place on the following aspects of customer relationship in the bank.

- (i) No account is opened in anonymous or fictitious/ benami name(s);
- (ii) Parameters of risk perception are clearly defined in terms of the nature of business activity, location of customer and his clients, mode of payments, volume of turnover, social and financial status etc. to enable categorisation of customers into low, medium and high risk (banks may choose any suitable nomenclature viz. level I, level II and level III). Customers requiring very high level of monitoring, e.g. Politically Exposed Persons (PEPs) may, if considered necessary, be categorised even higher;
- (iii) Documentation requirements and other information to be collected in respect of different categories of customers depending on perceived risk and keeping in mind the requirements of PML Act, 2002 and instructions/guidelines issued by Reserve Bank from time to time;
- (iv) Not to open an account or close an existing account where the bank is unable to apply appropriate customer due diligence measures i.e. bank is unable to verify the identity and /or obtain documents required as per the risk categorisation due to non cooperation of the customer or non reliability of the data/information furnished to the bank. It is, however, necessary to have suitable built in safeguards

to avoid harassment of the customer. For example, decision by a bank to close an account should be taken at a reasonably high level after giving due notice to the customer explaining the reasons for such a decision;

- (v) Circumstances, in which a customer is permitted to act on behalf of another person/entity, should be clearly spelt out in conformity with the established law and practice of banking as there could be occasions when an account is operated by a mandate holder or where an account is opened by an intermediary in fiduciary capacity and
- (vi) Necessary checks before opening a new account so as to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organisations etc.

b) Banks should prepare a profile for each new customer based on risk categorisation. The customer profile may contain information relating to customer's identity, social/financial status, nature of business activity, information about his clients' business and their location etc. The nature and extent of due diligence will depend on the risk perceived by the bank. However, while preparing customer profile banks should take care to seek only such information from the customer, which is relevant to the risk category and is not intrusive. The customer profile is a confidential document and details contained therein should not be divulged for cross selling or any other purposes.

c) For the purpose of risk categorisation, individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile, may be categorised as low risk. Illustrative examples of low risk customers could be salaried employees whose salary structures are well defined, people belonging to lower economic strata of the society whose accounts show small balances and low turnover, Government Departments and Government owned companies, regulators and statutory bodies etc. In such cases, the policy may require that only the basic requirements of verifying the identity and location of the customer are to be met. Customers that are likely to pose a higher than average risk to the bank should be categorised as medium or high risk depending on customer's background, nature and location of activity, country of origin, sources of funds and his client profile etc. Banks should apply enhanced due diligence measures based on the risk assessment, thereby requiring intensive 'due diligence' for higher risk customers, especially those for whom the sources of funds are not clear. Examples of customers requiring higher due diligence include (a) non-resident customers; (b) high net worth individuals; (c) trusts, charities, NGOs and organizations receiving donations; (d) companies having close family shareholding or beneficial ownership; (e) firms with 'sleeping partners'; (f) politically exposed persons (PEPs) of foreign origin; (g) non-face to face customers and (h) those with dubious reputation as per public information available etc.

d) It is important to bear in mind that the adoption of customer acceptance policy and its implementation should not become too restrictive and must not result in denial of banking services to general public, especially to those, who are financially or socially disadvantaged.

2.4 Customer Identification Procedure (CIP)

a) The policy approved by the Board of banks should clearly spell out the Customer Identification Procedure to be carried out at different stages i.e. while establishing a banking relationship; carrying out a financial transaction or when the bank has a doubt about the authenticity/veracity or the adequacy of the previously obtained customer identification data. Customer identification means identifying the customer and verifying his/her identity by using reliable, independent source documents, data or information. Banks need to obtain sufficient information necessary to establish, to their satisfaction, the identity of each new customer, whether regular or occasional, and the purpose of the intended nature of banking relationship. Being satisfied means that the bank must be able to satisfy the competent authorities that due diligence was observed based on the risk profile of the customer in compliance with the extant guidelines in place. Such risk based approach is considered necessary to avoid disproportionate cost to banks and a burdensome regime for the customers. Besides risk perception, the nature of information/documents required would also depend on the type of customer (individual, corporate etc.). For customers that are natural persons, the banks should obtain sufficient identification data to verify the identity of the customer, his address/location, and also his recent photograph. For customers that are legal

persons or entities, the bank should (i) verify the legal status of the legal person/entity through proper and relevant documents; (ii) verify that any person purporting to act on behalf of the legal person/entity is so authorised and identify and verify the identity of that person; (iii) understand the ownership and control structure of the customer and determine who are the natural persons who ultimately control the legal person. Customer identification requirements in respect of a few typical cases, especially, legal persons requiring an extra element of caution are given in paragraph 2.5 below for guidance of banks. Banks may, however, frame their own internal guidelines based on their experience of dealing with such persons/entities, normal bankers' prudence and the legal requirements as per established practices. If the bank decides to accept such accounts in terms of the Customer Acceptance Policy, the bank should take reasonable measures to identify the beneficial owner(s) and verify his/her/their identity in a manner so that it is satisfied that it knows who the beneficial owner(s) is/are.

b) It has been observed that some close relatives, e.g. wife, son, daughter and parents etc. who live with their husband, father/mother and son, as the case may be, are finding it difficult to open account in some banks as the utility bills required for address verification are not in their name. It is clarified, that in such cases, banks can obtain an identity document and a utility bill of the relative with whom the prospective customer is living along with a declaration from the relative that the said person (prospective customer) wanting to open an account is a relative and is staying with him/her. Banks can use any supplementary evidence such as a letter received through post for further verification of the address. While issuing operational instructions to

the branches on the subject, banks should keep in mind the spirit of instructions issued by the Reserve Bank and avoid undue hardships to individuals who are, otherwise, classified as low risk customers.

c) Banks should introduce a system of periodical updation of customer identification data (including photograph/s) after the account is opened. The periodicity of such updation should not be less than once in five years in case of low risk category customers and not less than once in two years in case of high and medium risk categories.

d) An indicative list of the nature and type of documents/information that may be relied upon for customer identification is given in Annex-I to this Master Circular. It is clarified that permanent correct address, as referred to in Annex-I, means the address at which a person usually resides and can be taken as the address as mentioned in a utility bill or any other document accepted by the bank for verification of the address of the customer.

e) It has been brought to our notice that the said indicative list furnished in Annex – I, is being treated by some banks as an exhaustive list as a result of which a section of public is being denied access to banking services. Banks are, therefore, advised to take a review of their extant internal instructions in this regard.

2.5 Customer Identification Requirements – Indicative Guidelines

i) Trust/Nominee or Fiduciary Accounts

There exists the possibility that trust/nominee or fiduciary accounts can be used to circumvent the customer identification procedures. Banks should determine whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary. If so, banks should insist on receipt of satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also obtain details of the nature of the trust or other arrangements in place. While opening an account for a trust, banks should take reasonable precautions to verify the identity of the trustees and the settlors of trust (including any person settling assets into the trust), grantors, protectors, beneficiaries and signatories. Beneficiaries should be identified when they are defined. In the case of a 'foundation', steps should be taken to verify the founder managers/ directors and the beneficiaries, if defined.

ii) Accounts of companies and firms

Banks need to be vigilant against business entities being used by individuals as a 'front' for maintaining accounts with banks. Banks should examine the control structure of the entity, determine the source of funds and identify the natural persons who have a controlling interest and who comprise the management. These requirements may be moderated according to the risk perception e.g. in the case of a public company it will not be necessary to identify all the shareholders.

iii) Client accounts opened by professional intermediaries

When the bank has knowledge or reason to believe that the client account opened by a professional intermediary is on behalf of a single client, that client must be identified. Banks may hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds. Banks also maintain 'pooled' accounts managed by lawyers/chartered accountants or stockbrokers for funds held 'on deposit' or 'in escrow' for a range of clients. Where funds held by the intermediaries are not co-mingled at the bank and there are 'sub-accounts', each of them attributable to a beneficial owner, all the beneficial owners must be identified. Where such funds are co-mingled at the bank, the bank should still look through to the beneficial owners. Where the banks rely on the 'customer due diligence' (CDD) done by an intermediary, they should satisfy themselves that the intermediary is regulated and supervised and has adequate systems in place to comply with the KYC requirements. It should be understood that the ultimate responsibility for knowing the customer lies with the bank.

iv) Accounts of Politically Exposed Persons (PEPs) resident outside India

Politically exposed persons are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States or of Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc. Banks should gather sufficient information on any person/customer of this category intending to establish a relationship and

check all the information available on the person in the public domain. Banks should verify the identity of the person and seek information about the sources of funds before accepting the PEP as a customer. The decision to open an account for a PEP should be taken at a senior level which should be clearly spelt out in Customer Acceptance Policy. Banks should also subject such accounts to enhanced monitoring on an ongoing basis. The above norms may also be applied to the accounts of the family members or close relatives of PEPs.

v) Accounts of non-face-to-face customers

With the introduction of telephone and electronic banking, increasingly accounts are being opened by banks for customers without the need for the customer to visit the bank branch. In the case of non-face-to-face customers, apart from applying the usual customer identification procedures, there must be specific and adequate procedures to mitigate the higher risk involved. Certification of all the documents presented should be insisted upon and, if necessary, additional documents may be called for. In such cases, banks may also require the first payment to be effected through the customer's account with another bank which, in turn, adheres to similar KYC standards. In the case of cross-border customers, there is the additional difficulty of matching the customer with the documentation and the bank may have to rely on third party certification/introduction. In such cases, it must be ensured that the third party is a regulated and supervised entity and has adequate KYC systems in place.

2.6 Small Deposit Accounts

(i) Although flexibility in the requirements of documents of identity and proof of address has been provided in the above mentioned KYC guidelines, it has been observed that a large number of persons, especially, those belonging to low income group both in urban and rural areas are not able to produce such documents to satisfy the bank about their identity and address. This would lead to their inability to access the banking services and result in their financial exclusion. Accordingly, the KYC procedure also provides for opening accounts for those persons who intend to keep balances not exceeding Rupees Fifty Thousand (Rs. 50,000/-) in all their accounts taken together and the total credit in all the accounts taken together is not expected to exceed Rupees One Lakh (Rs. 1,00,000/-) in a year. In such cases, if a person who wants to open an account and is not able to produce documents mentioned in Annex I of this master circular, banks should open an account for him, subject to:

Introduction from another account holder who has been subjected to full KYC procedure. The introducer's account with the bank should be at least six months old and should show satisfactory transactions. Photograph of the customer who proposes to open the account and also his address need to be certified by the introducer,

or

any other evidence as to the identity and address of the customer to the satisfaction of the bank.

ii) While opening accounts as described above, the customer should be made aware that if at any point of time, the balances in all his/her accounts with the bank (taken together) exceeds Rupees Fifty Thousand (Rs. 50,000/-) or total credit in the account exceeds Rupees One Lakh (Rs. 1,00,000/-) in a year, no further transactions will be permitted until the full KYC procedure is completed. In order not to inconvenience the customer, the bank must notify the customer when the balance reaches Rupees Forty Thousand (Rs. 40,000/-) or the total credit in a year reaches Rupees Eighty thousand (Rs. 80,000/-) that appropriate documents for conducting the KYC must be submitted otherwise operations in the account will be stopped.

2.7 Monitoring of Transactions

Ongoing monitoring is an essential element of effective KYC procedures. Banks can effectively control and reduce their risk only if they have an understanding of the normal and reasonable activity of the customer so that they have the means of identifying transactions that fall outside the regular pattern of activity. However, the extent of monitoring will depend on the risk sensitivity of the account. Banks should pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose. Banks may prescribe threshold limits for a particular category of accounts and pay particular attention to the transactions which exceed these limits. Transactions that involve large

amounts of cash inconsistent with the normal and expected activity of the customer should particularly attract the attention of the bank. Very high account turnover inconsistent with the size of the balance maintained may indicate that funds are being 'washed' through the account. High-risk accounts have to be subjected to intensified monitoring. Every bank should set key indicators for such accounts, taking note of the background of the customer, such as the country of origin, sources of funds, the type of transactions involved and other risk factors. Banks should put in place a system of periodical review of risk categorization of accounts and the need for applying enhanced due diligence measures. Such review of risk categorisation of customers should be carried out at a periodicity of **not less** than once in six months.

2.8 Closure of accounts

Where the bank is unable to apply appropriate KYC measures due to non-furnishing of information and /or non-cooperation by the customer, the bank should consider closing the account or terminating the banking/business relationship after issuing due notice to the customer explaining the reasons for taking such a decision. Such decisions need to be taken at a reasonably senior level.

2.9 Risk Management

a) The Board of Directors of the bank should ensure that an effective KYC programme is put in place by establishing appropriate procedures and ensuring their effective implementation. It should cover proper management oversight, systems and controls, segregation of duties, training and other related matters. Responsibility should be explicitly allocated within the bank

for ensuring that the bank's policies and procedures are implemented effectively. Banks should, in consultation with their boards, devise procedures for creating risk profiles of their existing and new customers and apply various anti money laundering measures keeping in view the risks involved in a transaction, account or banking/business relationship.

b) Banks' internal audit and compliance functions have an important role in evaluating and ensuring adherence to the KYC policies and procedures. As a general rule, the compliance function should provide an independent evaluation of the bank's own policies and procedures, including legal and regulatory requirements. Banks should ensure that their audit machinery is staffed adequately with individuals who are well-versed in such policies and procedures. Concurrent/ Internal Auditors should specifically check and verify the application of KYC procedures at the branches and comment on the lapses observed in this regard. The compliance in this regard should be put up before the Audit Committee of the Board on quarterly intervals.

2.10 Introduction of New Technologies – Credit cards/debit cards/ smart cards/gift cards

Banks should pay special attention to any money laundering threats that may arise from new or developing technologies including internet banking that might favour anonymity, and take measures, if needed, to prevent their use in money laundering schemes. Many banks are engaged in the business of issuing a variety of Electronic Cards that are used by customers for buying goods and services, drawing cash from ATMs, and can be used for electronic transfer of funds. Further, marketing of these cards is generally done through

the services of agents. Banks should ensure that appropriate KYC procedures are duly applied before issuing the cards to the customers. It is also desirable that agents are also subjected to KYC measures.

2.11 Combating financing of terrorism

a) In terms of PMLA Rules, suspicious transaction should include *inter alia* transactions which give rise to a reasonable ground of suspicion that these may involve financing of the activities relating to terrorism. Banks are, therefore, advised to develop suitable mechanism through appropriate policy framework for enhanced monitoring of accounts 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) As and when list of individuals and entities, approved by Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs), are received from Government of India, Reserve Bank circulates these to all banks and financial institutions. Banks/Financial Institutions should ensure to update the consolidated list of individuals and entities as circulated by Reserve Bank. Further, the updated list of such individuals/entities can be accessed in the United Nations website at <http://www.un.org/sc/committees/1267/consolist.shtml>. Banks are advised that before opening any new account it should be ensured that the name/s of the proposed customer does not appear in the list. Further, banks should scan all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the list. Full details of accounts bearing resemblance with any of the individuals/entities in the list should immediately be intimated to RBI and FIU-IND.

2.12 Correspondent Banking

a) Correspondent banking is the provision of banking services by one bank (the “correspondent bank”) to another bank (the “respondent bank”). These services may include cash/funds management, international wire transfers, drawing arrangements for demand drafts and mail transfers, payable-through-accounts, cheques clearing etc. Banks should gather sufficient information to understand fully the nature of the business of the correspondent/respondent bank. Information on the other bank’s 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 correspondent's/respondent’s country may be of special relevance. Similarly, banks should try to ascertain from publicly available information whether the other bank has been subject to any money laundering or terrorist financing investigation or regulatory action. While it is desirable that such relationships should be established only with the approval of the Board, in case the Boards of some banks wish to delegate the power to an administrative authority, they may delegate the power to a committee headed by the Chairman/CEO of the bank while laying down clear parameters for approving such relationships. Proposals approved by the Committee should invariably be put up to the Board at its next meeting for post facto approval. The responsibilities of each bank with whom correspondent banking relationship is established should be clearly documented. In the case of payable-through-accounts, the correspondent bank should be satisfied that the respondent bank has verified the identity of the customers having direct access to the accounts and is undertaking

ongoing 'due diligence' on them. The correspondent bank should also ensure that the respondent bank is able to provide the relevant customer identification data immediately on request.

b) Correspondent relationship with a “Shell Bank”

Banks should refuse to enter into a correspondent relationship with a “shell bank” (i.e. a bank which is incorporated in a country where it has no physical presence and is unaffiliated to any regulated financial group). Shell banks are not permitted to operate in India. Banks should also guard against establishing relationships with respondent foreign financial institutions that permit their accounts to be used by shell banks. Banks should be extremely cautious while continuing relationships with respondent banks located in countries with poor KYC standards and countries identified as 'non-cooperative' in the fight against money laundering and terrorist financing. Banks should ensure that their respondent banks have anti money laundering policies and procedures in place and apply enhanced 'due diligence' procedures for transactions carried out through the correspondent accounts.

2.13 Wire Transfers

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 a rapid and secure method for transferring value from one location to another.

- i)** The salient features of a wire transfer transaction are as under :
- a) Wire transfer is a transaction carried out on behalf of an originator person (both natural and legal) through a bank by electronic means with a view to making an amount of money available to a beneficiary person at a bank. The originator and the beneficiary may be the same person.
 - b) Cross-border transfer means any wire transfer where the originator and the beneficiary bank or financial institution are located in different countries. It may include any chain of wire transfers that has at least one cross-border element.
 - c) Domestic wire transfer means any wire transfer where the originator and receiver are located in the same country. It may also include a chain of wire transfers that takes place entirely within the borders of a single country even though the system used to effect the wire transfer may be located in another country.
 - d) The originator is the account holder, or where there is no account, the person (natural or legal) that places the order with the bank to perform the wire transfer.
- ii)** Wire transfer is an instantaneous and most preferred route for transfer of funds across the globe and hence, there is a need for preventing terrorists and other criminals from having unfettered access to wire transfers for moving their funds and for detecting any misuse when it occurs. This can be achieved if basic information on the originator of wire transfers is immediately available to appropriate law enforcement and/or prosecutorial authorities in order to assist them in detecting, investigating,

prosecuting terrorists or other criminals and tracing their assets. The information can be used by Financial Intelligence Unit - India (FIU-IND) for analysing suspicious or unusual activity and disseminating it as necessary. The originator information can also be put to use by the beneficiary bank to facilitate identification and reporting of suspicious transactions to FIU-IND. Owing to the potential terrorist financing threat posed by small wire transfers, the objective is to be in a position to trace all wire transfers with minimum threshold limits. Accordingly, banks must ensure that all wire transfers are accompanied by the following information :

(A) Cross-border wire transfers

- a) All cross-border wire transfers must be accompanied by accurate and meaningful originator information.
- b) 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.
- c) 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 (b) above.

(B) Domestic wire transfers

- a)** Information accompanying all domestic wire transfers of Rs. 50000/- (Rupees Fifty Thousand) and above must include complete originator information i.e. name, address and account number etc., unless full originator information can be made available to the beneficiary bank by other means.
- b)** If a bank has reason to believe that a customer is intentionally structuring wire transfers to below Rs. 50000/- (Rupees Fifty Thousand) to several beneficiaries in order to avoid reporting or monitoring, the bank must insist on complete customer identification before effecting the transfer. In case of non-cooperation from the customer, efforts should be made to establish his identity and Suspicious Transaction Report (STR) should be made to FIU-IND.
- c)** When a credit or debit card is used to effect money transfer, necessary information as (a) above should be included in the message.

