RBI/2007-2008/381
RPCD.CO.RF.AML.BC.No.81/07.40.00/2007-08

June 25, 2008

The Chief Executives of
All State and Central Co-operative Banks

Dear Sir,

Prevention of Money Laundering Act, 2002 -
Obligation of Banks in Terms of Rules Notified there under

Please refer to our circular RPCD.CO.RF.AML.BC.65/07.02.12/2005-06 dated March 3, 2006. In Paragraph 3 of the said circular, it was advised that banks are required to maintain and preserve information in respect of transactions **with its client referred to in Rule 3** in hard and soft copies. It is further clarified that banks should also report information in respect of all transactions referred to in **Rule 3, ibid** to the Director, Financial Intelligence Unit-India (FIU-IND).

2. In terms of instructions contained in paragraph 2 of the guidelines on 'Know Your Customer Norms' and 'Anti-Money Laundering Measures' of our circular dated February 18, 2005, banks are required to prepare a profile for each customer based on risk categorization. Further, vide paragraph 4 of our circular dated February 28, 2008, the need for periodical review of risk categorization 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.

3. In paragraph paragraph 6 of our circular dated March 3, 2006, referred to above, banks were advised to initiate urgent steps to ensure electronic filing of cash transaction report (CTR) and Suspicious Transaction Reports (STR) to FIU-IND. It has been reported by FIU-IND that many banks are yet to file electronic reports. It is, therefore, advised that in case of banks, where all the branches are not yet fully computerized, the Principal Officer of the bank should cull out the transaction details from branches which are not 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 on their website http://fiuindia.gov.in.

4. In paragraph 6(I)(a) of our circular dated March 3, 2006, referred to above, banks were advised to make Cash Transaction Reports (CTR) to FIU-India for every month latest by 15th of the succeeding month. It is further clarified that cash transaction reporting by branches to their Principal Officer should invariably be submitted on monthly basis **(not on fortnightly basis)** and the Principal Officer, in turn, should ensure to submit CTR for every month to FIU-IND within the prescribed time schedule.

5. In regard to CTR, it is reiterated that the cut-off limit of Rupees ten lakh is applicable to integrally connected cash transactions also. Further, after consultation with FIU-IND, it is clarified that:

a) For determining integrally connected cash transactions, banks should take into account all individual cash transactions **in an account during a calendar month**, where either debit or credit summation, computed separately, exceeds Rupees ten lakh during the month. However, while filing CTR, details of individual cash transactions below rupees fifty thousand may not be indicated. Illustration of integrally connected cash transactions is furnished in Annex-I to this circular.

b) 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.

c) 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 format (Counterfeit Currency Report - CCR) as per Annex-II & III. Electronic data structure has been furnished in Annex-IV to enable banks to generate electronic CCRs. 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.

6. In paragraph 4 of the Guidelines on KYC Norms / AML Measures annexed to our circular RPCD.AML.BC.No.80/07.40.00/2004-05 dated February 18, 2005, 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 / memoranda 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. These records are required to be preserved for ten years as is required under PMLA, 2002. Such records and related documents should be made available to help auditors in their work relating to scrutiny of transactions and also to Reserve Bank / other relevant authorities.

7. In paragraph 7 of our March 3, 2006 circular, banks have been advised that the customer should not be tipped off on the STRs made by them to FIU-IND. 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.

8. While making STRs, banks should be guided by the definition of 'suspicious transaction' as contained in Rule 2(g) of Rules ibid. It is further clarified that banks should make STRs if they have reasonable ground to believe that the transaction involves 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.

9. 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' (copy enclosed).

10. These guidelines are issued under Section 35A of the Banking Regulation Act, 1949 (As Applicable to Co-operative Societies) and Rules ibid. Any contravention of the said guidelines may attract penalties under the relevant provisions of the Act.

Yours faithfully,

(G. Srinivasan)
Chief General Manager-in-Charge

Annex – I

Illustration of Integrally Connected Cash Transaction

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**	

(i) 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 lakh. 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/-.

(ii) 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.

FIU-IND Financial Intelligence Unit- India

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

PART 2 DETAILS OF COUNTERFEIT CURRENCY

	Denomination	Number of pieces	Value
2.1	1000		
2.2			
2.3			
2.4			
2.5	20		
2.6	10		
2.7			
2.8	**Total Value of Counterfeit Currency**		

PART 3 DETAILS OF DETECTION

3.1 Date of Cash Tendering

3.2 Total Cash Deposited

3.3 Date of Detection

3.4 Detected at

A Cash Counter B Branch Level C Currency Chest

D RBI's CVPS Z Other

3.5 Whether local police station has been informed Yes No

3.6 Details of FIR (*if available*)

3.7 Additional Information, if any

PART 4 DETAILS OF RELATED PERSONS

4.1 Name of Tendering Person

4.2 Name of Account Holder

4.3 Account / Card No.

Signature

Name

Designation

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 counterfiet 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 renderer 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 currrency 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, polic station etc., if available.

3.7 Mention addtional 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 counterfiet 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.

ANNEX - III

FIU-IND Financial Intelligence Unit- India

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

PART 2 STATISTICS

2.1	Number of Counterfeit Currency Reports enclosed	
2.2	Total Value of Counterfeit Currency	

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

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

SUMMARY OF COUNTERFEIT CURRENCY REPORTS (CCRs)

INSTRUCTIONS

GENERAL INSTRUCTIONS

Under the Prevention of Money Laundering Act 2002 (PMLA), every reporting entity (bank, financial instituion, 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.

ANNEX - IV

ELECTRONIC DATA STRUCTURE

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

Contents

Appendix

Counterfeit Currency Report
Summary of Counterfeit Currency Report

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.

