UTTAR BIHAR GRAMIN BANK

Head Office, Muzaffarpur

Fraud Risk Management Policy

(Amended upto Jan 2021)

Annexure

"Frauds - Guidelines for Classification, Reporting and Monitoring of Frauds"

"Frauds - Guidelines for Classification, Reporting and Monitoring of Frauds"

1. PREAMBLE

Banks by virtue of the nature of activities undertaken and its operating environment are vulnerable to frauds, which take place when aggressive business strategy and process for quick growth is adopted without adequate/appropriate internal controls or non-adhering of operating standards/controls. In the recent past, incidence of frauds in the Banking industry has increased which calls for concerted steps in investigating the frauds and identifying the fraudsters for eventual criminal prosecution and internal punitive action.

As fraudsters resort to careful planning before striking at the system of its most vulnerable points, bank has to continuously strengthen its operational practices, procedures, controls and review mechanism so that fraud-prone areas are sanitized against both internal and external frauds. The advent of computerization and services offered to customers over different platforms
/ channels by the Bank has added new dimensions to frauds and the potential of frauds being committed has increased.

Therefore, Bank should recognize that, frauds are major operational risks and acknowledges the concerns of RBI by way of well-developed Fraud Risk Management Policy to address the issues of fraud prevention / investigation and monitoring.

2. SCOPE AND PURPOSE

The purpose of this policy is to create a proactive framework addressing the occurrence of frauds in the banking system covering early detection, prevention, reporting, monitoring, recovery and follow-up of frauds as also to:

- Develop common understanding of Fraud Risk and facilitate its management,
- Have in place a suitable organization structure,
- Ensure that all the departments are aware of their responsibilities for identifying exposures to fraudulent activities and for establishing / improving the controls and procedures for preventing such fraudulent activity and/or detecting such fraudulent activity when it occurs,
- Provide guidance to staff as to the actions to be taken when they suspect any fraudulent activity,
- Provide assurance that any and all suspected fraudulent activity will be fully investigated.
- Develop and maintain a data bank of the frauds.

3.OBJECTIVE

The objective of the policy is to obviate fraud risks in the face of acceleration of Bank‟s business by strengthening internal controls to protect the brand, reputation and assets of the Bank from loss or damage resulting from suspected or confirmed incidents of fraud.

4. Introduction

4.1. Incidence of frauds, dacoities, robberies, etc., in banks is a matter of concern. While the primary responsibility for preventing frauds lies with banks themselves, the RBI /NABARD has been advising banks from time to time about the major fraud prone areas and the safeguards necessary for prevention of frauds. In the recent past, incidence of frauds in the Banking industry has increased which calls for concerted steps in investigating the frauds and identifying the fraudsters for eventual criminal prosecution and internal punitive action. Therefore, Bank should recognize that, frauds are major operational risks and acknowledges the concerns of RBI by way of well developed Fraud Risk Management Policy to address the issues of fraud prevention / investigation and monitoring.

5. Definition of fraud

5.1. As per the Indian Penal Code (IPC), a fraud is defined as:

"Any behaviour by which one person intends to gain a dishonest advantage over another"

RBI has defined fraud as an act of commission and / or abetment, which is intended to cause illicit gain to one person (s) / entity and wrongful loss to the other, either by way of concealment of facts, by deceit or by playing a confidence trick.

"Fraud" is a willful act intentionally committed by an individual(s) by deception, suppression, cheating or any other fraudulent or any other illegal means, thereby causing wrongful gain(s) to self or any other individual(s) and wrongful loss to other(s). Many a times such acts are undertaken with a view to deceive/mislead others leading them to do or prohibiting them from doing a bonafide act or take bonafide decision which is not based on material facts."

While fraudulent activity could have a very wide range of coverage, the following are some of the act(s) which constitute fraud.

a) Forgery or alteration of any document or account belonging to the Company

b) Forgery or alteration of cheque, bank draft or any other financial instrument etc.

c) Misappropriation of funds, securities, supplies or other assets by fraudulent means etc.

d) Falsifying records such as pay-rolls, removing the documents from files and /or replacing it by a fraudulent note etc.

e) Willful suppression of facts/deception in matters of appointment, placements, submission of reports, tender committee recommendations etc. as a result of which a wrongful gain(s) is made to one and wrongful loss(s) is caused to the others.

f) Utilizing Company funds for personal purposes.

g) Authorizing or receiving payments for goods not supplied or services not rendered. Recording wrongful quantities / measurement of work done, recording of false measurements, wrong classification of items with intent to favour the supplier/contractors/vendors.

h) Destruction, disposition, removal of records or any other assets of the Company with an ulterior motive to manipulate and misrepresent the facts so as to create suspicion / suppression /cheating as a result of which objective assessment/decision would not be arrived at.

i) Releasing of security and other deposits/EMD without having fulfilled conditions precedent to release of such deposits / guarantees as per contractual obligations, without approval of authority.

j) Misappropriation of amounts collected on behalf of the Company from farmers/vendors/public, etc.

k) Any other act that falls under the gamut of fraudulent activity.