(iii) Exemptions

Interbank transfers and settlements where both the originator and beneficiary are banks or financial institutions would be exempted from the above requirements.

(iv) Role of Ordering, Intermediary and Beneficiary banks

(a) Ordering bank

An ordering bank is the one that originates a wire transfer as per the order placed by its customer. The ordering bank must ensure that qualifying wire transfers contain complete originator information. The bank must also verify and preserve the information at least for a period of ten years.

(b) Intermediary bank

For both cross-border and domestic wire transfers, a bank processing an intermediary element of a chain of wire transfers must ensure that all originator information accompanying a wire transfer is retained with the transfer. Where technical limitations prevent full originator information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, a record must be kept at least for ten years (as required under Prevention of Money Laundering Act, 2002) by the receiving intermediary bank of all the information received from the ordering bank.

(c) Beneficiary bank

A beneficiary bank should have effective risk-based procedures in place to identify wire transfers lacking complete originator information. The lack of complete originator information may be considered as a factor in assessing whether a wire transfer or related transactions are suspicious and whether they should be reported to the Financial Intelligence Unit-India. The beneficiary bank should also take up the matter with the ordering bank if a transaction is not accompanied by detailed information of the fund remitter. If

the ordering bank fails to furnish information on the remitter, the beneficiary bank should consider restricting or even terminating its business relationship with the ordering bank.

2.14 Principal Officer

a) Banks should appoint a senior management officer to be designated as Principal Officer. Principal Officer shall 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 institution which are involved in the fight against money laundering and combating financing of terrorism.

b) The Principal Officer will be responsible for timely submission of CTR, STR and reporting of counterfeit notes to FIU-IND.

2.15 Maintenance of records of transactions/Information to be preserved / Maintenance and preservation of records/Cash and Suspicious transactions reporting to Financial Intelligence Unit-India (FIU-IND)

Government of India, Ministry of Finance, Department of Revenue, vide its notification dated July 1, 2005 in the Gazette of India, has notified the Rules under the Prevention of Money Laundering Act (PMLA), 2002. In terms of the said Rules, the provisions of PMLA, 2002 came into effect from July 1, 2005. Section 12 of the PMLA, 2002 casts certain obligations on the banking companies in regard to preservation and reporting of customer account information. Banks are, therefore, advised to go through the provisions of PMLA, 2002 and the Rules notified there under and take all steps considered

necessary to ensure compliance with the requirements of Section 12 of the Act *ibid*.

(i) Maintenance of records of transactions

Banks should introduce a system of maintaining proper record of transactions prescribed under Rule 3, as mentioned below:

- a) all cash transactions of the value of more than Rupees Ten Lakh or its equivalent in foreign currency;
- b) all series of cash transactions integrally connected to each other which have been valued below Rupees Ten Lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the aggregate value of such transactions exceeds Rupees Ten Lakh;
- c) all cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security or a document has taken place facilitating the transaction;
- d) all suspicious transactions whether or not made in cash and by way of as mentioned in the Rules.
- e) **Explanation - Integrally connected cash transactions referred to at (b) above**

The following transactions have taken place in a branch during the month of April , 2008:

Date	Mode	Dr (in Rs.)	Cr (in Rs.)	Balance (in Rs.)
				BF - 8,00,000.00
02/04/2008	Cash	5,00,000.00	3,00,000.00	6,00,000.00
07/04/2008	Cash	40,000.00	2,00,000.00	7,60,000.00
08/04/2008	Cash	4,70,000.00	1,00,000.00	3,90,000.00
Monthly summation		10,10,000.00	6,00,000.00	

f) As per above clarification, the debit transactions in the above example are integrally connected cash transactions because total cash debits during the calendar month exceeds Rs. 10 lakhs. However, the bank should report only the debit transaction taken place on 02/04 & 08/04/2008. The debit transaction dated 07/04/2008 should not be separately reported by the bank, which is less than Rs.50,000/-.

g) All the credit transactions in the above example would not be treated as integrally connected, as the sum total of the credit transactions during the month does not exceed Rs.10 lakh and hence credit transaction dated 02, 07 & 08/04/2008 should not be reported by banks.

(ii) Information to be preserved

Banks are required to maintain the following information in respect of transactions referred to in Rule 3:

- a) the nature of the transactions;
- b) the amount of the transaction and the currency in which it was denominated;
- c) the date on which the transaction was conducted; and
- d) the parties to the transaction.

(iii) Maintenance and Preservation of records

a) Banks are required to maintain the records containing information in respect of transactions referred to in Rule 3 above. Banks should take appropriate steps to 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. Further, banks should maintain for at least ten years from the date of cessation of transaction between the bank and the client, all necessary records of transactions, both domestic or international, which will permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of persons involved in criminal activity.

b) Banks should ensure that records pertaining to the identification of the customer and his address (e.g. copies of documents like passports, identity cards, driving licenses, PAN, card, utility bills etc.) obtained while opening the account and during the course of business relationship, are properly

preserved for at least ten years after the business relationship is ended. The identification records and transaction data should be made available to the competent authorities upon request.

c) In paragraph 2.7 of this Master Circular, banks have been advised to pay special attention to all complex, unusual large transactions and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. It is further clarified that the background including all documents/office records/memorandums pertaining to such transactions and purpose thereof should, as far as possible, be examined and the findings at branch as well as Principal Officer level should be properly recorded. Such records and related documents should be made available to help auditors in their day-to-day work relating to scrutiny of transactions and also to Reserve Bank/other relevant authorities. These records are required to be preserved for ten years as is required under PMLA, 2002.

(iv) Reporting to Financial Intelligence Unit-India

a) In terms of the PMLA rules, banks are required to report information relating to cash and suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND) in respect of transactions referred to in Rule 3 at the following address:

Director, FIU-IND,
Financial Intelligence Unit-India,
6th Floor, Hotel Samrat,
Chanakyapuri,
New Delhi-110021.

Website - <http://fiuindia.gov.in/>

b) Banks should carefully go through all the reporting formats. There are altogether eight reporting formats, as detailed in Annex II, viz. i) Cash Transactions Report (CTR); ii) Summary of CTR iii) Electronic File Structure-CTR; iv) Suspicious Transactions Report (STR); v) Electronic File Structure-STR; vi) Counterfeit Currency Report (CCR); vii) Summary of CCR and viii) Electronic File Structure-CCR. The reporting formats contain detailed guidelines on the compilation and manner/procedure of submission of the reports to FIU-IND. It would be necessary for banks to initiate urgent steps to ensure electronic filing of all types of reports to FIU-IND. The related hardware and technical requirement for preparing reports in an electronic format, the related data files and data structures thereof are furnished in the instructions part of the concerned formats.

c) FIU-IND have placed on their website editable electronic utilities to enable banks to file electronic CTR/STR who are yet to install/adopt suitable technological tools for extracting CTR/STR from their live transaction data base. It is, therefore, advised that in cases of banks, where all the branches are not fully computerized, the Principal Officer of the bank should cull out the transaction details from branches which are not yet computerized and suitably arrange to feed the data into an electronic file with the help of the editable electronic utilities of CTR/STR as have been made available by FIU-IND in their website <http://fiuindia.gov.in>.

d) In terms of instructions contained in paragraph 2.3(b) of this Master Circular, banks are required to prepare a profile for each customer based on risk categorisation. Further, vide paragraph 2.7, the need for periodical review of risk categorisation has been emphasized. It is, therefore, reiterated that banks, as a part of transaction monitoring mechanism, are required to put in place an appropriate software application to throw alerts when the transactions are inconsistent with risk categorization and updated profile of customers. It is needless to add that a robust software throwing alerts is essential for effective identification and reporting of suspicious transactions.

2.16 Cash Transaction Reports (CTR)

a) While detailed instructions for filing all types of reports are given in the instructions part of the related formats, banks should scrupulously adhere to the following:

- i) The Cash Transaction Report (CTR) for each month should be submitted to FIU-IND by 15th of the succeeding month. Cash transaction reporting by branches to their controlling offices should, therefore, invariably be submitted on monthly basis **(not on fortnightly basis)** and banks should ensure to submit CTR for every month to FIU-IND within the prescribed time schedule.
- ii) All cash transactions, where forged or counterfeit Indian currency notes have been used as genuine should be reported by the Principal Officer to FIU-IND immediately in the specified format (Counterfeit Currency Report – CCR). These cash transactions should also include transactions where forgery of valuable security or documents has taken place and may be reported to FIU-IND in plain text form.

- iii) While filing CTR, details of individual transactions below Rupees Fifty Thousand need not be furnished.
- iv) CTR should contain only the transactions carried out by the bank on behalf of their clients/customers excluding transactions between the internal accounts of the bank.
- v) A summary of cash transaction report for the bank as a whole should be compiled by the Principal Officer of the bank in physical form as per the format specified. The summary should be signed by the Principal Officer and submitted.

b) Suspicious Transaction Reports (STR)

- i) While determining suspicious transactions, banks should be guided by definition of suspicious transaction contained in PMLA Rules as amended from time to time.
- 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. It is clarified that banks should report all such attempted transactions in STRs, even if not completed by customers, irrespective of the amount of the transaction.
- iii) Banks should make STRs if they have reasonable ground to believe that the transaction involve proceeds of crime generally irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences in part B of Schedule of PMLA, 2002 .

- iv) The Suspicious Transaction Report (STR) should be furnished within 7 days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature. The Principal Officer should record his reasons for treating any transaction or a series of transactions as suspicious. It should be ensured that there is no undue delay in arriving at such a conclusion once a suspicious transaction report is received from a branch or any other office. Such report should be made available to the competent authorities on request.
- v) In the context of creating KYC/AML awareness among the staff and for generating alerts for suspicious transactions, banks may consider the indicative list of suspicious activities contained in Annex-E of the 'IBA's Guidance Note for Banks, 2005'.
- vi) Banks should not put any restrictions on operations in the accounts where an STR has been made. Moreover, it should be ensured that there is no **tipping off** to the customer at any level.

2.17 Customer Education/Employee's Training/Employee's Hiring

a) Customer Education

Implementation of KYC procedures requires banks to demand certain information from customers which may be of personal nature or which has hitherto never been called for. This can sometimes lead to a lot of questioning by the customer as to the motive and purpose of collecting such information. There is, therefore, a need for banks to prepare specific literature/ pamphlets etc. so as to educate the customer of the objectives of the KYC programme.

The front desk staff needs to be specially trained to handle such situations while dealing with customers.

b) Employees' Training

Banks must have an ongoing employee training programme so that the members of the staff are adequately trained in KYC procedures. Training requirements should have different focuses for frontline staff, compliance staff and staff dealing with new customers. It is crucial that all those concerned fully understand the rationale behind the KYC policies and implement them consistently.

c) Hiring of Employees

It may be appreciated that KYC norms/AML standards/CFT measures have been prescribed to ensure that criminals are not allowed to misuse the banking channels. It would, therefore, be necessary that adequate screening mechanism is put in place by banks as an integral part of their recruitment/hiring process of personnel.

	<p>employees to transact business on its behalf (iv) Copy of PAN allotment letter (v) Copy of the telephone bill</p>
<p>Accounts of partnership firms</p> <ul style="list-style-type: none"> - Legal name - Address - Names of all partners and their addresses - Telephone numbers of the firm and partners 	<p>(i) Registration certificate, if registered (ii) Partnership deed (iii) Power of Attorney granted to a partner or an employee of the firm to transact business on its behalf (iv) Any officially valid document identifying the partners and the persons holding the Power of Attorney and their addresses (v) Telephone bill in the name of firm/partners</p>
<p>Accounts of trusts & foundations</p> <ul style="list-style-type: none"> - Names of trustees, settlers, beneficiaries and signatories - Names and addresses of the founder, the managers/directors and the beneficiaries - Telephone/fax numbers 	<p>(i) Certificate of registration, if registered (ii) Power of Attorney granted to transact business on its behalf (iii) Any officially valid document to identify the trustees, settlors, beneficiaries and those holding Power of Attorney, founders/managers/directors and their addresses (iv) Resolution of the managing body of the foundation/association (v) Telephone bill</p>

Annex – II

(List of various reports and their formats)

1. Cash Transaction Report (CTR)
2. Summary of CTR
3. Electronic File Structure - CTR
4. Suspicious Transaction Report (STR)
5. Electronic File Structure - STR
6. Counterfeit Currency Report (CCR)
7. Summary of CCR
8. Electronic File Structure - CCR

ANNEX - III

(List of Circulars on 'Know your customer' and monitoring of cash transactions)

Sr. No.	Circular No. and date	Subject	Gist of instructions
1	DBOD.BP.BC.92 /C.469-76 dated 12 th August, 1976	Issue of DDs/TTs in excess of Rs.5000/-	Applicants (whether customer or not) for DD/MT/TT/Travellers cheques for amount exceeding Rs.10,000/- should affix Permanent Income Tax Number on the application.
2	DBOD.GC.BC.6 2/c.408(A)/87 dated 11 th November, 1987	Frauds in banks- opening of new accounts.	Payment for imports should be made by debit to the accounts maintained with the same bank or any other bank and under no circumstances cash should be accepted for retirement of import bills. There should be reasonable gap of say, 6 months between the time an introducer opens his account and introduces another prospective account holder to the bank. Introduction of an account should enable proper identification of the person opening an account so that the person can be traced if the account is misused.
3	DBOD.BP.BC.11 4/C.469 (81)-91 dated 19 th April, 1991	Misuse of banking channels for violation of fiscal laws and evasion of taxes – Issue	Banks to issue travellers cheques, demand drafts, mail transfers, telegraphic transfers for Rs. 50,000/- and above by debit to customers accounts or against

Sr. No.	Circular No. and date	Subject	Gist of instructions
		and payment of demand drafts for Rs.50,000 and above.	cheques only and not against cash.
4	DBOD.BC.20/17.04.001/92 dated 25 th August, 1992	Committee to enquire into various aspects relating to frauds and malpractices in banks.	Banks advised to adhere to the prescribed norms and safeguards while opening accounts etc.
5	DBOD.BP.BC.60 /21.01.023/92 dated 21st December,1992	Diversion of working capital funds.	Banks to ensure that withdrawals from cash credit/overdraft accounts are strictly for the purpose for which the credit limits were sanctioned by them. There should be no diversion of working capital finance for acquisition of fixed assets, investments in associate companies/ subsidiaries and acquisition of shares, debentures, units of UTI and other mutual funds and other investments in the capital market.
6	DBOD.FMC.No. 153/27.01.003/93-94 dated 1st September, 1993	Monitoring of flow of funds.	Banks to be vigilant and ensure proper end use of bank funds/monitoring flow of funds. Banks to keep vigil over heavy cash withdrawals by account holders which may be disproportionate to their normal trade/business requirements and

Sr. No.	Circular No. and date	Subject	Gist of instructions
			cases of unusual trends. Doubtful cases to be reported to DBOD, Regional office.
7	DBOD.GC.BC.1 93/17.04.001/93 dated 18 th November, 1993	Frauds in banks – Encashment of Interest/Dividend Warrants, Refund Orders etc.	Banks to be vigilant in opening new accounts without proper introduction, new accounts with fictitious names and addresses. Banks instructed to strictly adhere to the instructions issued on opening and operating of bank accounts.
8	DBOD.GC.BC.2 02/17.04.001/93 dated 6 th December, 1993	The Committee to enquire into various aspects relating to frauds and malpractices in banks.	Customer identification while opening accounts including obtaining of photographs of customers while opening accounts.
9	DBOD.No.GC.B C.46/17.04.001 dated 22 nd April, 1994	The Committee to enquire into various aspects relating to frauds and malpractices in banks.	Clarifications given to banks regarding obtaining photographs of the depositors/account holder authorised to operate new accounts with effect from 1.1.1994. Obtaining of photographs would apply to residents and non-residents and all categories of deposits including fixed/recurring/cumulative deposit accounts and also to those persons authorised to operate the accounts.

Sr. No.	Circular No. and date	Subject	Gist of instructions
10	DBOD.BP.BC.10 6/21.01.001/94 dated 23 rd September, 1994	Fraudulent operations in deposit accounts- opening and collection of cheques/pay orders etc.	Banks to examine every request for opening joint accounts very carefully, look into the purpose, other relevant aspects relating to business, the financial position of the account holders and whether number of account holders are large. 'Generally crossed' cheques and payable to 'order' should be collected only on proper endorsement by the payee. Banks to exercise care in collection of cheques of large amounts and ensure that joint accounts are not used for benami transactions.
11	DBOD.BP.BC.57 /21.01.001/95 dated 4 th May, 1995	Frauds in banks – Monitoring of deposit accounts.	Banks to introduce system of close watch of new deposit accounts and monitoring of cash withdrawals and deposits for Rs.10 lakh and above in deposit, cash credit and overdraft accounts. Banks to keep record of details of these large cash transactions in a separate register.
12	DBOD.BP.BC.10 2/21.01.001/95 dated 20 th September, 1995	Monitoring of Deposit Accounts.	Reporting of all cash deposits and withdrawals of Rs.10 lakhs and above with full details in fortnightly statements by bank branches to their controlling offices. Transactions of suspicious nature to be apprised to Head Office. RBI

Sr. No.	Circular No. and date	Subject	Gist of instructions
			to look into these statements at the time of inspections
13	DBOD.BP.BC.42 /21.01.001/96 dated 6 th April, 1996	Monitoring cash deposits and withdrawals of Rs.10 lakh and above in deposit/other accounts.	Banks asked to submit feedback on implementation of the system of close monitoring of large cash deposits and withdrawals of Rs.10 lakh and above.
14	DBOD.No.BP.B C.12/21.01.023/ 98 dated 11 th February 1998	Furnishing of data-violation of secrecy obligations.	Banks should satisfy themselves that information sought will not violate the laws relating to secrecy in banking transactions except under compulsion of law, duty to the public to disclose, where interest of bank requires disclosure and where disclosure is made with the express or implied consent of the customer.
15	DBS.FGV.BC.56 .23.04.001/98-99 dated 21 st June, 1999	Report of the Study Group on Large Value Bank Frauds.	Banks advised to implement the main recommendations of the Study Group on Large Value Bank Frauds.
16	DBOD.COMP.B C.No.130/07.03. 23/2000-01 dated 14 th June, 2001	Internet Banking in India- Guidelines.	Banking facilities on Internet will be subject to the existing regulatory framework. Banks having physical presence in India only will be allowed to offer banking services over Internet to residents in India and any cross border transactions will be subject

Sr. No.	Circular No. and date	Subject	Gist of instructions
			to existing exchange control regulations. Banks to establish identity and also make enquiries about integrity and reputation of the prospective customer. Internet accounts should be opened only after proper introduction and physical verification of the identity of the customer.
17	DBOD.BP.52/21.01.001/2001-02 dated 5 th December, 2001	Prevention of Terrorism Ordinance,2001-Implementation thereof.	Banks should keep a watchful eye on the transactions of the 23 terrorist organisations listed in the Schedule to the Ordinance. Violations of the extant Acts or normal banking operations must be reported to the appropriate authorities under the Ordinance under advice to RBI. Banks to undertake 'due diligence' in respect of the 'KYC' principle.
18	DBOD.AML.BC.89/14.01.001/2001-02 dated 15 th April, 2002	Freezing of funds pursuant to United Nations Security Council Resolution, 1390.	Accounts of individuals and entities listed should be immediately frozen as informed by the Security Council Sanctions Committee of the UN. If any transaction is detected involving any of these entities, banks to report to RBI promptly for necessary action.