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)

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 “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 XXXXXXXXXX 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 Currency Reports*	NUM	8	639	646	Number of CCRs enclosed in 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 XXXXXXXXXX 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.: 2nd 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.: 2nd 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.

Annex E of the 'IBA's Guidance Note for Banks, 2005'

An Indicative List of Suspicious Activities

Transactions Involving Large Amounts of Cash

(i) Exchanging an unusually large amount of small denomination notes for those of higher denomination;

(ii) Purchasing or selling of foreign currencies in substantial amounts by cash settlement despite the customer having an account with the bank;

(iii) Frequent withdrawal of large amounts by means of cheques, including traveller's cheques;

(iv) Frequent withdrawal of large cash amounts that do not appear to be justified by the customer's business activity;

(v) Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received an unexpected large credit from abroad;

(vi) Company transactions, both deposits and withdrawals, that are denominated by unusually large amounts of cash, rather than by way of debits and credits normally associated with the normal commercial operations of the company, e.g. cheques, letters of credit, bills of exchange etc.;

(vii) Depositing cash by means of numerous credit slips by a customer such that the amount of each deposit is not substantial, but the total of which is substantial.

Transactions that do not make Economic Sense

(i) A customer having a large number of accounts with the same bank, with frequent transfers between different accounts;

(ii) Transactions in which assets are withdrawn immediately after being deposited, unless the customer's business activities furnish a plausible reason for immediate withdrawal.

Activities not consistent with the Customer's Business

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

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

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

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

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

Attempts to avoid Reporting/Record-keeping Requirements

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

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

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

Unusual Activities

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

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

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

Customer who provides Insufficient or Suspicious Information

(i) A customer/company who is reluctant to provide complete information regarding the purpose of the business, prior banking relationships, officers or directors, or its locations.

(ii) A customer/company who is reluctant to reveal details about its activities or to provide financial statements.

(iii) A customer who has no record of past or present employment but makes frequent large transactions.

Certain Suspicious Funds Transfer Activities

(i) Sending or receiving frequent or large volumes of remittances to/from countries outside India.

(ii) Receiving large TT/DD remittances from various centers and remitting the consolidated amount to a different account/center on the same day leaving minimum balance in the account.

(iii) Maintaining multiple accounts, transferring money among the accounts and using one account as a master account for wire/funds transfer.

Certain Bank Employees arousing Suspicion

(i) An employee whose lavish lifestyle cannot be supported by his or her salary.

(ii) Negligence of employees/willful blindness is reported repeatedly.

Some examples of suspicious activities/transactions to be monitored by the operating staff-

- Large Cash Transactions
- Multiple accounts under the same name
- Frequently converting large amounts of currency from small to large denomination notes
- Placing funds in term Deposits and using them as security for more loans
- Large deposits immediately followed by wire transfers
- Sudden surge in activity level
- Same funds being moved repeatedly among several accounts
- Multiple deposits of money orders, Banker's cheques, drafts of third parties
- Transactions inconsistent with the purpose of the account
- Maintaining a low or overdrawn balance with high activity

Check list for preventing money-laundering activities:

- A customer maintains multiple accounts, transfer money among the accounts and uses one account as a master account from which wire/funds transfer originates or into which wire/funds transfer are received (a customer deposits funds in several accounts, usually in amounts below a specified threshold and the funds are then consolidated into one master account and wired outside the country).
- A customer regularly depositing or withdrawing large amounts by a wire transfer to, from, or through countries that are known sources of narcotics or where Bank secrecy laws facilitate laundering money.
- A customer sends and receives wire transfers (from financial haven countries) particularly if there is no apparent business reason for such transfers and is not consistent with the customer's business or history.
- A customer receiving many small incoming wire transfer of funds or deposits of cheques and money orders, then orders large outgoing wire transfers to another city or country.
- A customer experiences increased wire activity when previously there has been no regular wire activity.
- Loan proceeds unexpectedly are wired or mailed to an offshore Bank or third party.

- A business customer uses or evidences or sudden increase in wired transfer to send and receive large amounts of money, internationally and/ or domestically and such transfers are not consistent with the customer's history.
- Deposits of currency or monetary instruments into the account of a domestic trade or business, which in turn are quickly wire transferred abroad or moved among other accounts for no particular business purpose.
- Sending or receiving frequent or large volumes of wire transfers to and from offshore institutions.
- Instructing the Bank to transfer funds abroad and to expect an equal incoming wire transfer from other sources.
- Wiring cash or proceeds of a cash deposit to another country without changing the form of the currency

- Receiving wire transfers and immediately purchasing monetary instruments prepared for payment to a third party.
- Periodic wire transfers from a person's account/s to Bank haven countries.
- A customer pays for a large (international or domestic) wire transfers using multiple monetary instruments drawn on several financial institutions.
- A customer or a non-customer receives incoming or makes outgoing wire transfers involving currency amounts just below a specified threshold, or that involve numerous Bank or travelers cheques
- A customer or a non customer receives incoming wire transfers from the Bank to 'Pay upon proper identification' or to convert the funds to bankers' cheques and mail them to the customer or non-customer, when
  - The amount is very large (say over Rs.10lakhs)
  - The amount is just under a specified threshold (to be decided by the Bank based on local regulations, if any)
  - The funds come from a foreign country or
  - Such transactions occur repeatedly.

- A customer or a non-customer arranges large wire transfers out of the country which are paid for by multiple Bankers' cheques (just under a specified threshold)

A Non-customer sends numerous wire transfers using currency amounts just below a specified threshold limit.