6. Classification of Fraud

6.1. Frauds can be broadly categorized into external frauds and internal frauds. However, frauds in banks arising out of both system and human failures may be grouped into 4 categories on the basis of perpetrator of fraud.

a) Frauds committed by employees.
b) Frauds committed by employees in collusion with outsiders who may or may not be the customer of the bank.
c) Frauds committed by outsiders / customers with insider support / involvement.
d) Frauds committed exclusively by outsider who may or may not be the customer of the bank.

6.2. In order to have uniformity in reporting, frauds have been classified as under, based mainly on the provisions of the Indian Penal Code (IPC):

a) Misappropriation and criminal breach of trust.

b) Fraudulent encashment through forged instruments, manipulation of books of account or through fictitious accounts and conversion of property.

c) Unauthorised credit facilities extended for reward or for illegal gratification.

d) Negligence and cash shortages.

e) Cheating and forgery.

f) Irregularities in foreign exchange transactions.

g) Any other type of fraud not coming under the specific heads as above.

6.3. Cases of 'negligence and cash shortages' and irregularities in foreign exchange transactions referred to in item (d) & (f) above are to be reported as fraud if the intention to cheat / defraud is suspected / proved. However, in the following cases where fraudulent intention is not suspected / proved at the time of detection, will be treated as fraud and reported accordingly.

a) Cases of cash shortages more than ₹ 10,000 (including ATMs) and

b) Cases of cash shortages more than ₹ 5,000 if detected by Management / Auditor / Inspecting Officer and not reported on the day of occurrence by the persons handling cash.

6.4. To ensure uniformity and to avoid duplication, frauds involving forged negotiable instruments may be reported only by the paying banker and not by the collecting banker. However, in the case of collection of an instrument which is genuine but the amount is collected fraudulently by a person who is not true owner, the collecting bank, which is defrauded, will have to file fraud report with NABARD.

6.5. Cases of theft, burglary, dacoity and robbery should not be reported as fraud. Such cases may be reported separately as detailed in paragraph 26.

7. DETECTION OF FRAUD

Systems and procedures prescribed by the Bank adequately facilitate timely detection of frauds. Some of the sources unearthing the fraud could be:

a) Complaints from customers / alerts from investigating agencies
b) Electronic / Print Media / other sources.
c) Customer and transaction details through centralized data base, especially by the Offsite Monitoring Cells at Head Office and Regional Offices.
d) Prompt reconciliation of inter office accounts.
e) Controllers' visits
f) Various audit / inspections both by internal and external agencies.
g) Periodical changes in incumbencies
h) Anonymous / pseudonymous complaints with verifiable facts.

8. Willful Default

While investigating fraud in borrowal accounts the cases of willful default have to be clearly looked into.

A willful default is deemed to have occurred if any one or more of the following events take place in a borrowal account:

i) The unit has defaulted in meeting its payment/repayment obligations to the lender even when it has the capacity to honour the said obligations.

ii) The unit has defaulted in meeting its payment/repayment obligations to the lender and has not utilized the finance from the lender for the specific purposes for which finance was availed of but has diverted the funds for other purposes.

iii) The unit has defaulted in meeting its payment/repayment obligations to the lender and has siphoned off the funds so that the funds have not been utilized for the specific purpose for which finance was availed of, nor are the funds available with the unit in the form of other assets.

iv) The unit has defaulted in meeting its payment/repayment obligations to the lender and has also disposed off or removed the movable fixed assets or immovable property given by him or it for the purpose of securing a term loan without the knowledge of the bank/ lender.

9. DETECTION, INVESTIGATION AND REPORTING OF FRAUDS- ADHERENCE TO TIME NORMS

Time norms for investigation and crystallization of fraud have been prescribed to curtail the delay in reporting of fraud after occurrence.

9.1 As soon as a fraud is suspected at any branch/ office, a preliminary/flash report either through Fax/e-mail to be sent to the respective Regional Office under copy to AID, HO within 24 hours, but not later than 48 hours of detection of any fraud/ suspected fraud.

9.2 Preliminary Investigation:-

On receipt of the preliminary/ flash report, an experienced Senior Official shall be deputed by the Regional Office to the branch for immediate investigation into the matter.