Sr. No.	Circular No. and date	Subject	Gist of instructions
19	DBOD.AML.BC. No.102/14.01.00 1/2001-02 dated 10 th May,2002	Monitoring of accounts - compliance with instructions.	Banks should ensure that no new accounts are opened by banned organisations. Banks to strictly adhere to the extant guidelines regarding opening and monitoring of accounts. Banks to confirm having issued instructions for immediate compliance by the branches and controlling offices.
20	DBOD.AML.BC. 18/14.01.001/20 02-03 dated August 16, 2002	Guidelines on "Know Your Customer" norms and "Cash transactions"	First circular on KYC. The customer identification should entail verification through an introductory reference from an existing account holder/a person known to the bank or on the basis of documents provided by the customer. The Board of Directors of the banks should have in place adequate policies that establish procedures to verify the bonafide identification of individual/ corporates opening an account. Branches of banks are required to report all cash deposits and withdrawals of Rs.10 lakhs and above as well as transactions of suspicious nature with full details in fortnightly statements to their controlling offices.
21	DBOD.NO.AML. BC.58/14.01.001 /2004-05 dated	'Know Your Customer' (KYC) Guidelines –	Our guidelines were revisited to make those compliant with FATF recommendations and Basel

Sr. No.	Circular No. and date	Subject	Gist of instructions
	/2004-05 dated November 29, 2004	Guidelines – Anti Money Laundering Standards	Committee Report on CDD. Four pronged approach was prescribed to banks based on Customer Acceptance Policy, Customer Identification Procedure, Monitoring of Transaction and Risk Management.
22	DBOD.NO.AML.BC.28 /14.01.001/2005-06 dated August 23, 2005	Know Your Customer Guidelines- Anti-Money Laundering Standards	KYC guidelines on document requirement were relaxed for people belonging to financially disadvantaged sections in the society, who could open account with introductory reference.
23	DBOD.NO.AML.BC.63/14.01.001 /2005-06 dated February 15, 2006	Prevention of Money Laundering Act, 2002 – Obligation of banks in terms of Rules notified thereunder	Reporting mechanism and formats were prescribed to banks to report cash and suspicious transactions to Financial Intelligence Unit- India (FIU-IND).
24	DBOD.AML.BC.No.77/ 14.01.001 / 2006-07 April 13, 2007	Wire transfers	Banks were advised to ensure that all wire transfers involving domestic and cross boarder fund transfers are accompanied by full originator information.
25	DBOD.AML.BC.No. 63/ 14.01.001/2007-08 dated February 18, 2008	Know Your Customer (KYC) Norms/Anti Money Laundering (AML)	Revised guidelines on KYC/AML issued on review of risk categorization of customers; periodical updation of customer identification data and screening

Sr. No.	Circular No. and date	Subject	Gist of instructions
		Standards/Combating of Financing of Terrorism (CFT)	mechanism for recruitment /hiring process of personnel.
26	DBOD.AML.BC. No. 85/ 14.01.001/ 2007 -08 dated May 22, 2008	Prevention of Money Laundering Act, 2002 – Obligation of banks in terms of Rules notified thereunder.	Revised guidelines issued on CTR and STR by banks to FIU-IND.

CASH TRANSACTION REPORT (CTR) FOR A BANKING COMPANY

Kindly fill in CAPITAL. Read the instructions before filling the form.

PART 5 LIST OF OTHER RELATED PERSONS (other than account holders)

	Name of Individual/Legal Person/Entity	Customer ID/number (if allotted)	Relation	Annexure
5.1				
5.2				
5.3				
5.4				
5.5				

Mention B for Auth. Signatory, C for Director/Partner/Member etc., D for Introducer. E for Guarantor, Z for others

Mention A for Individuals, B for Legal Person/ Entity

Mention appropriate Annexure number

Tick ✓ to confirm

(Details of all persons should be furnished in prescribed annexure)

Number of additional sheets for PART 5 attached (Leave blank if space provided above is sufficient and no extra sheet is attached)

PART 6 DETAILS OF TRANSACTIONS

	Date of Transaction	Debit /Credit	Amount in Rupees	Remarks
6.1				
6.2				
6.3				
6.4				
6.5				
6.6				
6.7				
6.8				
6.9				
6.10				

DD - MM - YYYY

D for Debit and C for Credit

Number of additional sheets for PART 6 attached (Leave blank if space provided above is sufficient and no extra sheet is attached)

PART 7 CUMULATIVE TOTALS

7.1 Total debits in the bank account in the financial year

7.2 Total credits in the bank account in the financial year

DO NOT FILL. FOR FIU-IND USE ONLY

ACK. NO. | | | | | | | | | |

DATE | | | | 2 | 0 | 0 | | | |
D D M M Y Y Y Y

Signature

Name

Designation

DO NOT FILL. FOR FIU-IND USE ONLY.

CBA02

CASH TRANSACTION REPORT (CTR) FOR A BANKING COMPANY INSTRUCTIONS

GENERAL INSTRUCTIONS

The Prevention of Money Laundering Act 2002

Under the Prevention of Money Laundering Act 2002, every banking company shall furnish details of :

(A) All cash transactions of the value of more than rupees ten lakhs or its equivalent in foreign currency;

(B) All series of cash transactions integrally connected to each other which have been valued below rupees ten lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month;

Provided that where the principal officer of a banking company has reason to believe that a single transaction or series of transactions integrally connected to each other have been valued below the prescribed limit so as to defeat the provisions of this section, such officer shall furnish information in respect of such transactions to the Director within the prescribed time.

How to submit

Every bank branch must submit this form to the Director, FIU-IND only through the principal officer of the banking company designated under PMLA, 2002

EXPLANATION OF SPECIFIC TERMS

PART 1: DETAILS OF REPORT

Replacement report is a report submitted in replacement of an earlier CTR. When a replacement report is submitted, date of submitting original CTR may be mentioned and the complete CTR has to be submitted again.

PART 2: DETAILS OF REPORTING BRANCH / LOCATION

Particulars of the branch/location in which the reported account is maintained should be submitted in this part.

2.3. ID allotted by FIU-IND may be left blank till the same is communicated by FIU-IND.

PART 3: DETAILS OF BANK ACCOUNT

A separate CTR is required to be filed for each reported bank account.

PART 4: LIST OF ACCOUNT HOLDERS

Customer ID/number is the number allotted by bank to identify the customer. Enclose a separate annexure for each account holder.

PART 5: LIST OF OTHER RELATED PERSONS

The customer ID/number may be mentioned if the related person is also a customer of the bank. The related person can be of following types:

“B”- Authorised signatory

“C”- Director/Partner/Member etc. of a Legal Person/Entity

“D”- Introducer

“E”- Guarantor

“Z” - Other

Enclose a separate annexure for each related person.

PART 6: DETAILS OF TRANSACTIONS

Debit- Cash withdrawn from the bank account.

Credit- Cash deposited in the bank account.

The amount should be rounded off to nearest rupee without decimal. If this amount was not in Indian Rupees, it should be converted into rupees. Mention any other information related to the transaction (such as amount and type of foreign currency) in the Remarks column.

PART 7: CUMULATIVE TOTALS

7.1. Total of all debit entries in the bank account from 1st April of the financial year till the last day of the month of reporting.

7.2. Total of all credit entries in the bank account from 1st April of the financial year till the last day of the month of reporting.

ALL ANNEXURES MUST BE ENCLOSED.

ANNEXURE A - INDIVIDUAL DETAIL SHEET FOR A BANKING COMPANY

INDIVIDUAL **A**

Use separate annexure for each individual.

Kindly fill in CAPITAL.

1. Name of bank (with branch)	<input type="text"/>		
2. BSR code	<input type="text"/>		
3. Annexure enclosed with	<input type="checkbox"/> A	Cash Transaction Report	<input type="checkbox"/> B Counterfeit Currency Report
	<input type="checkbox"/> C	Suspicious Transaction Report	(Tick ✓ as applicable)
4. Full name of individual	<input type="text"/>		
5. Customer ID/number	<input type="text"/> (If allotted)		
6. Name of father/spouse	<input type="text"/>		
7. Occupation	<input type="text"/>		
8. Date of birth	<input type="text"/>	9. Sex (M/F) <input type="checkbox"/>	10. Nationality <input type="text"/>
11. Identification document	DD - MM - YYYY		
	<input type="checkbox"/> A	Passport	<input type="checkbox"/> B Election ID card <input type="checkbox"/> C PAN card
	<input type="checkbox"/> D	ID card	<input type="checkbox"/> E Driving license <input type="checkbox"/> F Account introducer
	<input type="checkbox"/> Z	Other (Specify)	<input type="text"/>
12. Identification number	<input type="text"/>	(Number mentioned in the identification document)	
13. Issuing authority	<input type="text"/>	(Authority which had issued the document)	
14. Place of Issue	<input type="text"/>	(Place where the document was issued)	
15. PAN	<input type="text"/>		
Communication address			
16. No., Building	<input type="text"/>		
17. Street/Road	<input type="text"/>		
18. Locality	<input type="text"/>		
19. City/Town, District	<input type="text"/>		
20. State, Country	<input type="text"/>		
21. Pin code	<input type="text"/>	22. Tel (with STD code)	<input type="text"/>
23. Mobile number	<input type="text"/>	24. E-mail	<input type="text"/>
25. Name of Organisation/Employer	<input type="text"/>		
Second Address (Permanent address/Place of work)			
26. No., Building	<input type="text"/>		
27. Street/Road	<input type="text"/>		
28. Locality	<input type="text"/>		
29. City/Town, District	<input type="text"/>		
30. State, Country	<input type="text"/>		
31. Pin code	<input type="text"/>	32. Tel (with STD code)	<input type="text"/>
DO NOT FILL. FOR FIU-IND USE ONLY.			BAA

ANNEXURE B - LEGAL PERSON/ENTITY DETAIL SHEET FOR A BANKING COMPANY

LEGAL PERSON/ENTITY **B**

Use separate annexure for each legal person/entity. Kindly fill in CAPITAL.

1. Name of bank (with branch)	<input style="width:100%;" type="text"/>		
2. BSR code	<input style="width:100%;" type="text"/>		
3. Annexure enclosed with	<input type="checkbox"/> A	Cash Transaction Report	<input type="checkbox"/> B
	<input type="checkbox"/> C	Suspicious Transaction Report	(Tick ✓ as applicable)
4. Name of legal person/entity	<input style="width:100%;" type="text"/>		
5. Customer ID/number	<input style="width:100%;" type="text"/> (If allotted)		
6. Nature of business	<input style="width:100%;" type="text"/>		
7. Date of incorporation	<input style="width:100%;" type="text"/>		
8. Type of Constitution	DD - MM - YYYY		
	<input type="checkbox"/> A	Sole proprietorship	<input type="checkbox"/> B
	<input type="checkbox"/> D	Pvt. ltd. company	<input type="checkbox"/> E
	<input type="checkbox"/> G	Association	<input type="checkbox"/> H
	<input type="checkbox"/> Z	Other (Specify)	<input type="checkbox"/> I
		Firm	<input type="checkbox"/> C
		Public ltd. company	<input type="checkbox"/> F
		Trust	<input type="checkbox"/> I
		HUF	<input type="checkbox"/> C
		Society	<input type="checkbox"/> F
		Liquidator	<input type="checkbox"/> I
9. Registration number	<input style="width:100%;" type="text"/> (Number mentioned in the deed/document)		
10. Registering Authority	<input style="width:100%;" type="text"/> (Authority registering the deed/document)		
11. Place of Registration	<input style="width:100%;" type="text"/> (Place where the document was registered)		
12. PAN	<input style="width:100%;" type="text"/>		
Communication address:			
13. No., Building	<input style="width:100%;" type="text"/>		
14. Street/Road	<input style="width:100%;" type="text"/>		
15. Locality	<input style="width:100%;" type="text"/>		
16. City/Town, District	<input style="width:100%;" type="text"/>		
17. State, Country	<input style="width:100%;" type="text"/>		
18. Pin code	<input style="width:100%;" type="text"/>	19. Tel (with STD code)	<input style="width:100%;" type="text"/>
20. Fax (with STD code)	<input style="width:100%;" type="text"/>	21. E-mail	<input style="width:100%;" type="text"/>
22. List of directors /partners / members and other related persons			
	Name of Individual/Legal Person/Entity	Customer ID/number	Relation Annexure
22.1	<input style="width:100%;" type="text"/>	<input style="width:100%;" type="text"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
22.2	<input style="width:100%;" type="text"/>	<input style="width:100%;" type="text"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
22.3	<input style="width:100%;" type="text"/>	<input style="width:100%;" type="text"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
22.4	<input style="width:100%;" type="text"/>	<input style="width:100%;" type="text"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
22.5	<input style="width:100%;" type="text"/>	<input style="width:100%;" type="text"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Mention B for Authorised Signatory, C for Director/member etc. , D for Introducer. E for Guarantor, Z for others			
Mention A for Individuals, B for Legal Person/ Entity			
Mention appropriate Annexure number			
Tick ✓ to confirm			
DO NOT FILL. FOR FIU-IND USE ONLY.			BAB

SUMMARY OF CASH TRANSACTION REPORTS (CTRs) FOR A BANKING COMPANY

Kindly fill in CAPITAL. Read the instructions before filling the form.

PART 1 DETAILS OF THE SUMMARY

- 1.1 Month and year of summary 2 | 0 | 0
M M Y Y Y Y
- 1.2 Is this a supplementary to an earlier summary ? NO YES *(Tick ✓ as applicable)*
- 1.3 Date of sending original summary if this is a supplementary 2 | 0 | 0
D D M M Y Y Y Y

PART 2 DETAILS OF THE PRINCIPAL OFFICER

- 2.1 Name of Bank
- 2.2 BSR code 2.3 ID allotted by FIU-IND
- 2.4 Category of bank *(Refer to Instructions)*
- 2.5 Name of principal officer
- 2.6 Designation
- 2.7 Address (No., Building)
- 2.8 Street/Road
- 2.9 Locality
- 2.10 City/Town, District
- 2.11 State, Country
- 2.12 Pin code 2.13 Tel (with STD code)
- 2.14 Fax 2.15 E-mail

PART 3 STATISTICS FOR THE MONTH

- 3.1 Number of total branches
- 3.2 Number of branches which have sent reports (including NIL report)
- 3.3 Number of branches which have submitted CTRs (excluding NIL report)
- 3.4 Number of original CTRs (bank accounts) enclosed with this summary
- 3.5 Number of replacement CTRs (bank accounts) enclosed with this summary
- 3.6 Total original CTRs (bank accounts) reported for the month (cumulative)

DO NOT FILL. FOR FIU-IND USE ONLY

ACK. NO.

DATE 2 | 0 | 0
D D M M Y Y Y Y

Signature

Name

(Should be same as the person mentioned in PART 2)

DO NOT FILL. FOR FIU-IND USE ONLY.

CBAS

SUMMARY OF CASH TRANSACTION REPORTS (CTRs) FOR A BANKING COMPANY INSTRUCTIONS

GENERAL INSTRUCTIONS

The Prevention of Money Laundering Act 2002

Under the Prevention of Money Laundering Act 2002, every banking company shall furnish details of:

(A) All cash transactions of the value of more than rupees ten lakhs or its equivalent in foreign currency;

(B) All series of cash transactions integrally connected to each other which have been valued below rupees ten lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month;

Provided that where the principal officer of a banking company has reason to believe that a single transaction or series of transactions integrally connected to each other have been valued below the prescribed limit so as to defeat the provisions of this section, such officer shall furnish information in respect of such transactions to the Director within the prescribed time.

How to submit

The principal officer should submit this summary alongwith CTRs received from branches /locations to the Director, FIU-IND.

Address	Director, FIU-IND Financial Intelligence Unit-India 6th Floor, Hotel Samrat Chanakyapuri, New Delhi -110021 India
---------	---

EXPLANATION OF SPECIFIC TERMS

PART 1: DETAILS OF THE SUMMARY

Separate summary should be furnished for each month.

Supplementary summary is required to be submitted where a summary for the month has already been submitted. In case of supplementary summary, only additional CTRs need to be enclosed.

PART 2: DETAILS OF THE PRINCIPAL OFFICER

2.3. ID allotted by FIU-IND may be left blank till the same is communicated by FIU-IND.

2.4. Category of the bank

- “A”-Public Sector Bank
- “B”-Private Sector Bank
- “C”-Foreign Bank
- “D”-Co-operative Bank
- “E”-Regional Rural Bank
- “F”-Local Area Bank
- “Z”-Other

2.5. Principal officer is the officer designated by the banking company under PMLA, 2002

PART 3: STATISTICS FOR THE MONTH

3.1. Number of branches of the bank.

3.2. Number of branches which have sent CTRs or submitted NIL report for the month.

3.3. Number of branches which have submitted CTRs for the month.

3.4. Number of original CTRs (bank accounts) should match with the original CTRs enclosed with this summary.

3.5. Number of replacement CTRs (bank accounts) should match with the replacement CTRs enclosed with this summary. All replacement CTRs received from branches should be enclosed at the end of the reports for the month.

3.6. This figure should be the cumulative total of 3.4. above for the all the summaries of the month

ALL CTRs MUST BE ENCLOSED.

ELECTRONIC FILE STRUCTURE

<i>Report</i>	CASH TRANSACTION REPORT
<i>Reporting Agency</i>	BANKING COMPANY
<i>Version</i>	1.0

Contents

1.	Introduction.....	1
2.	Financial Intelligence Unit – India	1
3.	Prevention of Money Laundering Act, 2002	1
4.	Cash Transaction Report.....	2
5.	Due Date	2
6.	Banking Company	2
7.	Methods of filing	2
8.	Manual format	3
9.	Electronic Format	3
10.	Description of Data Files	3
11.	Preparation of Data files	4
12.	Validation of Data files.....	4
13.	General Notes for all Data Files	5
14.	Data Structure of Control File (CBACTL.txt).....	6
15.	Data Structure of Branch Data File (CBABRC.txt)	8
16.	Data Structure of Account Data File (CBAACC.txt)	8
17.	Data Structure of Transaction Data File (CBATRN.txt)	10
18.	Data Structure of Individual Data File (CBAINP.txt)	11
19.	Data Structure of Legal Person/Entity Data File (CBALPE.txt).....	12

Appendix

[Summary of Cash Transaction Reports for a Banking Company](#)

[Cash Transaction Report for a Banking Company](#)

[Annexure A- Individual Detail Sheet for a Banking Company](#)

[Annexure B- Legal Person/ Entity Detail Sheet for a Banking Company](#)

Report CASH TRANSACTION REPORT	Reporting Agency BANKING COMPANY	Version 1.0
-----------------------------------	-------------------------------------	----------------

1. Introduction

The Prevention of Money Laundering Act, 2002 (PMLA 2002) forms the core of the legal framework put in place by India to combat money laundering. PMLA 2002 and the Rules notified thereunder came into force with effect from July 1, 2005. Director, FIU-IND and Director (Enforcement) have been conferred with exclusive and concurrent powers under relevant Sections of the Act to implement the provisions of the Act.

The PMLA 2002 and Rules notified thereunder impose an obligation on banking companies, financial institutions and intermediaries of the securities market to verify identity of clients, maintain records and furnish information to FIU-IND.

2. Financial Intelligence Unit – India

The Government of India set up Financial Intelligence Unit – India (FIU-IND) on 18th November 2004 as an independent body to report directly to the Economic Intelligence Council (EIC) headed by the Finance Minister.

FIU-IND has been established as the central national agency responsible for receiving, processing, analyzing and disseminating information relating to suspect financial transactions. FIU-IND is also responsible for coordinating and strengthening efforts of national and international intelligence and enforcement agencies in pursuing the global efforts against money laundering and related crimes. The address of Financial Intelligence Unit – India (FIU-IND) is:

Director, FIU-IND
Financial Intelligence Unit-India
6th Floor, Hotel Samrat
Chanakyapuri, New Delhi -110021
India

Website address: www.fiuindia.gov.in

3. Prevention of Money Laundering Act, 2002

Section 12 of the Prevention of Money Laundering Act, 2002 lays down following obligations on banking companies.

- “12. (1) Every banking company, financial institution and intermediary shall-*
- (a) maintain a record of all transactions, the nature and value of which may be prescribed, whether such transactions comprise of a single transaction or a series of transactions integrally connected to each other, and where such series of transactions take place within a month;*
 - (b) furnish information of transactions referred to in clause (a) to the Director within such time as may be prescribed;*
 - (c) verify and maintain the records of the identity of all its clients, in such a manner as may be prescribed.*

Provided that where the principal officer of a banking company or financial institution or intermediary, as the case may be has reason to believe that a single transaction or series of transactions integrally connected to each other have been valued below the prescribed limit so as to defeat the provisions of this section, such officer shall furnish information in respect of such transactions to the Director within the prescribed time.

Report CASH TRANSACTION REPORT	Reporting Agency BANKING COMPANY	Version 1.0
--	--	-----------------------

(2) The records referred to in sub-section (1) shall be maintained for a period of ten years from the date of cessation of the transactions between the clients and the banking company or financial institution or intermediary, as the case may be.”

4. Cash Transaction Report

The Prevention of Money laundering Act, 2002 and the Rules thereunder require every banking company to furnish details of the following cash transactions:

(A) All cash transactions of the value of more than rupees ten lakhs or its equivalent in foreign currency.

(B) All series of cash transactions integrally connected to each other which have been valued below rupees ten lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month.

5. Due Date

Rule 8 of Notification No. 9/2005 dated 1-7-2005 require the Principal Officer of a banking company to furnish the information of the cash transactions of a month to Director, FIU-IND by the 15th day (Substituted for the 7th day by Notification No. 15/2005 dated 13-12-2005) of the succeeding month.

6. Banking Company

Banking company means a banking company or a co-operative bank to which the Banking Regulation Act, 1949 applies and includes any bank or banking institution referred to in section 51 of that Act (Defined in 2(1)(e) of PMLA 2002). Banking Company includes:

- i) All nationalized banks, private Indian banks and private foreign banks,
- ii) All co-operative banks viz. primary co-operative banks, state co-operative banks and central co-operative banks,
- iii) State Bank of India and its associates and subsidiaries,
- iv) Regional Rural Banks

7. Methods of filing

Cash Transaction Reports can be filed either in manual or electronic format. However, a reporting agency must submit all reports to FIU-IND in electronic format if it has the technical capability to do so. The required technical capability is defined as follows:

- i) A personal computer with 32 MB memory RAM, 800 x 600 VGA video display, Windows® 98/Me/NT/2000/XP; and
- ii) An Internet connection.

It must be noted that every banking company has to ensure reporting by all its branches either in manual or electronic format. Thus, a banking company has to adopt only one format for all its branches.

Report CASH TRANSACTION REPORT	Reporting Agency BANKING COMPANY	Version 1.0
--	--	-----------------------

8. Manual format

Cash Transaction Reports in manual format consists of following forms:

Form	Information	Completed by
Summary of Cash Transaction Reports for a Banking Company	Contains summary of enclosed CTRs	Principal officer of the banking company
Cash Transaction Report for a Banking Company	Details of bank account and cash transactions	Reporting bank branch
Annexure A- Individual Detail Sheet for a Banking Company	Identification details of individual	Reporting bank branch
Annexure B- Legal Person/ Entity Detail Sheet for a Banking Company	Identification details of legal person /entity	Reporting bank branch

The above forms are given in the Appendix.

9. Electronic Format

FIU-IND is in the process of developing technological infrastructure to enable submission of electronic return over a secure gateway. In the interim the banks exercising the electronic option should submit the following to Director, FIU-IND:

- i) One CD containing six data files in prescribed data structure. A label mentioning name of the bank, BSR code, type of report (CTR), month and year of report should be affixed on each CD for the purpose of identification.
- ii) Each CD should be accompanied by Summary of Cash Transaction Reports for Banking Company (same form should be used for both manual as well as electronic format) in physical form duly signed by the principal officer. This summary should match with the data in Control File (CBACTL.txt).

Important:

- i) In case the size of data files exceeds the capacity of one CD, the data files should be compressed by using Winzip 8.1 or ZipItFast 3.0 (or higher version) compression utility only to ensure quick and smooth acceptance of the file.
- ii) The CD should be virus free.

10. Description of Data Files

In case of electronic filing, the consolidated CTR data for the banking company should have following six data files:

S No.	Filename	Description
1	CBACTL.txt	Control File
2	CBABRC.txt	Branch Data File
3	CBAACC.txt	Account Data File
4	CBATRN.txt	Transaction Data File
5	CBAINP.txt	Individual Data File
6	CBALPE.txt	Legal Person/Entity Data File

Report CASH TRANSACTION REPORT	Reporting Agency BANKING COMPANY	Version 1.0
--	--	-----------------------

11. Steps in preparation of data files

- i) The records containing details of cash transactions to be reported are extracted in Transaction Data File (CBATRN.txt).
- ii) The records containing details of bank accounts containing the cash transactions are extracted in Accounts Data File (CBAACC.txt).
- iii) If the account is for Individuals, the records containing details of Individuals who are account holders are extracted in Individual Data File (CBAINP.txt). The Relation Flag should be set to “A”.
- iv) If the account is for a Legal Person /Entity, the records containing details of Legal Persons /Entities who are account holders are extracted in Legal Persons /Entities Data File (CBALPE.txt). The Relation Flag should be set to “A”.
- iii) If the account is for a Legal Person /Entity, the records containing details of Directors/ Partner/ Members etc. of Legal Persons /Entities are appended to Individual Data File (CBAINP.txt). The Relation Flag should be set to “C”.
- v) The records containing details of authorised signatories if not an account holder are appended to Individual Data File (CBAINP.txt) or Legal Persons /Entities Data File (CBALPE.txt) as the case may be. The Relation Flag should be set to “B”.
- vi) The records containing details of account introducers are appended to Individual Data File (CBAINP.txt) or Legal Persons /Entities Data File (CBALPE.txt) as the case may be. The Relation Flag should be set to “D”.
- vii) The records containing details of account guarantors are appended to Individual Data File (CBAINP.txt) or Legal Persons /Entities Data File (CBALPE.txt) as the case may be. The Relation Flag should be set to “E”.
- viii) The records containing details of bank branches which have reported cash transactions are extracted in Branch Data File (CBABRC.txt).
- ix) The report level details and summary of other five tables is entered in Control file. (CBACTL.txt)

12. Steps in validation of data files

- i) There should be six data files with appropriate naming convention.
- ii) The data files should be as per specified data structure and business rules.
- iii) None of the mandatory fields should be left blank.
- iv) Month and Year of report should be same in all data files.
- v) The summary figures in control file should match with the totals in other data files.
- vi) The primary key integrity should be validated as under:
 - a. [Branch Reference Number] should be unique in Branch Data File (CBABRC.txt)
 - b. [Branch Reference Number + Account Number] should be unique in Account Data File (CBAACC.txt)

Report CASH TRANSACTION REPORT	Reporting Agency BANKING COMPANY	Version 1.0
--	--	-----------------------

- vii) The foreign key integrity should be validated as under:
 - a. All values of [Branch Reference Number] in Account Data File (CBAACC.txt) should have a matching [Branch Reference Number] value in Branch Data File (CBABRC.txt)
 - b. All values of [Branch Reference Number + Account Number] in Transaction Data File (CBATRN.txt) should have matching [Branch Reference Number + Account Number] value in Account Data File (CBAACC.txt)
 - c. All values of [Branch Reference Number + Account Number] in Individual Data File (CBAINP.txt) should have matching [Branch Reference Number + Account Number] value in Account Data File (CBAACC.txt)
 - d. All values of [Branch Reference Number + Account Number] in Legal Person / Entity Data File (CBALPE.txt) should have matching [Branch Reference Number + Account Number] value in Account Data File (CBAACC.txt)
- viii) The data sufficiency should be validated as under:
 - a. All values of [Branch Reference Number + Account Number] in Account Data File (CBAACC.txt) should have at least one matching [Branch Reference Number + Account Number] value in Transaction Data File (CBATRN.txt).
 - b. All values of [Branch Reference Number + Account Number] in Account Data File (CBAACC.txt) should have at least one matching [Branch Reference Number + Account Number] value in Individual Data File (CBAINP.txt). (As account for legal person/entity would have individuals as authorised signatories).
 - c. All values of [Branch Reference Number + Account Number] in Account Data File (CBAACC.txt) with Type of Account Holder = "B" (Legal Person/Entity) should have at least one matching [Branch Reference Number + Account Number] value in Legal Person / Entity Data File (CBALPE.txt).

13. General Notes for all Data Files

- i) All Data Files should be generated in ASCII Format with ".txt" as filename extension.
- ii) Each Record (including last record) must start on new line and must end with a newline character. Hex Values: "0D" & "0A".
- iii) All CHAR fields must be left justified.
- iv) If CHAR field has no data or less data with respect to defined length, then the entire field (in case of no data) or the remaining field (in case of less data) has to be filled with right justified blank characters (Spaces).
- v) All NUM fields must be right justified.
- vi) If NUM field has no data or less data with respect to defined length, then the entire field (in case of no data) or the remaining field (in case of less data) has to be filled with left justified zeroes.
- vii) If DATE field has no data then the entire field has to be filled with blank characters (Spaces).
- viii) Fields with an asterisk (*) have to be compulsorily filled up.

Report CASH TRANSACTION REPORT	Reporting Agency BANKING COMPANY	Version 1.0
-----------------------------------	-------------------------------------	----------------

- ix) For fields that do not have an asterisk (*), reasonable efforts have to be made to get the information. Enter “N/A” to indicate that the field is not applicable. Do not substitute any other abbreviations or special characters (e.g., “x”, “-” or “*”).

14. Data Structure of Control File (CBACTL.txt)

	Field	Type	Size	From	To	Remarks
1	Report Name*	CHAR	3	1	3	Value should be “CBA” signifying CTR for Banks
2	Serial Number of Report*	NUM	8	4	11	Indicates the running sequence number of CTR for the reporting agency starting from 00000001
3	Record Type*	CHAR	3	12	14	Value should be “CTL” signifying Control file
4	Month of Report*	NUM	2	15	16	01 for Jan, 02 for Feb and so on
5	Year of Report*	NUM	4	17	20	2005, 2006
6	Complete name of Bank*	CHAR	80	21	100	Field + filler spaces = 80
7	Category of Bank*	CHAR	1	101	101	“A”-Public Sector Bank “B”-Private Sector Bank “C”-Foreign Bank “D”-Co-operative Bank “E”-Regional Rural Bank “F”-Local Area Bank “Z”-Other
8	BSR code *	CHAR	7	102	108	BSR code issued by RBI
9	Unique ID issued by FIU*	CHAR	10	109	118	Use XXXXXXXXXXXX till the ID is communicated
10	Principal Officer’s Name*	CHAR	80	119	198	Field + filler spaces = 80
11	Principal Officer’s Designation*	CHAR	80	199	278	Field + filler spaces = 80
12	Principal Officer’s Address1*	CHAR	45	279	323	No., Building Field + filler spaces = 45
13	Principal Officer’s Address2	CHAR	45	324	368	Street/Road Field + filler spaces = 45
14	Principal Officer’s Address3	CHAR	45	369	413	Locality Field + filler spaces = 45
15	Principal Officer’s Address4	CHAR	45	414	458	City/Town, District Field + filler spaces = 45
16	Principal Officer’s Address5	CHAR	45	459	503	State, Country Field + filler spaces = 45
17	Principal Officer’s Pin code*	NUM	6	504	509	Pin code without “-” or space
18	Principal Officer’s Telephone	CHAR	30	510	539	Telephone in format STD Code-Telephone number
19	Principal Officer’s FAX	CHAR	30	540	569	Fax number in format STD Code-Telephone number
20	Principal Officer’s E-mail	CHAR	50	570	619	E-mail address

Report CASH TRANSACTION REPORT	Reporting Agency BANKING COMPANY	Version 1.0
--	--	-----------------------

21	Report Type*	CHAR	1	620	620	“N”- New Report “R”- Replacement to earlier submitted report
22	Reason for Replacement*	CHAR	1	621	621	“A” – Acknowledgement of Original Report had many warnings or error messages. “B” – Operational error, data omitted in Original Report. “C” – Operational error, wrong data submitted in Original Report. “N”- Not Applicable as this is a new report “Z”- Other Reason
23	Serial Number of Original Report *	NUM	8	622	629	Serial Number of the Original Report which is being replaced. Mention 00000000 if Report Type is “N”
24	Operational Mode*	CHAR	1	630	630	“P”- Actual/ Production mode “T”- Test / Trial mode
25	Data Structure Version*	CHAR	1	631	631	Value should be 1 to indicate Version 1.0
26	Number of Total Branches*	NUM	8	632	639	Total Number of branches of the bank
27	Number of Branches which have sent reports (including NIL report)*	NUM	8	640	647	Include branches which have sent NIL reports
28	Number of Branches which have submitted CTRs (excluding NIL report)*	NUM	8	648	655	Exclude branches which have sent NIL reports. This should match the count of total number of records in CBABRC.txt
29	Number of CTRs (Reported Accounts)*	NUM	8	656	663	Count of total number of records in CBAACC.txt
30	Number of Transactions*	NUM	8	664	671	Count of total number of records in CBATRN.txt
31	Number of Individual Persons*	NUM	8	672	679	Count of total number of records in CBAINP.txt
32	Number of Legal Person/entities*	NUM	8	680	687	Count of total number of records in CBALPE.txt
33	Acknowledgement Number	NUM	10	688	697	For internal use of FIU-IND. Use value 0000000000
34	Date of Acknowledgement	DATE	8	698	705	For internal use of FIU-IND. Use value “XXXXXXXXXX”

Report CASH TRANSACTION REPORT	Reporting Agency BANKING COMPANY	Version 1.0
-----------------------------------	-------------------------------------	----------------

15. Data Structure of Branch Data File (CBABRC.txt)

	Field	Type	Size	From	To	Remarks
1	Record Type*	CHAR	3	1	3	Value should be "BRC" signifying Branch Data file
2	Month of Report*	NUM	2	4	5	01 for Jan, 02 for Feb and so on
3	Year of Report*	NUM	4	6	9	2005, 2006
4	Line Number*	NUM	6	10	15	Running Sequence Number for each line in the file starting from 000001. This Number will be used during validation checks.
5	Name of Branch*	CHAR	80	16	95	Field + filler spaces = 80
6	Branch Reference Number*	CHAR	7	96	102	BSR code issued by RBI
7	Unique ID issued by FIU*	CHAR	10	103	112	Use XXXXXXXXXXXX till the ID is communicated
8	Branch Address1*	CHAR	45	113	157	No., Building Field + filler spaces = 45
9	Branch Address2*	CHAR	45	158	202	Street/Road Field + filler spaces = 45
10	Branch Address3	CHAR	45	203	247	Locality Field + filler spaces = 45
11	Branch Address4	CHAR	45	248	292	City/Town, District Field + filler spaces = 45
12	Branch Address5	CHAR	45	293	337	State, Country Field + filler spaces = 45
13	Branch Pin code*	NUM	6	338	343	Pin code without "-" or space
14	Branch Telephone	CHAR	30	344	373	Telephone number in format STD Code-Telephone number
15	Branch Fax	CHAR	30	374	403	Fax number in format STD Code-Telephone number
16	Branch E-mail	CHAR	50	404	453	E-mail address

16. Data Structure of Account Data File (CBAACC.txt)

	Field	Type	Size	From	To	Remarks
1	Record Type*	CHAR	3	1	3	Value should be "RAC" signifying Reported Account file
2	Month of Report*	NUM	2	4	5	01 for Jan, 02 for Feb and so on
3	Year of Report*	NUM	4	6	9	2005, 2006
4	Line Number*	NUM	6	10	15	Running Sequence Number for each line in the file starting from 000001. This Number

Report CASH TRANSACTION REPORT	Reporting Agency BANKING COMPANY	Version 1.0
-----------------------------------	-------------------------------------	----------------

						will be used during validation checks.
5	Branch Reference Number*	CHAR	7	16	22	BSR code of the Bank Branch
6	Account Number*	CHAR	20	23	42	Bank account number
7	Name of first/sole account holder	CHAR	80	43	122	Field + filler spaces = 80
8	Type of Account*	CHAR	1	123	123	“A”- Savings Account “B”- Current Account “C”- Cash Credit Account “Z”- Other
9	Type of Account Holder*	CHAR	1	124	124	“A”- Individual “B”-Legal Person /Entity excluding “C” and “D” “C”- Central/ State Government “D”- Central/ State Government owned undertaking “Z”- Other
10	Date of Account opening*	DATE	8	125	132	Date in DDMMYYYY Format
11	Risk Category	CHAR	1	133	133	Risk Category as per the Internal Risk Assessment System of the Bank “A”- Low Risk “B”- Medium Risk “C”- High Risk
12	Cumulative Credit Turnover*	NUM	20	134	153	Sum of all credits in the Bank account from 1 st April of the financial year till the last day of the month of reporting. If report is being furnished for Jan 2006 then transactions from 1 st April 2005 to 31 st Jan 2006 have to be aggregated. The amount should be rounded off to nearest rupee without decimal.
13	Cumulative Debit Turnover*	NUM	20	154	173	Sum of all debits in the Bank account from 1 st April of the financial year till the last day of the month of reporting. The amount should be rounded off to nearest rupee without decimal.
14	Cumulative Cash Deposit Turnover*	NUM	20	174	193	Sum of cash deposits in the Bank account from 1 st April of the financial year till the last day of the month of reporting. The amount should be rounded off to nearest rupee without

Report CASH TRANSACTION REPORT	Reporting Agency BANKING COMPANY	Version 1.0
--	--	-----------------------

						decimal.
15	Cumulative Cash Withdrawal Turnover*	NUM	20	194	213	Sum of cash withdrawals in the Bank account from 1 st April of the financial year till the last day of the month of reporting. The amount should be rounded off to nearest rupee without decimal.

17. Data Structure of Transaction Data File (CBATR.N.txt)

	Field	Type	Size	From	To	Remarks
1	Record Type*	CHAR	3	1	3	Value should be "TRN" signifying Transaction data file
2	Line Number*	NUM	6	4	9	Running Sequence Number for each line in the file starting from 000001. This Number will be used during validation checks.
3	Branch Reference Number*	CHAR	7	10	16	BSR code of the Bank Branch
4	Account Number*	CHAR	20	17	36	Bank account number
5	Transaction ID	CHAR	20	37	56	Unique ID to identify transaction (if available)
6	Date of Transaction*	DATE	8	57	64	Date in DDMMYYYY Format
7	Mode of Transaction*	CHAR	1	65	65	Mention "C"- Cash
8	Debit/Credit*	CHAR	1	66	66	"D" – Debit (Cash Withdrawal in the account) "C" – Credit (Cash Deposit in the account)
9	Amount*	NUM	20	67	86	The amount should be rounded off to nearest rupee without decimal. If this amount was not in Indian Rupees, it should be converted into Indian rupees.
10	Currency of Transaction*	CHAR	3	87	89	"INR" for Indian Rupees, Mention Currency code as per SWIFT Code
11	Disposition of Funds	CHAR	1	90	90	Reserved for later use. Use Value "X"
12	Remarks	CHAR	10	91	100	Mention any other information related to the transaction.