9.3 Detailed Investigation:-

a. Detailed Investigation of fraud/suspected fraud cases, wherever required, may be got conducted as per requirement of Regional Offices/ HO Department, through Audit & Inspection Department (AID). Regional Offices may decide for detailed investigation of suspected fraud/ fraud incidents in the circumstances, such as:

- Fraud not established by preliminary investigation;

- On the basis of nature of incident initially, detailed investigation be advised;
- NABARD communications regarding frauds by unscrupulous borrower;
- Fraud reported by other Banks/ Financial Institutions as informed by CRILC/CFR;
- Account identified as RFA;
- After detection of fraud by certain official/ branch to unearth further frauds.

b. AID deputes Internal/ external auditors of the bank for the investigation of suspected fraud/ fraud cases. Investigation into a fraud should bring out the modus operandi, lapses, and the persons accountable for the loss to the Bank, lacuna observed, if any.

c. Investigation reports are analyzed at AID HO Department and matter is taken up with the concerned Department for appropriate action to plug the lacunae and strengthening of systems & procedures of the bank so as to avoid occurrence of frauds.

d. Investigation report should also elaborate about role of Third Party Entities (advocate, valuer, supplier, chartered accountant, builder etc.), if their negligence, mala-fide, involvement connivance has been perceived in occurrence of fraud.

e. Based on the nature of the fraud and amount involved, it is then decided whether the fraud case should be marked for administrative action or vigilance action. Accordingly, staff side action should be initiated by the concerned department.

9.4 Time Norms for Investigation and Crystallization of Fraud-To expedite crystallization of fraud following time norms shall be adhered to:-

S.No	Action & Time norms
1	Regional Office shall advise the detailed investigation to within 3 working days of cited instances .
2	AID-HO shall depute the auditor within 2 working days of receipt of such advice.
3	Auditor shall ensure investigation and submission of the report to AID-HO within minimum timeframe on case to case basis and category to category basis (borrowal or non-borrowal) within maximum outer limit of 14 working days.
4	Vetting at AID level and subsequent submission to Regional/Controlling Office be completed within 7 working days from the date of submission of Investigation report.

5	Regional Head shall take view of the investigation report and crystallize the incident as fraud or otherwise within 3 working days of receipt of report. Date of such crystallization of fraud would be treated as the date of detection for onward reporting to NABARD. Investigation Report/ other correspondence would be sent through email followed by hard copy.
6	In case the Investigating Official feels that he/she requires extra time in addition to the prescribed outer limit of 14 days, the extra days shall be permitted on request through proper channel by the GM, AID,HO (Maximum 7 days).
7	In exceptional cases where more days are required, in addition to the extra days, the same shall be permitted on request through proper channel by the GM, AID, HO.

10. STAFF RESPONSIBILITY

At the Branch level the responsibility is to abide by the guidelines in all manuals and policies and to report all frauds or red flags through the whistle-blower policy or otherwise to their immediate superiors.

Monitoring responsibilities of Regional Managers

Regional Managers must perform following broad (not limited to) activities in respect of fraud risk management:

1. Have frequent and meaningful/purposeful visits to the branches
2. Test check staff accounts at random for unusual transactions and also check balances shown in General Ledger.
3. Strengthen off-site surveillance / scrutinize the statistical and control returns critically and do detailed analysis for focused concentration on the branches showing abnormalities.
4. Look for unusual life style and behaviour of staff members.
5. Ensure proper rotation of staff in the branches and other offices as per extant HRD policy and avoid deputing the staff to previous branch as far as possible.
6. Hold frequent interactions with the branch customers to ascertain the level of satisfaction.
7. Attend all the complaints seriously and promptly as complaints have proved to be a good source of signals on frauds. Controlling Authorities should also address the root cause of the complaint.
8. Ensure submission of „Monthly Compliance Certificate‟ by the branches.

The above given list is only illustrative and does not limit the scope of the action in fraud prevention/ control.

11. Reporting of Frauds to NABARD

11.1. Frauds involving amounts of less than ₹1.00 lakh

The cases of individual frauds involving amounts of less than ₹1.00 lakh are not to be reported individually to NABARD. Statistical data in respect of such frauds should, however, be submitted to NABARD in a quarterly statement as detailed in para 12.1.

11.2. Frauds involving amounts of ₹ 1.00 lakh and above

The cases of individual frauds involving amounts of ₹ 1.00 lakh and above should be reported to NABARD through "ENSURE" portal, in the format given in DoS-FMS-1, within three weeks from the date of detection.