Report CASH TRANSACTION REPORT	Reporting Agency BANKING COMPANY	Version 1.0
-----------------------------------	-------------------------------------	----------------

18. Data Structure of Individual Data File (CBAINP.txt)

	Field	Type	Size	From	To	Remarks
1	Record Type*	CHAR	3	1	3	Value should be "INP" signifying Individual data file
2	Month of Report*	NUM	2	4	5	01 for Jan, 02 for Feb and so on
3	Year of Report*	NUM	4	6	9	2005, 2006
4	Line Number*	NUM	6	10	15	Running Sequence Number for each line in the file starting from 000001. This Number will be used during validation checks.
5	Branch Reference Number*	CHAR	7	16	22	BSR code of the Bank Branch
6	Account Number*	CHAR	20	23	42	Bank account number
7	Relation Flag*	CHAR	1	43	43	"A"- Account Holder "B"- Authorised Signatory "C"- Director/ Partner/Member etc. of a Legal Person /Entity "D"- Introducer "E"- Guarantor "Z" - Other
8	Full name of Individual*	CHAR	80	44	123	Full Name Field + filler spaces = 80
9	Customer ID/Number	CHAR	10	124	133	Customer ID/Number in the bank if it has been allotted
10	Name of Father/Spouse	CHAR	80	134	213	Full Name of Father/Spouse Field + filler spaces = 80
11	Occupation	CHAR	50	214	263	Where Applicable
12	Date of Birth	DATE	8	264	271	In DDMMYYYY format
13	Sex	CHAR	1	272	272	"M"- Male "F"- Female
14	Nationality	CHAR	2	273	274	Country code as per SWIFT
15	Type of Identification	CHAR	1	275	275	"A" –Passport "B"- Election ID Card "C"- PAN Card "D"- ID Card "E"- Driving License "F"- Account Introducer "Z" - Other
16	Identification Number	CHAR	10	276	285	Number mentioned in the identification document
17	Issuing Authority	CHAR	20	286	305	Authority which had issued the identification document
18	Place of Issue	CHAR	20	306	325	Place where document was issued
19	PAN	CHAR	10	326	335	Ten Digit PAN used by Income Tax Department

Report CASH TRANSACTION REPORT	Reporting Agency BANKING COMPANY	Version 1.0
--	--	-----------------------

20	Communication Address 1*	CHAR	45	336	380	Field + filler spaces = 45
21	Communication Address 2	CHAR	45	381	425	Field + filler spaces = 45
22	Communication Address 3	CHAR	45	426	470	Field + filler spaces = 45
23	Communication Address 4	CHAR	45	471	515	Field + filler spaces = 45
24	Communication Address 5	CHAR	45	516	560	Field + filler spaces = 45
25	Communication Address Pin code*	NUM	6	561	566	Pin code without “-” or space
26	Contact Telephone	CHAR	30	567	596	Telephone number in format STD Code-Telephone number
27	Contact Mobile number	CHAR	30	597	626	Mobile number
28	Contact E-mail	CHAR	50	627	676	E-mail address
29	Place of Work	CHAR	80	677	756	Name of Organisation/ employer
30	Second Address 1	CHAR	45	757	801	Permanent address / Place of work (if other than communication address)
31	Second Address 2	CHAR	45	802	846	Field + filler spaces = 45
32	Second Address 3	CHAR	45	847	891	Field + filler spaces = 45
33	Second Address 4	CHAR	45	892	936	Field + filler spaces = 45
34	Second Address 5	CHAR	45	937	981	Field + filler spaces = 45
35	Second Address Pin code	NUM	6	982	987	Pin code without “-” or space
36	Second Telephone	CHAR	30	988	1017	Telephone number in format STD Code-Telephone number

19. Data Structure of Legal Person/Entity Data File (CBALPE.txt)

	Field	Type	Size	From	To	Remarks
1	Record Type*	CHAR	3	1	3	Value should be “LPE” signifying Legal Persons/ Entity data file
2	Month of Report*	NUM	2	4	5	01 for Jan, 02 for Feb and so on
3	Year of Report*	NUM	4	6	9	2005, 2006
4	Line Number*	NUM	6	10	15	Running Sequence Number for each line in the file starting from 000001. This Number will be used during validation checks.
5	Branch Reference Number*	CHAR	7	16	22	BSR code of the Bank Branch
6	Account Number*	CHAR	20	23	42	Bank account number
7	Relation Flag*	CHAR	1	43	43	“A”- Account Holder “D”- Introducer “E”- Guarantor “Z”- Other
8	Name of Legal Person /Entity*	CHAR	80	44	123	Full Name Field + filler spaces = 80
9	Customer ID/Number	CHAR	10	124	133	Customer ID/Number in the bank if allotted
10	Nature of Business	CHAR	50	134	183	Where Applicable
11	Date of Incorporation	DATE	8	184	191	In DDMMYYYY format

Report CASH TRANSACTION REPORT	Reporting Agency BANKING COMPANY	Version 1.0
--	--	-----------------------

12	Type of Constitution*	CHAR	1	192	192	“A”- Sole Proprietorship “B”- Firm “C”- HUF “D”- Private Ltd. Company “E”- Public Ltd. Company “F”- Society “G”- Association “H”- Trust “I”- Liquidator “Z”- Other
13	Registration Number	CHAR	20	193	212	Registration Number of mentioned in deed/document
14	Registering authority	CHAR	20	213	232	Authority Registering deed/document
15	Place of Registration	CHAR	20	233	252	Place where the document was registered
16	PAN	CHAR	10	253	262	Ten Digit PAN used by Income Tax Department
17	Communication Address 1*	CHAR	45	263	307	Field + filler spaces = 45
18	Communication Address 2	CHAR	45	308	352	Field + filler spaces = 45
19	Communication Address 3	CHAR	45	353	397	Field + filler spaces = 45
20	Communication Address 4	CHAR	45	398	442	Field + filler spaces = 45
21	Communication Address 5	CHAR	45	443	487	Field + filler spaces = 45
22	Communication Address Pin code*	NUM	6	488	493	Pin code without “-” or space
23	Contact Telephone	CHAR	30	494	523	Telephone number in format STD Code-Telephone number
24	Contact Fax	CHAR	30	524	553	Fax number in format STD Code-Telephone number
25	Contact Email	CHAR	50	554	603	E-mail address
26	Registered Address 1	CHAR	45	604	648	Registered address (if different from above).
27	Registered Address 2	CHAR	45	649	693	Field + filler spaces = 45
28	Registered Address 3	CHAR	45	694	738	Field + filler spaces = 45
29	Registered Address 4	CHAR	45	739	783	Field + filler spaces = 45
30	Registered Address 5	CHAR	45	784	828	Field + filler spaces = 45
31	Registered Address Pin code	NUM	6	829	834	Pin code without “-” or space
32	Registered office Telephone	CHAR	30	835	864	Telephone number in format STD Code-Telephone number
33	Registered office Fax	CHAR	30	865	894	Fax number in format STD Code-Telephone number

SUSPICIOUS TRANSACTION REPORT (STR) FOR A BANKING COMPANY

Kindly fill in CAPITAL. Read the instructions before filling the form.

PART 1 DETAILS OF REPORT

1.1 Date of sending report 2 | 0 | 0
D D M M Y Y Y Y

1.2 Is this a replacement to an earlier report ? NO YES (Tick ✓ as applicable)

1.3 Date of sending original report if this is a replacement report 2 | 0 | 0
D D M M Y Y Y Y

PART 2 DETAILS OF PRINCIPAL OFFICER

2.1 Name of Bank

2.2 BSR code 2.3 ID allotted by FIU-IND

2.4 Category of bank (Refer to Instructions)

2.5 Name of principal officer

2.6 Designation

2.7 Address (No., Building)

2.8 Street/Road

2.9 Locality

2.10 City/Town, District

2.11 State, Country

2.12 Pin code 2.13 Tel (with STD code)

2.14 Fax 2.15 E-mail

PART 3 DETAILS OF REPORTING BRANCH / LOCATION

3.1 Name of Branch/Location

3.2 BSR code 3.3 ID allotted by FIU-IND

3.4 Address (No., Building)

3.5 Street/Road

3.6 Locality

3.7 City/Town, District

3.8 State, Country

3.9 Pin code 3.10 Tel (with STD code)

3.11 Fax 3.12 E-mail

SUSPICIOUS TRANSACTION REPORT (STR) FOR A BANKING COMPANY

Kindly fill in CAPITAL. Read the Instructions before filling the form.

PART 4 LIST OF INDIVIDUALS LINKED TO TRANSACTIONS

	Name of individual	Customer ID/number (if allotted)	Annexure
4.1			A 1
4.2			A 2
4.3			A 3
4.4			A 4
4.5			A 5
4.6			A 6
4.7			A 7
4.8			A 8
4.9			A 9
4.10			A 10
4.11			A 11
4.12			A 12
4.13			A 13
4.14			A 14
4.15			A 15

(Details of all individuals should be furnished in prescribed annexure) Tick to confirm

Number of additional sheets for PART 4 attached (Leave blank if space provided above is sufficient and no extra sheet is attached)

PART 5 LIST OF LEGAL PERSONS/ENTITIES LINKED TO TRANSACTIONS

	Name of legal person/entity	Customer ID/number (if allotted)	Annexure
5.1			B 1
5.2			B 2
5.3			B 3
5.4			B 4
5.5			B 5
5.6			B 6
5.7			B 7
5.8			B 8
5.9			B 9
5.10			B 10

(Details of all legal persons/entities should be furnished in prescribed annexure) Tick to confirm

Number of additional sheets for PART 5 attached (Leave blank if space provided above is sufficient and no extra sheet is attached)

SUSPICIOUS TRANSACTION REPORT (STR) FOR A BANKING COMPANY

Kindly fill in CAPITAL. Read the Instructions before filling the form.

PART 6 LIST OF ACCOUNTS LINKED TO TRANSACTIONS

	Account Number	Name of First Account Holder	Annexure
6.1			C 1
6.2			C 2
6.3			C 3
6.4			C 4
6.5			C 5
6.6			C 6
6.7			C 7
6.8			C 8
6.9			C 9
6.10			C 10

(Details of all accounts should be furnished in prescribed annexure)

Tick to confirm

Number of additional sheets for PART 6 attached (Leave blank if space provided above is sufficient and no extra sheet is attached)

PART 7 DETAILS OF SUSPICIOUS TRANSACTION

7.1 Reasons for suspicion (Tick as applicable. Multiple selection is possible. Refer to instructions)

- | | | |
|---|--|---|
| <input type="checkbox"/> A Identity of client | <input type="checkbox"/> B Background of client | <input type="checkbox"/> C Multiple accounts |
| <input type="checkbox"/> D Activity in account | <input type="checkbox"/> E Nature of transaction | <input type="checkbox"/> F Value of transaction |
| <input type="checkbox"/> Z Other reason (specify) | <input type="text"/> | |

7.2 Grounds of Suspicion (Mention summary of suspicion and sequence of events)

(continued on next page)

SUSPICIOUS TRANSACTION REPORT (STR) FOR A BANKING COMPANY

Kindly fill in CAPITAL. Read the Instructions before filling the form.

7.3 Grounds of Suspicion (continued from previous page)

Number of additional sheets for PART 7 attached (Leave blank if space provided above is sufficient and no extra sheet is attached)

PART 8 DETAILS OF ACTION TAKEN

8.1 Whether the matter is/was under any investigation? (Mention the name of agency, person and contact details)

Number of additional sheets for PART 8 attached (Leave blank if space provided above is sufficient and no extra sheet is attached)

DO NOT FILL. FOR FIU-IND USE ONLY	
ACK. NO.	_ _ _ _ _ _ _ _ _
DATE	_ _ _ _ 2 0 0 D D M M Y Y Y Y

Signature

Name

(Should be same as the person mentioned in PART 2)

DO NOT FILL. FOR FIU-IND USE ONLY.

_ _ _ _ _ _ _ _ _

SBA04

SUSPICIOUS TRANSACTION REPORT (STR) FOR A BANKING COMPANY INSTRUCTIONS

GENERAL INSTRUCTIONS

The Prevention of Money Laundering Act 2002

Under the Prevention of Money Laundering Act 2002, every banking company shall furnish details of suspicious transactions whether or not made in cash.

Suspicious transaction means a 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 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.

How to submit

Every bank branch must submit this form to the Director, FIU-IND only through the principal officer of the banking company designated under PMLA, 2002. In urgent cases, the form should also be sent by fax.

Address Director, FIU-IND
 Financial Intelligence Unit-India
 6th Floor, Hotel Samrat
 Chanakyapuri, New Delhi -110021
 India

Fax +91-11-26874459

EXPLANATION OF SPECIFIC TERMS

PART 1: DETAILS OF REPORT

- 1.1. Date of sending report is the date on which the principal officer sends the report to Director (FIU-IND).
- 1.2. Replacement report is a report submitted in replacement of an earlier STR. When a replacement report is submitted, date of submitting original STR may be mentioned and the complete STR has to be submitted again.

PART 2: DETAILS OF PRINCIPAL OFFICER

- 2.3. ID allotted by FIU-IND may be left blank till the same is communicated by FIU-IND.
- 2.4. Category of the bank
 "A"-Public Sector Bank "E"-Regional Rural Bank
 "B"-Private Sector Bank "F"-Local Area Bank
 "C"-Foreign Bank "Z"-Other
 "D"-Co-operative Bank

- 2.5. Principal officer is the officer designated by the banking company under PMLA, 2002

PART 3: DETAILS OF REPORTING BRANCH / LOCATION

Particulars of the branch/location in which the reported accounts are maintained should be submitted in this part.

PART 4: LIST OF INDIVIDUALS LINKED TO TRANSACTIONS

Customer ID/number may be given if allotted by bank. Enclose a separate Annexure A for each individual.

PART 5: LIST OF LEGAL PERSONS/ENTITIES LINKED TO TRANSACTIONS

Customer ID/number may be given if allotted by bank. Enclose a separate Annexure B for each legal person/entity. Include the details about individuals (Director/Partner/Member etc.) related to the

PART 6: LIST OF ACCOUNTS LINKED TO TRANSACTIONS

Enclose a separate Annexure C for each account.

PART 7: DETAILS OF SUSPICIOUS TRANSACTION

Reasons for suspicion

Reason	Examples of suspicious transaction
Identity of client	<i>False identification documents</i>
	<i>Identification documents which could not be verified within reasonable time</i>
	<i>Accounts opened with names very close to other established business entities</i>
Background of client	<i>Suspicious background or links with known criminals</i>
Multiple accounts	<i>Large number of accounts having a common account holder, introducer or authorized signatory with no rationale</i>
	<i>Unexplained transfers between multiple accounts with no rationale</i>
Activity in accounts	<i>Unusual activity compared with past transactions</i>
	<i>Sudden activity in dormant accounts</i>
	<i>Activity inconsistent with what would be expected from declared business</i>
Nature of transactions	<i>Unusual or unjustified complexity</i>
	<i>No economic rationale or bonafide purpose</i>
	<i>Frequent purchases of drafts or other negotiable instruments with cash</i>
Value of transactions	<i>Nature of transactions inconsistent with what would be expected from declared business</i>
	<i>Value just under the reporting threshold amount in an apparent attempt to avoid reporting</i>
	<i>Value inconsistent with the client's apparent financial standing</i>

ALL ANNEXURES MUST BE ENCLOSED.

ANNEXURE A - INDIVIDUAL DETAIL SHEET FOR A BANKING COMPANY

INDIVIDUAL **A**

Use separate annexure for each individual.

Kindly fill in CAPITAL.

1. Name of bank (with branch)	<input style="width: 100%;" type="text"/>		
2. BSR code	<input style="width: 100%;" type="text"/>		
3. Annexure enclosed with	<input type="checkbox"/> A Cash Transaction Report	<input type="checkbox"/> B Counterfeit Currency Report	
	<input type="checkbox"/> C Suspicious Transaction Report <i>(Tick ✓ as applicable)</i>		
4. Full name of individual	<input style="width: 100%;" type="text"/>		
5. Customer ID/number	<input style="width: 100%;" type="text"/> <i>(If allotted)</i>		
6. Name of father/spouse	<input style="width: 100%;" type="text"/>		
7. Occupation	<input style="width: 100%;" type="text"/>		
8. Date of birth	<input style="width: 100px;" type="text"/>	9. Sex (M/F) <input type="checkbox"/>	10. Nationality <input style="width: 100px;" type="text"/>
11. Identification document	DD - MM - YYYY		
	<input type="checkbox"/> A Passport	<input type="checkbox"/> B Election ID card	<input type="checkbox"/> C PAN card
	<input type="checkbox"/> D ID card	<input type="checkbox"/> E Driving license	<input type="checkbox"/> F Account introducer
	<input type="checkbox"/> Z Other (Specify) <input style="width: 150px;" type="text"/>		
12. Identification number	<input style="width: 150px;" type="text"/>	<i>(Number mentioned in the identification document)</i>	
13. Issuing authority	<input style="width: 150px;" type="text"/>	<i>(Authority which had issued the document)</i>	
14. Place of Issue	<input style="width: 150px;" type="text"/>	<i>(Place where the document was issued)</i>	
15. PAN	<input style="width: 100%;" type="text"/>		
Communication address			
16. No., Building	<input style="width: 100%;" type="text"/>		
17. Street/Road	<input style="width: 100%;" type="text"/>		
18. Locality	<input style="width: 100%;" type="text"/>		
19. City/Town, District	<input style="width: 100%;" type="text"/>		
20. State, Country	<input style="width: 100%;" type="text"/>		
21. Pin code	<input style="width: 100px;" type="text"/>	22. Tel (with STD code)	<input style="width: 100px;" type="text"/>
23. Mobile number	<input style="width: 100px;" type="text"/>	24. E-mail	<input style="width: 100px;" type="text"/>
25. Name of Organisation/Employer	<input style="width: 100%;" type="text"/>		
Second Address (Permanent address/Place of work)			
26. No., Building	<input style="width: 100%;" type="text"/>		
27. Street/Road	<input style="width: 100%;" type="text"/>		
28. Locality	<input style="width: 100%;" type="text"/>		
29. City/Town, District	<input style="width: 100%;" type="text"/>		
30. State, Country	<input style="width: 100%;" type="text"/>		
31. Pin code	<input style="width: 100px;" type="text"/>	32. Tel (with STD code)	<input style="width: 100px;" type="text"/>
DO NOT FILL. FOR FIU-IND USE ONLY.			BAA

ANNEXURE B - LEGAL PERSON/ENTITY DETAIL SHEET FOR A BANKING COMPANY

LEGAL PERSON/ENTITY **B**

Use separate annexure for each legal person/entity. Kindly fill in CAPITAL.

1. Name of bank (with branch)	<input style="width:100%;" type="text"/>			
2. BSR code	<input style="width:100%;" type="text"/>			
3. Annexure enclosed with	<input type="checkbox"/> A	Cash Transaction Report	<input type="checkbox"/> B	Counterfeit Currency Report
	<input type="checkbox"/> C	Suspicious Transaction Report	<i>(Tick ✓ as applicable)</i>	
4. Name of legal person/entity	<input style="width:100%;" type="text"/>			
5. Customer ID/number	<input style="width:100%;" type="text"/> <i>(If allotted)</i>			
6. Nature of business	<input style="width:100%;" type="text"/>			
7. Date of incorporation	<input style="width:100%;" type="text"/>			
8. Type of Constitution	DD - MM - YYYY			
	<input type="checkbox"/> A	Sole proprietorship	<input type="checkbox"/> B	Firm
	<input type="checkbox"/> D	Pvt. ltd. company	<input type="checkbox"/> E	Public ltd. company
	<input type="checkbox"/> G	Association	<input type="checkbox"/> H	Trust
	<input type="checkbox"/> Z	Other (Specify)	<input type="checkbox"/> C	HUF
			<input type="checkbox"/> F	Society
			<input type="checkbox"/> I	Liquidator
9. Registration number	<input style="width:100%;" type="text"/> <i>(Number mentioned in the deed/document)</i>			
10. Registering Authority	<input style="width:100%;" type="text"/> <i>(Authority registering the deed/document)</i>			
11. Place of Registration	<input style="width:100%;" type="text"/> <i>(Place where the document was registered)</i>			
12. PAN	<input style="width:100%;" type="text"/>			
Communication address:				
13. No., Building	<input style="width:100%;" type="text"/>			
14. Street/Road	<input style="width:100%;" type="text"/>			
15. Locality	<input style="width:100%;" type="text"/>			
16. City/Town, District	<input style="width:100%;" type="text"/>			
17. State, Country	<input style="width:100%;" type="text"/>			
18. Pin code	<input style="width:100%;" type="text"/>	19. Tel (with STD code)	<input style="width:100%;" type="text"/>	
20. Fax (with STD code)	<input style="width:100%;" type="text"/>	21. E-mail	<input style="width:100%;" type="text"/>	
22. List of directors /partners / members and other related persons				
	Name of Individual/Legal Person/Entity	Customer ID/number	Relation	Annexure
22.1	<input style="width:100%;" type="text"/>	<input style="width:100%;" type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
22.2	<input style="width:100%;" type="text"/>	<input style="width:100%;" type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
22.3	<input style="width:100%;" type="text"/>	<input style="width:100%;" type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
22.4	<input style="width:100%;" type="text"/>	<input style="width:100%;" type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
22.5	<input style="width:100%;" type="text"/>	<input style="width:100%;" type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
Mention B for Authorised Signatory, C for Director/member etc. , D for Introducer. E for Guarantor, Z for others				
Mention A for Individuals, B for Legal Person/ Entity				
Mention appropriate Annexure number				
Tick ✓ to confirm				
DO NOT FILL. FOR FIU-IND USE ONLY.			BAB	

ANNEXURE C - ACCOUNT DETAIL SHEET FOR A BANKING COMPANY

ACCOUNT

Use separate annexure for each account. Kindly fill in CAPITAL.

1	Name of bank (with branch)	<input style="width:100%;" type="text"/>		
2	BSR code	<input style="width:100%;" type="text"/>		
3	Annexure enclosed with	<input type="checkbox"/> A Cash Transaction Report	<input type="checkbox"/> B Counterfeit Currency Report	
		<input type="checkbox"/> C Suspicious Transaction Report (Tick ✓ as applicable)		
4	Account number	<input style="width:100%;" type="text"/>		
5	Type of account	<input type="checkbox"/> A Savings account	<input type="checkbox"/> B Current account	<input type="checkbox"/> C Cash credit account
		<input type="checkbox"/> Z Other (Specify) <input style="width:100%;" type="text"/>		
6	Type of account holder	<input type="checkbox"/> A Individual	<input type="checkbox"/> B Legal person/entity	<input type="checkbox"/> C Central/State Government
		<input type="checkbox"/> D Central/State Government owned undertaking	<input type="checkbox"/> Z Other	
7	Date of account opening	<input style="width:100%;" type="text"/>		
		DD - MM - YYYY		

8 List of account holders

	Name of Individual/Legal Person/Entity	Customer ID/number (if allotted)	Annexure	
8.1	<input style="width:100%;" type="text"/>	<input style="width:100%;" type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.2	<input style="width:100%;" type="text"/>	<input style="width:100%;" type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.3	<input style="width:100%;" type="text"/>	<input style="width:100%;" type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>

Mention A for Individuals, B for Legal Person/ Entity
Mention appropriate annexure number

(Details of all account holders should be furnished in prescribed annexure, Tick ✓ to confirm)

Number of additional sheets for account holders (Leave blank if space provided above is sufficient and no extra sheet is attached)

9 List of related persons (other than mentioned at 8 above)

	Name of Individual/Legal Person/Entity	Customer ID/number (if allotted)	Relation	Annexure	
9.1	<input style="width:100%;" type="text"/>	<input style="width:100%;" type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.2	<input style="width:100%;" type="text"/>	<input style="width:100%;" type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.3	<input style="width:100%;" type="text"/>	<input style="width:100%;" type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.4	<input style="width:100%;" type="text"/>	<input style="width:100%;" type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.5	<input style="width:100%;" type="text"/>	<input style="width:100%;" type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Mention B for Authorised Signatory, D for Introducer, E for Guarantor, Z for others
Mention A for Individuals, B for Legal Person/ Entity
Mention appropriate Annexure number

(Details of all related persons should be furnished in prescribed annexure) Tick ✓ to confirm

Number of additional sheets for related persons (Leave blank if space provided above is sufficient and no extra sheet is attached)

DO NOT FILL. FOR FIU-IND USE ONLY. BAC

ANNEXURE C - ACCOUNT DETAIL SHEET FOR A BANKING COMPANY

ACCOUNT **C**

Kindly fill in CAPITAL.

(mention the same number as on the previous page)

10 Transaction details

	Date of Transaction	Mode	Debit	Amount in Rupees	Remarks <i>(foreign currency and other details)</i>
10.1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
10.2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
10.3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
10.4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
10.5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
10.6	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
10.7	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
10.8	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
10.9	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
10.10	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

DD - MM - YYYY

D for Debit and C for Credit

A- Cheque B- Transfer within Branch C- Cash D- Demand Draft E- Electronic Funds Transfer
 F- Traveller's Cheque Z-Other (Specify)

Number of additional sheets for transactions (Leave blank if space provided above is sufficient and no extra sheet is attached)

11 Cumulative Totals

11.1 Total debits in the bank account in the financial year

11.2 Total credits in the bank account in the financial year

(Total of entries in the bank account from 1st April of the financial year till the date of reporting)

12 Write up about transactions (transactions mentioned in 10 above)

ELECTRONIC FILE STRUCTURE

<i>Report</i>	SUSPICIOUS TRANSACTION REPORT
<i>Reporting Agency</i>	BANKING COMPANY
<i>Version</i>	1.0

Contents

1.	Introduction.....	1
2.	Financial Intelligence Unit – India	1
3.	Prevention of Money Laundering Act, 2002	1
4.	Suspicious Transaction Report	2
5.	Due Date	3
6.	Banking Company	3
7.	Methods of filing	3
8.	Manual format	3
9.	Electronic Format	3
10.	Description of Data files.....	4
11.	Steps in preparation of Data files.....	4
12.	Steps in validation of Data files.....	5
13.	General Notes for all Data files	6
14.	Data Structure of Control File (SBACTL.txt)	6
15.	Data Structure of Branch Data File (SBABRC.txt).....	8
16.	Data Structure of Account Data File (SBAACC.txt).....	9
17.	Data Structure of Transaction Data File (SBATRN.txt)	10
18.	Data Structure of Individual Data File (SBAINP.txt)	11
19.	Data Structure of Legal Person/Entity Data File (SBALPE.txt)	13

Appendix

[Suspicious Transaction Report for a Banking Company](#)

[Annexure A- Individual Detail Sheet for a Banking Company](#)

[Annexure B- Legal Person/ Entity Detail Sheet for a Banking Company](#)

[Annexure C- Account Detail Sheet for a Banking Company](#)

Report SUSPICIOUS TRANSACTION REPORT	Reporting Agency BANKING COMPANY	Version 1.0
---	-------------------------------------	----------------

1. Introduction

The Prevention of Money Laundering Act, 2002 (PMLA 2002) forms the core of the legal framework put in place by India to combat money laundering. PMLA 2002 and the Rules notified thereunder came into force with effect from July 1, 2005. Director, FIU-IND and Director (Enforcement) have been conferred with exclusive and concurrent powers under relevant Sections of the Act to implement the provisions of the Act.

The PMLA 2002 and Rules notified thereunder impose an obligation on banking companies, financial institutions and intermediaries of the securities market to verify identity of clients, maintain records and furnish information to FIU-IND.

2. Financial Intelligence Unit – India

The Government of India set up Financial Intelligence Unit – India (FIU-IND) on 18th November 2004 as an independent body to report directly to the Economic Intelligence Council (EIC) headed by the Finance Minister.

FIU-IND has been established as the central national agency responsible for receiving, processing, analyzing and disseminating information relating to suspect financial transactions. FIU-IND is also responsible for coordinating and strengthening efforts of national and international intelligence and enforcement agencies in pursuing the global efforts against money laundering and related crimes. The address of Financial Intelligence Unit – India (FIU-IND) is:

Director, FIU-IND
Financial Intelligence Unit-India
6th Floor, Hotel Samrat
Chanakyapuri, New Delhi -110021
India

Website: www.fiuindia.gov.in

3. Prevention of Money Laundering Act, 2002

Section 12 of the Prevention of Money Laundering Act, 2002 lays down following obligations on banking companies.

- “12. (1) Every banking company, financial institution and intermediary shall-*
- (a) maintain a record of all transactions, the nature and value of which may be prescribed, whether such transactions comprise of a single transaction or a series of transactions integrally connected to each other, and where such series of transactions take place within a month;*
 - (b) furnish information of transactions referred to in clause (a) to the Director within such time as may be prescribed;*
 - (c) verify and maintain the records of the identity of all its clients, in such a manner as may be prescribed.*

Provided that where the principal officer of a banking company or financial institution or intermediary, as the case may be has reason to believe that a single transaction or series of transactions integrally connected to each other have been valued below the prescribed limit so as to defeat the provisions of this section, such officer shall furnish information in respect of such transactions to the Director within the prescribed time.

Report SUSPICIOUS TRANSACTION REPORT	Reporting Agency BANKING COMPANY	Version 1.0
--	--	-----------------------

(2) The records referred to in sub-section (1) shall be maintained for a period of ten years from the date of cessation of the transactions between the clients and the banking company or financial institution or intermediary, as the case may be.”

4. Suspicious Transaction Report

The Prevention of Money laundering Act, 2002 and the Rules thereunder require every banking company to furnish details of suspicious transactions whether or not made in cash. Suspicious transaction means a 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 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.

Broad categories of reason for suspicion and examples of suspicious transactions for a banking company are indicated as under:

Identity of client

- False identification documents
- Identification documents which could not be verified within reasonable time
- Accounts opened with names very close to other established business entities

Background of client

- Suspicious background or links with known criminals

Multiple accounts

- Large number of accounts having a common account holder, introducer or authorized signatory with no rationale
- Unexplained transfers between multiple accounts with no rationale

Activity in accounts

- Unusual activity compared with past transactions
- Sudden activity in dormant accounts
- Activity inconsistent with what would be expected from declared business

Nature of transactions

- Unusual or unjustified complexity
- No economic rationale or bonafide purpose
- Frequent purchases of drafts or other negotiable instruments with cash
- Nature of transactions inconsistent with what would be expected from declared business

Value of transactions

- Value just under the reporting threshold amount in an apparent attempt to avoid reporting
- Value inconsistent with the client’s apparent financial standing

Report SUSPICIOUS TRANSACTION REPORT	Reporting Agency BANKING COMPANY	Version 1.0
--	--	-----------------------

5. Due Date

Rule 8 of Notification No. 9/2005 dated 1-7-2005 require the Principal Officer of a banking company to furnish the information of the suspicious transactions to Director, FIU-IND not later than three working days from the date of occurrence of such transactions.

6. Banking Company

Banking company means a banking company or a co-operative bank to which the Banking Regulation Act, 1949 applies and includes any bank or banking institution referred to in section 51 of that Act (Defined in 2(1)(e) of PMLA 2002). Banking Company includes:

- i) All nationalized banks, private Indian banks and private foreign banks,
- ii) All co-operative banks viz. primary co-operative banks, state co-operative banks and central co-operative banks,
- iii) State Bank of India and its associates and subsidiaries,
- iv) Regional Rural Banks

7. Methods of filing

Suspicious Transaction Reports can be filed either in manual or electronic format. However, a reporting agency must submit all reports to FIU-IND in electronic format if it has the technical capability to do so. The required technical capability is defined as follows:

- i) A personal computer with 32 MB memory RAM, 800 x 600 VGA video display, Windows® 98/Me/NT/2000/XP; and
- ii) An Internet connection.

8. Manual format

Suspicious Transaction Report in manual format consists of the following forms:

Form	Information
Suspicious Transaction Report for a Banking Company	Details of suspicious transactions
Annexure A- Individual Detail Sheet for a Banking Company	Identification details of individual
Annexure B- Legal Person/ Entity Detail Sheet for a Banking Company	Identification details of legal person /entity
Annexure C- Account Detail Sheet for a Banking Company	Details of bank account and transactions

The above forms are given in the Appendix.

9. Electronic Format

FIU-IND is in the process of developing technological infrastructure to enable submission of electronic return over a secure gateway. In the interim the banks exercising the electronic option should submit the following to Director, FIU-IND:

- i) One CD containing six data files in prescribed data structure. A label mentioning name of the bank, BSR code of bank, type of report (STR), Serial number of STR for the

Report SUSPICIOUS TRANSACTION REPORT	Reporting Agency BANKING COMPANY	Version 1.0
--	--	-----------------------

bank, date of sending report should be affixed on each CD for the purpose of identification.

- ii) Each CD should be accompanied by Suspicious Transaction Report for a Banking Company (same form should be used for both manual as well as electronic format) in physical form duly signed by the principal officer. This summary should match with the data in Control File (SBACTL.txt). Other annexures (Annexure A to C) need not be submitted in the physical form.

Important:

- i) In case the size of data files exceeds the capacity of one CD, the data files should be compressed by using Winzip 8.1 or ZipItFast 3.0 (or higher version) compression utility only to ensure quick and smooth acceptance of the file.
- ii) The CD should be virus free.

10. Description of Data files

In case of electronic filing, the STR data for the banking company should have following six data files:

S No.	Filename	Description
1	SBACTL.txt	Control File
2	SBABRC.txt	Branch Data File
3	SBAACC.txt	Account Data File
4	SBATRN.txt	Transaction Data File
5	SBAINP.txt	Individual Data File
6	SBALPE.txt	Legal Person/Entity Data File

11. Steps in preparation of Data files

- i) The records containing details of suspicious transactions to be reported are extracted in Transaction Data File (SBATRN.txt).
- ii) The records containing details of bank accounts containing the suspicious transactions are extracted in Accounts Data File (SBAACC.txt).
- iii) If the account is for Individuals, the records containing details of Individuals who are account holders are extracted in Individual Data File (SBAINP.txt). The Relation Flag should be set to "A".
- iv) If the account is for a Legal Person /Entity, the records containing details of Legal Persons /Entities who are account holders are extracted in Legal Persons /Entities Data File (SBALPE.txt). The Relation Flag should be set to "A".
- iii) If the account is for a Legal Person /Entity, the records containing details of Directors/ Partner/ Members etc. of Legal Persons /Entities are appended to Individual Data File (SBAINP.txt). The Relation Flag should be set to "C".
- v) The records containing details of authorised signatories if not an account holder are appended to Individual Data File (SBAINP.txt) or Legal Persons /Entities Data File (SBALPE.txt) as the case may be. The Relation Flag should be set to "B".

Report SUSPICIOUS TRANSACTION REPORT	Reporting Agency BANKING COMPANY	Version 1.0
--	--	-----------------------

- vi) The records containing details of account introducers are appended to Individual Data File (SBAINP.txt) or Legal Persons /Entities Data File (SBALPE.txt) as the case may be. The Relation Flag should be set to “D”.
- vii) The records containing details of account guarantors are appended to Individual Data File (SBAINP.txt) or Legal Persons /Entities Data File (SBALPE.txt) as the case may be. The Relation Flag should be set to “E”.
- viii) The records containing details of bank branches which have reported suspicious transactions are extracted in Branch Data File (SBABRC.txt).
- ix) The report level details and summary of other five tables is entered in Control file. (SBACTL.txt)

12. Steps in validation of Data files

- i) There should be six data files with appropriate naming convention.
- ii) The data files should be as per specified data structure and business rules.
- iii) None of the mandatory fields should be left blank.
- iv) Date of report should be same in all data files.
- v) The summary figures in control file should match with the totals in other data files.
- vi) The primary key integrity should be validated as under:
 - a. [Branch Reference Number] should be unique in Branch Data File (SBABRC.txt)
 - b. [Branch Reference Number + Account Number] should be unique in Account Data File (SBAACC.txt)
- vii) The foreign key integrity should be validated as under:
 - a. All values of [Branch Reference Number] in Account Data File (SBAACC.txt) should have a matching [Branch Reference Number] value in Branch Data File (SBABRC.txt)
 - b. All values of [Branch Reference Number + Account Number] in Transaction Data File (SBATRN.txt) should have matching [Branch Reference Number + Account Number] value in Account Data File (SBAACC.txt)
 - c. All values of [Branch Reference Number + Account Number] in Individual Data File (SBAINP.txt) should have matching [Branch Reference Number + Account Number] value in Account Data File (SBAACC.txt)
 - d. All values of [Branch Reference Number + Account Number] in Legal Person / Entity Data File (SBALPE.txt) should have matching [Branch Reference Number + Account Number] value in Account Data File (SBAACC.txt)
- viii) The data sufficiency should be validated as under:
 - a. All values of [Branch Reference Number + Account Number] in Account Data File (SBAACC.txt) should have at least one matching [Branch Reference Number + Account Number] value in Transaction Data File (SBATRN.txt).

Report SUSPICIOUS TRANSACTION REPORT	Reporting Agency BANKING COMPANY	Version 1.0
--	--	-----------------------

- b. All values of [Branch Reference Number + Account Number] in Account Data File (SBAACC.txt) should have at least one matching [Branch Reference Number + Account Number] value in Individual Data File (SBAINP.txt). (As account for legal person/entity would have individuals as authorised signatories).
- c. All values of [Branch Reference Number + Account Number] in Account Data File (SBAACC.txt) with Type of Account Holder = “B” (Legal Person/Entity) should have at least one matching [Branch Reference Number + Account Number] value in Legal Person / Entity Data File (SBALPE.txt).

13. General Notes for all Data files

- i) All Data Files should be generated in ASCII Format with ".txt" as filename extension.
- ii) Each Record (including last record) must start on new line and must end with a newline character. Hex Values: "0D" & "0A".
- iii) All CHAR fields must be left justified.
- iv) If CHAR field has no data or less data with respect to defined length, then the entire field (in case of no data) or the remaining field (in case of less data) has to be filled with right justified blank characters (Spaces).
- v) All NUM fields must be right justified.
- vi) If NUM field has no data or less data with respect to defined length, then the entire field (in case of no data) or the remaining field (in case of less data) has to be filled with left justified zeroes.
- vii) If DATE field has no data then the entire field has to be filled with blank characters (Spaces).
- viii) Fields with an asterisk (*) have to be compulsorily filled up.
- ix) For fields that do not have an asterisk (*), reasonable efforts have to be made to get the information. Enter “N/A” to indicate that the field is not applicable. Do not substitute any other abbreviations or special characters (e.g., “x”, “-” or “*”).

14. Data Structure of Control File (SBACTL.txt)

	Field	Type	Size	From	To	Remarks
1	Report Name*	CHAR	3	1	3	Value should be “SBA” signifying STR for banking company
2	Serial Number of Report*	NUM	8	4	11	Indicates the running sequence number of STR for the reporting agency starting from 00000001
3	Record Type*	CHAR	3	12	14	Value should be “CTL” signifying Control file
4	Date of Report	DATE	8	15	22	Date of sending report in DDMMYYYY Format
5	Complete name of Bank*	CHAR	80	23	102	Field + filler spaces = 80
6	Category of Bank*	CHAR	1	103	103	“A”-Public Sector Bank “B”-Private Sector Bank “C”-Foreign Bank

Report SUSPICIOUS TRANSACTION REPORT	Reporting Agency BANKING COMPANY	Version 1.0
--	--	-----------------------

						“D”-Co-operative Bank “E”-Regional Rural Bank “F”-Local Area Bank “Z”-Other
7	BSR code *	CHAR	7	104	110	BSR code issued by RBI
8	Unique ID issued by FIU*	CHAR	10	111	120	Use XXXXXXXXXXXX till the ID is communicated
9	Principal Officer’s Name*	CHAR	80	121	200	Field + filler spaces = 80
10	Principal Officer’s Designation*	CHAR	80	201	280	Field + filler spaces = 80
11	Principal Officer’s Address1*	CHAR	45	281	325	No., Building Field + filler spaces = 45
12	Principal Officer’s Address2	CHAR	45	326	370	Street/Road Field + filler spaces = 45
13	Principal Officer’s Address3	CHAR	45	371	415	Locality Field + filler spaces = 45
14	Principal Officer’s Address4	CHAR	45	416	460	City/Town, District Field + filler spaces = 45
15	Principal Officer’s Address5	CHAR	45	461	505	State, Country Field + filler spaces = 45
16	Principal Officer’s Pin code*	NUM	6	506	511	Pin code without “-” or space
17	Principal Officer’s Telephone	CHAR	30	512	541	Telephone in format STD Code-Telephone number
18	Principal Officer’s FAX	CHAR	30	542	571	Fax number in format STD Code-Telephone number
19	Principal Officer’s E-mail	CHAR	50	572	621	E-mail address
20	Report Type*	CHAR	1	622	622	“N”- New Report “R”- Replacement to earlier submitted report
21	Reason for Replacement*	CHAR	1	623	623	“A” – Acknowledgement of Original Report had many warnings or error messages. “B” – Operational error, data omitted in Original Report. “C” – Operational error, wrong data submitted in Original Report. “N”- Not Applicable as this is a new report “Z”- Other Reason
22	Serial Number of Original Report *	NUM	8	624	631	Serial Number of the Original Report which is being replaced. Mention 00000000 if Report Type is “N”
23	Operational Mode*	CHAR	1	632	632	“P”- Actual/ Production mode “T”- Test / Trial mode
24	Data Structure Version*	CHAR	1	633	633	Value should be 1 to indicate

Report SUSPICIOUS TRANSACTION REPORT	Reporting Agency BANKING COMPANY	Version 1.0
--	--	-----------------------

						Version 1.0
25	Number of accounts linked to suspicious transactions*	NUM	8	634	641	Count of total number of records in SBAACC.txt
26	Number of Transactions*	NUM	8	642	649	Count of total number of records in SBATRN.txt
27	Number of Individual Persons*	NUM	8	650	657	Count of total number of records in SBAINP.txt
28	Number of Legal Person/entities*	NUM	8	658	665	Count of total number of records in SBALPE.txt
29	Suspicion due to Identity of Client*	CHAR	1	666	666	Mention "Y" or "N"
30	Suspicion due to Background of Client*	CHAR	1	667	667	Mention "Y" or "N"
31	Suspicion due to Multiple Accounts*	CHAR	1	668	668	Mention "Y" or "N"
32	Suspicion due to Activity in Accounts*	CHAR	1	669	669	Mention "Y" or "N"
33	Suspicion due to Nature of Transactions*	CHAR	1	670	670	Mention "Y" or "N"
34	Suspicion due to Value of Transactions*	CHAR	1	671	671	Mention "Y" or "N"
35	Grounds of Suspicion*	CHAR	4000	672	4671	Write summary of suspicion and sequence of events
36	Details of other investigations	CHAR	4000	4672	8671	Write details about agency, contact person and contact details
37	Acknowledgement Number	NUM	10	8672	8681	For internal use of FIU-IND. Use value 0000000000
38	Date of Acknowledgement	DATE	8	8682	8689	For internal use of FIU-IND. Use value "XXXXXXXX"

15. Data Structure of Branch Data File (SBABRC.txt)

	Field	Type	Size	From	To	Remarks
1	Record Type*	CHAR	3	1	3	Value should be "BRC" signifying Branch Data file
2	Date of Report	DATE	8	4	11	Date of sending report in DDMMYYYY Format. This date should be same as in control file
3	Line Number*	NUM	6	12	17	Running Sequence Number for each line in the file starting from 000001. This Number will be used during validation checks.
4	Name of Branch*	CHAR	80	18	97	Field + filler spaces = 80
5	Branch Reference Number*	CHAR	7	98	104	BSR code issued by RBI
6	Unique ID issued by FIU*	CHAR	10	105	114	Use XXXXXXXXXXXX till the ID is communicated

Report SUSPICIOUS TRANSACTION REPORT	Reporting Agency BANKING COMPANY	Version 1.0
--	--	-----------------------

7	Branch Address1*	CHAR	45	115	159	No., Building Field + filler spaces = 45
8	Branch Address2*	CHAR	45	160	204	Street/Road Field + filler spaces = 45
9	Branch Address3	CHAR	45	205	249	Locality Field + filler spaces = 45
10	Branch Address4	CHAR	45	250	294	City/Town, District Field + filler spaces = 45
11	Branch Address5	CHAR	45	295	339	State, Country Field + filler spaces = 45
12	Branch Pin code*	NUM	6	340	345	Pin code without “-” or space
13	Branch Telephone	CHAR	30	346	375	Telephone number in format STD Code-Telephone number
14	Branch Fax	CHAR	30	376	405	Fax number in format STD Code-Telephone number
15	Branch E-mail	CHAR	50	406	455	E-mail address

16. Data Structure of Account Data File (SBAACC.txt)

	Field	Type	Size	From	To	Remarks
1	Record Type*	CHAR	3	1	3	Value should be “RAC” signifying Reported Account file
2	Date of Report	DATE	8	4	11	Date of sending report in DDMMYYYY Format. This date should be same as in control file
3	Line Number*	NUM	6	12	17	Running Sequence Number for each line in the file starting from 000001. This Number will be used during validation checks.
4	Branch Reference Number*	CHAR	7	18	24	BSR code of the Bank Branch
5	Account Number*	CHAR	20	25	44	Bank account number
6	Name of first/sole account holder	CHAR	80	45	124	Field + filler spaces = 80
7	Type of Account*	CHAR	1	125	125	“A”- Savings Account “B”- Current Account “C”- Cash Credit Account “Z”- Other
8	Type of Account Holder*	CHAR	1	126	126	“A”- Individual “B”-Legal Person /Entity excluding “C” and “D” “C”- Central/ State Government “D”- Central/ State Government owned undertaking “Z”- Other

Report SUSPICIOUS TRANSACTION REPORT	Reporting Agency BANKING COMPANY	Version 1.0
--	--	-----------------------

9	Date of Account opening*	DATE	8	127	134	Date in DDMMYYYY Format
10	Risk Category	CHAR	1	135	135	Risk Category as per the Internal Risk Assessment System of the Bank “A”- Low Risk “B”- Medium Risk “C”- High Risk
11	Cumulative Credit Turnover*	NUM	20	136	155	Sum of all credits in the Bank account from 1 st April of the financial year till the last day of the month of reporting. If report is being furnished for Jan 2006 then transactions from 1 st April 2005 to 31 st Jan 2006 have to be aggregated. The amount should be rounded off to nearest rupee without decimal.
12	Cumulative Debit Turnover*	NUM	20	156	175	Sum of all debits in the Bank account from 1 st April of the financial year till the last day of the month of reporting. The amount should be rounded off to nearest rupee without decimal.
13	Cumulative Cash Deposit Turnover*	NUM	20	176	195	Sum of cash deposits in the Bank account from 1 st April of the financial year till the last day of the month of reporting. The amount should be rounded off to nearest rupee without decimal.
14	Cumulative Cash Withdrawal Turnover*	NUM	20	196	215	Sum of cash withdrawals in the Bank account from 1 st April of the financial year till the last day of the month of reporting. The amount should be rounded off to nearest rupee without decimal.

17. Data Structure of Transaction Data File (SBATR.txt)

	Field	Type	Size	From	To	Remarks
1	Record Type*	CHAR	3	1	3	Value should be “TRN” signifying Transaction data file
2	Line Number*	NUM	6	4	9	Running Sequence Number for each line in the file starting from 000001. This Number will be used during validation

Report SUSPICIOUS TRANSACTION REPORT	Reporting Agency BANKING COMPANY	Version 1.0
--	--	-----------------------

						checks.
3	Branch Reference Number*	CHAR	7	10	16	BSR code of the Bank Branch
4	Account Number*	CHAR	20	17	36	Bank account number
5	Transaction ID	CHAR	20	37	56	Unique ID to identify transaction (if available)
6	Date of Transaction*	DATE	8	57	64	Date in DDMMYYYY Format
7	Mode of Transaction*	CHAR	1	65	65	“A”- Cheque “B”- Transfer within Branch “C”- Cash “D”-Demand Draft “E”- Electronic Fund Transfer “F”-Travelers Cheque “Z”- Others
8	Debit/Credit*	CHAR	1	66	66	“D” – Debit (Withdrawal by customer) “C”– Credit (Deposit by customer)
9	Amount*	NUM	20	67	86	The amount should be rounded off to nearest rupee without decimal. If this amount was not in Indian Rupees, it should be converted into Indian rupees.
10	Currency of Transaction*	CHAR	3	87	89	“INR” for Indian Rupees, Mention Currency code as per SWIFT Code
11	Disposition of Funds	CHAR	1	90	90	Reserved for later use. Use Value “X”
12	Remarks	CHAR	10	91	100	Mention any other information related to the transaction.

18. Data Structure of Individual Data File (SBAINP.txt)

	Field	Type	Size	From	To	Remarks
1	Record Type*	CHAR	3	1	3	Value should be “INP” signifying Individual data file
2	Date of Report	DATE	8	4	11	Date of sending report in DDMMYYYY Format. This date should be same as in control file
3	Line Number*	NUM	6	12	17	Running Sequence Number for each line in the file starting from 000001. This Number will be used during validation checks.
4	Branch Reference Number*	CHAR	7	18	24	BSR code of the Bank Branch

Report SUSPICIOUS TRANSACTION REPORT	Reporting Agency BANKING COMPANY	Version 1.0
--	--	-----------------------

5	Account Number*	CHAR	20	25	44	Bank account number
6	Relation Flag*	CHAR	1	45	45	“A”- Account Holder “B”- Authorised Signatory “C”- Director/ Partner/Member etc. of a Legal Person /Entity “D”- Introducer “E”- Guarantor “Z” - Other
7	Full name of Individual*	CHAR	80	46	125	Full Name Field + filler spaces = 80
8	Customer ID/Number	CHAR	10	126	135	Customer ID/Number in the bank if it has been allotted
9	Name of Father/Spouse	CHAR	80	136	215	Full Name of Father/Spouse Field + filler spaces = 80
10	Occupation	CHAR	50	216	265	Where Applicable
11	Date of Birth	DATE	8	266	273	In DDMMYYYY format
12	Sex	CHAR	1	274	274	“M”- Male “F”- Female
13	Nationality	CHAR	2	275	276	Country code as per SWIFT
14	Type of Identification	CHAR	1	277	277	“A” –Passport “B”- Election ID Card “C”- PAN Card “D”- ID Card “E”- Driving License “F”- Account Introducer “Z” - Other
15	Identification Number	CHAR	10	278	287	Number mentioned in the identification document
16	Issuing Authority	CHAR	20	288	307	Authority which had issued the identification document
17	Place of Issue	CHAR	20	308	327	Place where document was issued
18	PAN	CHAR	10	328	337	Ten Digit PAN used by Income Tax Department
19	Communication Address 1*	CHAR	45	338	382	Field + filler spaces = 45
20	Communication Address 2	CHAR	45	383	427	Field + filler spaces = 45
21	Communication Address 3	CHAR	45	428	472	Field + filler spaces = 45
22	Communication Address 4	CHAR	45	473	517	Field + filler spaces = 45
23	Communication Address 5	CHAR	45	518	562	Field + filler spaces = 45
24	Communication Address Pin code*	NUM	6	563	568	Pin code without “-” or space
25	Contact Telephone	CHAR	30	569	598	Telephone number in format STD Code-Telephone number
26	Contact Mobile number	CHAR	30	599	628	Mobile number
27	Contact E-mail	CHAR	50	629	678	E-mail address
28	Place of Work	CHAR	80	679	758	Name of Organisation/ employer
29	Second Address 1	CHAR	45	759	803	Permanent address / Place of work (if other than

Report SUSPICIOUS TRANSACTION REPORT	Reporting Agency BANKING COMPANY	Version 1.0
--	--	-----------------------

						communication address)
30	Second Address 2	CHAR	45	804	848	Field + filler spaces = 45
31	Second Address 3	CHAR	45	849	893	Field + filler spaces = 45
32	Second Address 4	CHAR	45	894	938	Field + filler spaces = 45
33	Second Address 5	CHAR	45	939	983	Field + filler spaces = 45
34	Second Address Pin code	NUM	6	984	989	Pin code without “-” or space
35	Second Telephone	CHAR	30	990	1019	Telephone number in format STD Code-Telephone number

19. Data Structure of Legal Person/Entity Data File (SBALPE.txt)

	Field	Type	Size	From	To	Remarks
1	Record Type*	CHAR	3	1	3	Value should be “LPE” signifying Legal Persons/ Entity data file
2	Date of Report	DATE	8	4	11	Date of sending report in DDMMYYYY Format. This date should be same as in control file
3	Line Number*	NUM	6	12	17	Running Sequence Number for each line in the file starting from 000001. This Number will be used during validation checks.
4	Branch Reference Number*	CHAR	7	18	24	BSR code of the Bank Branch
5	Account Number*	CHAR	20	25	44	Bank account number
6	Relation Flag*	CHAR	1	45	45	“A”- Account Holder “D”- Introducer “E”- Guarantor “Z”- Other
7	Name of Legal Person /Entity*	CHAR	80	46	125	Full Name Field + filler spaces = 80
8	Customer ID/Number	CHAR	10	126	135	Customer ID/Number in the bank if allotted
9	Nature of Business	CHAR	50	136	185	Where Applicable
10	Date of Incorporation	DATE	8	186	193	In DDMMYYYY format
11	Type of Constitution*	CHAR	1	194	194	“A”- Sole Proprietorship “B”- Firm “C”- HUF “D”- Private Ltd. Company “E”- Public Ltd. Company “F”- Society “G”- Association “H”- Trust “I”- Liquidator “Z”- Other
12	Registration Number	CHAR	20	195	214	Registration Number of mentioned in deed/document

Report SUSPICIOUS TRANSACTION REPORT	Reporting Agency BANKING COMPANY	Version 1.0
--	--	-----------------------

13	Registering authority	CHAR	20	215	234	Authority Registering deed/document
14	Place of Registration	CHAR	20	235	254	Place where the document was registered
15	PAN	CHAR	10	255	264	Ten Digit PAN used by Income Tax Department
16	Communication Address 1*	CHAR	45	265	309	Field + filler spaces = 45
17	Communication Address 2	CHAR	45	310	354	Field + filler spaces = 45
18	Communication Address 3	CHAR	45	355	399	Field + filler spaces = 45
19	Communication Address 4	CHAR	45	400	444	Field + filler spaces = 45
20	Communication Address 5	CHAR	45	445	489	Field + filler spaces = 45
21	Communication Address Pin code*	NUM	6	490	495	Pin code without “-” or space
22	Contact Telephone	CHAR	30	496	525	Telephone number in format STD Code-Telephone number
23	Contact Fax	CHAR	30	526	555	Fax number in format STD Code-Telephone number
24	Contact Email	CHAR	50	556	605	E-mail address
25	Second Address 1	CHAR	45	606	650	Registered address (if different from above).
26	Second Address 2	CHAR	45	651	695	Field + filler spaces = 45
27	Second Address 3	CHAR	45	696	740	Field + filler spaces = 45
28	Second Address 4	CHAR	45	741	785	Field + filler spaces = 45
29	Second Address 5	CHAR	45	786	830	Field + filler spaces = 45
30	Second Address Pin code	NUM	6	831	836	Pin code without “-” or space
31	Second Telephone	CHAR	30	837	866	Telephone number in format STD Code-Telephone number
32	Second Fax	CHAR	30	867	896	Fax number in format STD Code-Telephone number

COUNTERFEIT CURRENCY REPORT (CCR)

Kindly fill in CAPITAL. Read the instructions before filling the form.

PART 1 DETAILS OF REPORTING BRANCH/LOCATION

1.1 Name of Entity	<input type="text"/>		
1.2 Name of Branch	<input type="text"/>		
1.3 Branch Reference Number	<input type="text"/>	1.4 ID allotted by FIU-IND	<input type="text"/>
1.5 Address (No., Building)	<input type="text"/>		
1.6 Street/Road	<input type="text"/>		
1.7 Locality	<input type="text"/>		
1.8 City/Town, District	<input type="text"/>		
1.9 State, Country	<input type="text"/>		
1.10 Pin code	<input type="text"/>	1.11 Tel (with STD code)	<input type="text"/>
1.12 Fax	<input type="text"/>	1.13 E-mail	<input type="text"/>

PART 2 DETAILS OF COUNTERFEIT CURRENCY

	Denomination	Number of pieces	Value
2.1	1000	<input type="text"/>	<input type="text"/>
2.2	500	<input type="text"/>	<input type="text"/>
2.3	100	<input type="text"/>	<input type="text"/>
2.4	50	<input type="text"/>	<input type="text"/>
2.5	20	<input type="text"/>	<input type="text"/>
2.6	10	<input type="text"/>	<input type="text"/>
2.7	5	<input type="text"/>	<input type="text"/>
2.8 Total Value of Counterfeit Currency		<input type="text"/>	

PART 3 DETAILS OF DETECTION

3.1 Date of Cash Tendering	<input type="text"/>	3.2 Total Cash Deposited	<input type="text"/>
3.3 Date of Detection	<input type="text"/>		
3.4 Detected at	<input type="checkbox"/> A Cash Counter <input type="checkbox"/> B Branch Level <input type="checkbox"/> C Currency Chest <input type="checkbox"/> D RBI's CVPS <input type="checkbox"/> Z Other		
3.5 Whether local police station has been informed	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
3.6 Details of FIR (if available)	<input type="text"/>		
3.7 Additional Information, if any	<input type="text"/>		

PART 4 DETAILS OF RELATED PERSONS

4.1 Name of Tendering Person	<input type="text"/>		
4.2 Name of Account Holder	<input type="text"/>		
4.3 Account / Card No.	<input type="text"/>		
	Signature	<input type="text"/>	
	Name	<input type="text"/>	
	Designation	<input type="text"/>	

DO NOT FILL. FOR FIU-IND USE ONLY.

CCR

COUNTERFEIT CURRENCY REPORT (CCR) INSTRUCTIONS

GENERAL INSTRUCTIONS

Under the Prevention of Money Laundering Act 2002 (PMLA), every reporting entity is required to furnish details of all cash transactions where forged or counterfeit currency notes of bank notes have been used as genuine. These transactions should be reported to Director, Financial Intelligence Unit, India not later than seven working days from the date of occurrence of such transactions.

HOW TO SUBMIT

Every reporting entity branch must submit this form to the Director, FIU- IND only through the principal officer designated under PMLA.

Note: A separate Counterfeit Currency Report (CCR) should be filed for each incident of detection of counterfeit Indian currency. If the detected counterfeit currency notes can be segregated on the basis of tendering person, a separate CCR should be filed for each such incident.

EXPLANATION OF SPECIFIC TERMS

PART 1: DETAILS OF REPORTING BRANCH / LOCATION

This section contains details of the branch/location where the counterfeit currency was detected.

- 1.1 Mention name of the reporting entity (bank, financial institution).
- 1.2 Mention name of the reporting branch/location.
- 1.3 Mention any unique number issued by the regulator or any temporary code to uniquely identify each branch/ location.
- 1.4 ID allotted by FIU-IND may be left blank till the same is communicated by FIU-IND.
- 1.10 Pincode should be a valid 6 digit numeric pincode of the branch/location.

PART 2: DETAILS OF COUNTERFEIT CURRENCY

This section contains the details of counterfeit currency. Total value of counterfeit currency should match with the total calculated value of Denomination x Number of pieces.

PART 3: DETAILS OF DETECTION

- 3.1 Mention the date on which cash was tendered, if available. Date should be reported in YYYYMMDD format. E.g. 2nd May, 2007 should be entered as 20070502.
- 3.2 Mention the total cash tendered by the tenderer including counterfeit currency, if available.
- 3.3 Mention the date on which counterfeit currency was detected in YYYYMMDD format. E.g. 2nd May 2007 should be entered as 20070502.
- 3.4 Select from the following counterfeit currency detection stages
 - "A"- Cash Counter by the teller
 - "B"- Branch Level during sorting
 - "C"- Currency Chest while counting
 - "D"- Currency Verification and Processing System at RBI
 - "Z"- Other

3.5 Mention Yes, if local police station has been informed.

3.6 Mention details of FIR, police station etc., if available.

3.7 Mention additional information such as quality of counterfeit currency, sequence of events, if available.

PART 4: DETAILS OF RELATED PERSONS

- 4.1 Person who tendered the counterfeit currency, if available.
- 4.2 Name of the sole/first account holder in whose account counterfeit currency was tendered, if available.
- 4.3 Account/Card Number of the person in whose account the counterfeit currency was tendered, if available.

The form should be signed by an officer at the branch/controlling office/head office.

SUMMARY OF COUNTERFEIT CURRENCY REPORTS

Kindly fill in CAPITAL. Read the instructions before filling the form.

PART 1 DETAILS OF THE PRINCIPAL OFFICER

1.1 Name of Reporting Entity	<input type="text"/>		
1.2 Branch Reference Number	<input type="text"/>	1.3 ID allotted by FIU-IND	<input type="text"/>
1.4 Category of Entity	<input type="text"/>	<i>(Refer to Instructions)</i>	
1.5 Name of Principal Officer	<input type="text"/>		
1.6 Designation	<input type="text"/>		
1.7 Address (No., Building)	<input type="text"/>		
1.8 Street/Road	<input type="text"/>		
1.9 Locality	<input type="text"/>		
1.10 City/Town, District	<input type="text"/>		
1.11 State, Country	<input type="text"/>		
1.12 Pin code	<input type="text"/>	1.13 Tel (with STD code)	<input type="text"/>
1.14 Fax	<input type="text"/>	1.15 E-mail	<input type="text"/>

PART 2 STATISTICS

2.1 Number of Counterfeit Currency Reports enclosed	<input type="text"/>
2.2 Total Value of Counterfeit Currency	<input type="text"/>

DO NOT FILL. FOR FIU-IND USE ONLY

ACK. NO.

DATE 2 0 0

D D M M Y Y Y Y

Signature

Name

(Should be same as the person mentioned in PART 1)

Date

SUMMARY OF COUNTERFEIT CURRENCY REPORTS (CCRs)

INSTRUCTIONS

GENERAL INSTRUCTIONS

Under the Prevention of Money Laundering Act 2002 (PMLA), every reporting entity (bank, financial institution, intermediary) is required to furnish details of all cash transactions where forged or counterfeit currency notes of bank notes have been used as genuine. These transactions should be reported to Director, Financial Intelligence Unit, India not later than seven working days from the date of occurrence of such transactions.

One CCR should be submitted for each incident of detection of counterfeit Indian currency. If the counterfeit currency detected can be segregated on the basis of tendering person, a separate CCR should be filed for each such incident.

How to submit

The principal officer should submit this summary alongwith CCRs received from branches /locations to the Director, FIU-IND.

Address Director, FIU-IND
Financial Intelligence Unit-India
6th Floor, Hotel Samrat
Chanakyapuri, New Delhi -110021
India

EXPLANATION OF SPECIFIC TERMS

PART 1: DETAILS OF THE PRINCIPAL OFFICER

1.3. ID allotted by FIU-IND may be left blank till the same is communicated by FIU-IND.

1.4. Category of the reporting entity

"A"-Public Sector Bank

"B"-Private Sector Bank

"C"-Foreign Bank

"D"-Co-operative Bank

"E"-Regional Rural Bank

"F"-Local Area Bank

"Z"-Other

1.5. Principal officer is the officer designated under PMLA.

PART 2: STATISTICS

2.1. Number of Counterfeit Currency Reports enclosed.

2.2. Total Value of counterfeit currency detected in the enclosed reports. (Sum of value is in 2.8 of each CCR).

ALL CCRs MUST BE ENCLOSED.

ELECTRONIC FILE STRUCTURE

Report | **COUNTERFEIT CURRENCY REPORT**
Version | **1.0**

Contents

1.	Introduction.....	1
2.	Counterfeit Currency Report	1
3.	Due Date	1
4.	Methods of filing	1
5.	Manual format	1
6.	Electronic format	2
7.	Description of Data Files	2
8.	Steps in preparation of data files	2
9.	Steps in validation /sufficiency of data files.....	2
10.	General Notes for all Data Files	3
11.	Data Structure of Control File (CCRCTL.txt).....	3
12.	Data Structure of Branch File (CCRBRC.txt)	5
13.	Data Structure of Transaction File (CCRTRN.txt).....	6

Appendix

Counterfeit Currency Report
Summary of Counterfeit Currency Report

Report COUNTERFEIT CURRENCY REPORT	Version 1.0
---------------------------------------	----------------

1. Introduction

The Prevention of Money Laundering Act, 2002 (PMLA) forms the core of the legal framework put in place by India to combat money laundering. PMLA and the Rules notified thereunder came into force with effect from July 1, 2005. Director, FIU-IND and Director (Enforcement) have been conferred with exclusive and concurrent powers under relevant Sections of the Act to implement the provisions of the Act.

2. Counterfeit Currency Report

The PMLA and Rules notified thereunder impose an obligation on banks, financial institutions and intermediaries of the securities market (reporting entity) to furnish details of all cash transactions where forged or counterfeit currency notes of bank notes have been used as genuine to the Director, FIU-IND.

A separate Counterfeit Currency Report (CCR) should be filed for each incident of detection of counterfeit Indian currency. If the detected counterfeit currency notes can be segregated on the basis of tendering person, a separate CCR should be filed for each such incident.

3. Due Date

These transactions should be reported to Director, Financial Intelligence Unit, India not later than seven working days from the date of occurrence of such transactions.

4. Methods of filing

The CCR should be submitted to the Financial Intelligence Unit – India (FIU-IND) at the following address:

Director, FIU-IND
 Financial Intelligence Unit-India
 6th Floor, Hotel Samrat
 Chanakyapuri, New Delhi -110021, India
 (Visit <http://fiuindia.gov.in> for more details)

Counterfeit Currency Reports can be filed either in manual or electronic format. However, the reporting entity must submit all reports to FIU-IND in electronic format if it has the technical capability to do so.

For reporting entities, which do not have technical capacity to generate report in electronic form, a report preparation utility for preparation of electronic Counterfeit Currency Report (CCRRPU.xls) can be downloaded from the website of the FIU-IND at <http://fiuindia.gov.in>

5. Manual format

Counterfeit Currency Reports in manual format consists of following forms:

Form	Information	Completed by
Summary of Counterfeit Currency Reports	Contains summary of enclosed CCRs	Principal officer of the reporting entity
Counterfeit Currency Report	Details of branch and counterfeit currency.	Reporting branch/office

The above forms are given in the Appendix.

Report COUNTERFEIT CURRENCY REPORT	Version 1.0
---------------------------------------	----------------

6. Electronic format

FIU-IND is in the process of developing technological infrastructure to enable submission of electronic return over a secure gateway. In the interim, the reporting entities should submit the following to Director, FIU-IND:

- i) One CD containing three data files in prescribed data structure. A label mentioning name of the reporting entity, Unique code, type of report (CCR), report dated should be affixed on each CD for the purpose of identification.
- ii) Each CD should be accompanied by Summary of Counterfeit Currency Report for Reporting entity (same form should be used for both manual as well as electronic format) in physical form duly signed by the principal officer. This summary should match with the data in Control File (CCRCTL.txt).

Important:

- i) In case the size of data files exceeds the capacity of one CD, the data files should be compressed by using Winzip 8.1 or ZipItFast 3.0 (or higher version) compression utility only to ensure quick and smooth acceptance of the file.
- ii) The CD should be virus free.

7. Description of Data Files

In case of electronic filing, the consolidated CCR data should have following three data files:

S No.	Filename	Description
1	CCRCTL.txt	Control File
2	CCRBRC.txt	Branch File
3	CCRTRN.txt	Transaction File

8. Steps in preparation of data files

- i) The details of counterfeit currency should be captured in the Transaction File (CCRTRN.txt).
- ii) The details of branches should be captured in the Branch File (CCRBRC.txt).
- iii) The report level details and summary should be captured in the Control file. (CCRCTL.txt)

9. Steps in validation /sufficiency of data files

- i) There should be three data files with appropriate naming convention.
- ii) The data files should be as per specified data structure and business rules.
- iii) None of the mandatory fields should be left blank.
- iv) All dates should be entered in YYYYMMDD format.
- v) The summary figures in control file should match with the totals in other data files.
- vi) [Branch Reference Number] should be unique in Branch Data File (CCRBRC.txt)

Report COUNTERFEIT CURRENCY REPORT	Version 1.0
---------------------------------------	----------------

- vii) All values of [Branch Reference Number] in Transaction Data File (CCRTRN.txt) should have matching [Branch Reference Number] value in Branch Data File (CCRBRC.txt)

10. General notes for all Data Files

- i) All Data Files should be generated in ASCII Format with ".txt" as filename extension.
- ii) Each Record (including last record) must start on new line and must end with a newline character. Hex Values: "0D" & "0A".
- iii) All CHAR fields must be left justified.
- iv) If CHAR field has no data or less data with respect to defined length, then the entire field (in case of no data) or the remaining field (in case of less data) has to be filled with right justified blank characters (Spaces).
- v) All NUM fields must be right justified.
- vi) If NUM field has no data or less data with respect to defined length, then the entire field (in case of no data) or the remaining field (in case of less data) has to be filled with left justified zeroes.
- vii) If DATE field has no data then the entire field has to be filled with blank characters (Spaces).
- viii) Fields with an asterisk (*) have to be compulsorily filled up.
- ix) For fields that do not have an asterisk (*), reasonable efforts have to be made to get the information. Enter "N/A" to indicate that the field is not applicable. Do not substitute any other abbreviations or special characters (e.g., "x", "-" or "*").

11. Data structure of Control File (CCRCTL.txt)

S. No.	Field	Type	Size	From	To	Remarks
1.	Report Name*	CHAR	3	1	3	Value should be "CCR" signifying Counterfeit Currency Report
2.	Serial Number of Report*	NUM	8	4	11	Indicates the running sequence number of CCR for the reporting entity starting from 1
3.	Record Type*	CHAR	3	12	14	Value should be "CTL" signifying Control file
4.	Report Date*	NUM	8	15	22	Date of sending report to FIU-IND in YYYYMMDD format
5.	Reporting Entity Name*	CHAR	80	23	102	Complete name of the reporting entity (Bank, financial institution, intermediary)
6.	Reporting Entity Category*	CHAR	1	103	103	"A"-Public Sector Bank "B"-Private Sector Bank "C"-Foreign Bank "D"-Co-operative Bank "E"-Regional Rural Bank

Report COUNTERFEIT CURRENCY REPORT	Version 1.0
---------------------------------------	----------------

						“F”-Local Area Bank “Z”-Other
7.	Unique code of the Reporting Entity*	CHAR	12	104	115	Unique code issued by the regulator, if applicable
8.	Unique ID issued by FIU*	CHAR	10	116	125	Use XXXXXXXXXXXX till the ID is communicated
9.	Principal Officer’s Name*	CHAR	80	126	205	Field + filler spaces = 80
10.	Principal Officer’s Designation*	CHAR	80	206	285	Field + filler spaces = 80
11.	Principal Officer’s Address1*	CHAR	45	286	330	No., Building Field + filler spaces = 45
12.	Principal Officer’s Address2	CHAR	45	331	375	Street/Road Field + filler spaces = 45
13.	Principal Officer’s Address3	CHAR	45	376	420	Locality Field + filler spaces = 45
14.	Principal Officer’s Address4	CHAR	45	421	465	City/Town, District Field + filler spaces = 45
15.	Principal Officer’s Address5	CHAR	45	466	510	State, Country Field + filler spaces = 45
16.	Principal Officer’s Pin code*	NUM	6	511	516	Pin code without “-” or space
17.	Principal Officer’s Telephone	CHAR	30	517	546	Telephone in format STD Code-Telephone number
18.	Principal Officer’s FAX	CHAR	30	547	576	Fax number in format STD Code-Telephone number
19.	Principal Officer’s E-mail	CHAR	50	577	626	E-mail address
20.	Report Type*	CHAR	1	627	627	“N”- New Report “R”- Replacement to earlier submitted report
21.	Reason for Replacement*	CHAR	1	628	628	“A” – Acknowledgement of Original Report had many warnings or error messages. “B” – Operational error, data omitted in Original Report. “C” – Operational error, wrong data submitted in Original Report. “N”- Not Applicable as this is a new report “Z”- Other Reason
22.	Serial Number of Original Report *	NUM	8	629	636	Serial Number of the Original Report which is being replaced. Mention 0 if Report Type is “N”
23.	Operational Mode*	CHAR	1	637	637	“P”- Actual/ Production mode “T”- Test / Trial mode
24.	Data Structure Version*	CHAR	1	638	638	Value should be 1 to indicate Version 1.0
25.	Number of Counterfeit	NUM	8	639	646	Number of CCRs enclosed in

	Currency Reports*					this summary. This figure should match with the number of records in CCRTRN.txt
26.	Total Value of Counterfeit Currency*	NUM	12	647	658	Total Value of Counterfeit Currency reported in enclosed CCRs. This figure should match with the sum of the Field Total Counterfeit Currency (S. No. 11) in CCRTRN.txt

12. Data structure of Branch File (CCRBRC.txt)

S. No.	Field	Type	Size	From	To	Remarks
1.	Record Type	CHAR	3	1	3	Value should be "BRC" signifying Control file
2.	Line Number*	NUM	6	4	9	Running Sequence Number for each line in the file starting from 1. This Number will be used during validation checks.
3.	Name of Branch*	CHAR	80	10	89	Name of branch/location where the counterfeit currency was tendered Field + filler spaces = 80
4.	Branch Reference Number*	CHAR	12	90	101	Unique Code issued by the regulator or any temporary code to uniquely identify each branch/office
5.	Unique ID issued by FIU*	CHAR	10	102	111	Use XXXXXXXXXXXX till the ID is communicated
6.	Branch Address1*	CHAR	45	112	156	No., Building Field + filler spaces = 45
7.	Branch Address2*	CHAR	45	157	201	Street/Road Field + filler spaces = 45
8.	Branch Address3	CHAR	45	202	246	Locality Field + filler spaces = 45
9.	Branch Address4	CHAR	45	247	291	City/Town, District Field + filler spaces = 45
10.	Branch Address5	CHAR	45	292	336	State, Country Field + filler spaces = 45
11.	Branch Pin code*	NUM	6	337	342	Pin code without "-" or space
12.	Branch Telephone	CHAR	30	343	372	Telephone number in format STD Code-Telephone number
13.	Branch Fax	CHAR	30	373	402	Fax number in format STD Code-Telephone number
14.	Branch E-mail	CHAR	50	403	452	E-mail address

13. Data structure of Transaction File (CCRTRN.txt)

S. No.	Field	Type	Size	From	To	Remarks
1.	Record Type*	CHAR	3	1	3	Value should be "TRN" signifying Transaction data file
2.	Line Number*	NUM	6	4	9	Running Sequence Number for each line in the file starting from 1. This Number will be used during validation checks.
3.	Branch Reference Number*	CHAR	12	10	21	Branch Reference Number of branch/location where counterfeit currency was tendered. Use any unique number issued by the regulator or any temporary code to uniquely identify each branch/location
4.	Denomination1000	NUM	10	22	31	Number of counterfeit currency notes of Rs. 1000/- each
5.	Denomination500	NUM	10	32	41	Number of counterfeit currency notes of Rs. 500/- each
6.	Denomination100	NUM	10	42	51	Number of counterfeit currency notes of Rs. 100/- each
7.	Denomination50	NUM	10	52	61	Number of counterfeit currency notes of Rs. 50/- each
8.	Denomination20	NUM	10	62	71	Number of counterfeit currency notes of Rs. 20/- each
9.	Denomination10	NUM	10	72	81	Number of counterfeit currency notes of Rs. 10/- each
10.	Denomination5	NUM	10	82	91	Number of counterfeit currency notes of Rs. 5/- each
11.	Total Counterfeit Currency	NUM	10	92	101	Value of counterfeit currency detected. This value should match with the value derived from the number of notes mentioned in S. No. 4 to 10 above.
12.	Tendering Date	NUM	8	102	109	Date of tendering counterfeit currency in YYYYMMDD format, if available. E.g.: 2 nd May 2007 should be written as 20070502
13.	Total Cash Tendered	NUM	20	110	129	Total Cash tendered by the tenderer including the counterfeit currency, if available
14.	Detection Date*	NUM	8	130	137	In YYYYMMDD format E.g.: 2 nd May 2007 should be written as 20070502

15.	Detected At*	CHAR	1	138	138	“A”- Cash Counter “B”- Branch Level “C”- Currency Chest “D”- RBI’s CVPS “Z”- Other
16.	Police Informed	CHAR	1	139	139	Y – for Yes, N – for No
17.	FIR Detail	CHAR	80	140	219	FIR, Police Station details etc., if available
18.	Additional Information	CHAR	80	220	299	Additional Information such as quality of counterfeit currency, sequence of events, if available
19.	Name of Tendering Person	CHAR	80	300	379	Person who tendered the counterfeit currency, if available.
20.	Name of Account Holder	CHAR	80	380	459	Name of the Sole/First account holder in whose account the counterfeit currency was tendered, if available.
21.	Account Number	CHAR	20	460	479	Account/Card Number of the person in whose account the counterfeit currency was tendered, if available.