11.2.1. In respect of frauds in borrowal accounts involving an amount of ₹ 20.00 lakh and above, additional information as prescribed under Part B of DoS-FMS-1 may also be furnished. It is observed while scrutinizing DoS – FMS-1 returns from the banks that certain vital fields in the returns are left blank. As the complete particulars on frauds perpetrated in the banks are vital for monitoring and supervisory purposes and issue of caution advices, banks should ensure that the data furnished are complete/accurate and up-to-date. Incidentally, if no data is to be provided in respect of any of the items, or if details of any of the items are not available at the time of reporting of DoS-FMS-1 return, the bank may indicate as "no particulars to be reported" or "details not available at present" etc. In such a situation, the banks have to collect the data and report the details invariably through DoS-FMS-3 return on quarterly basis.

11.2.2. Fraud reports should also be submitted in cases where central investigating agencies have initiated criminal proceedings suo-moto and/or where the NABARD / Reserve Bank of India has directed that such cases be reported as frauds.

11.2.3. Central Fraud Monitoring Cell (CFMC), NABARD will disseminate a directory of officers of all RRBs responsible for reporting of Frauds etc. All RRBs should furnish to CFMC, DoS, NABARD, HO any changes in the names of officials that will be necessary for inclusion in the directory on priority basis as and when called for.

12. Quarterly Returns

12.1. Report on Frauds Outstanding (DoS-FMS-2)

12.1.1. Banks should upload a copy each of the Quarterly Report on Frauds Outstanding in the format given in DoS-FMS-2 in "ENSURE" within 30 days of the end of the quarter to which it relates. Banks which may not be having any fraud outstanding as at the end of a quarter should submit a nil report.

12.1.2. Part - A of the report covers details of frauds outstanding as at the end of the quarter. Part B of the report give category-wise and perpetrator-wise details of frauds reported during the quarter respectively. The total number and amount of fraud cases reported during the quarter as shown in Part B should tally with the totals of columns 5 and 6 in Part - A of the report.

12.1.3. Banks should furnish a certificate, as part of the above report, to the effect that all individual fraud cases of ₹1.00 lakh and above reported to NABARD in DoS FMS - 1 during the quarter have also been put up to the bank's Board and have been incorporated in Part - A (columns 5 and 6) and Part B of DoS-FMS - 2.

12.2. Progress Report on Frauds (DoS-FMS-3)

12.2.1. Banks should upload case-wise quarterly progress reports on frauds involving ₹1.00 lakh and above in the format given in DoS FMS-3 in "ENSURE" within 30 days of the end of the quarter to which it relates.

12.2.2. In case of frauds where there are no developments during a quarter, a list of such cases with brief description including name of branch and date of reporting may be furnished in Part-B of DoS-FMS - 3.

12.2.3. If there are no fraud cases involving ₹1.00 lakh and above outstanding, banks may submit a nil report.

13. Delays in Reporting of Frauds

13.1. Banks should ensure that the reporting system is suitably streamlined so that delays in reporting of frauds, submission of delayed and incomplete fraud reports are avoided. Banks must fix staff accountability in respect of delays in reporting of fraud cases to NABARD.

13.2. Delay in reporting of frauds by banks and the consequent delay in alerting other banks about the modus operandi by way of issue of caution advices against unscrupulous borrowers could result in similar frauds being perpetrated elsewhere. Banks may, therefore, strictly adhere to the time-frame fixed in this circular for reporting fraud cases to NABARD failing which banks would be liable for penal action as prescribed under Section 47(A) of the Banking Regulation Act, 1949.

14. Reports to the Board

14.1. Reporting of Frauds

Banks should ensure that all frauds of ₹ 1.00 lakh and above are reported to their Boards promptly on their detection. Such reports should, among other things, take note of the failure on the part of the concerned branch officials and controlling authorities, and give details of action initiated against the officials responsible for the fraud.

14.2. Quarterly Review of Frauds

14.2.1. AID, HO will place a quarterly review of frauds for the quarters ended June, September and December of every year before the Audit Committee of Board during the month following the quarter to which it pertains.

14.2.2. These should be accompanied by supplementary material analysing statistical information and details of each fraud so that the Board would have adequate material to contribute effectively in regard to the punitive or preventive aspects of frauds.

14.2.3. A separate review for the quarter ending March is not required in view of the Annual Review for the year-ending March prescribed at para 14.3 below.

14.3. Annual Review of Frauds

14.3.1. Banks should conduct an annual review of the frauds and place a note before the Board of Directors for information. The reviews for the year-ended March may be placed before the Board by the end of June of the following year. Such reviews may be presented for verification by NABARD's Inspecting Officers.

14.3.2. The main aspects which may be taken into account while making such a review may include the following:

a) Whether the systems in the bank are adequate to detect frauds, once the incidences have taken place, within the shortest possible time.

b) Whether frauds are examined from staff angle and, wherever necessary, the staff side action is taken without undue delay.

c) Whether deterrent punishment is meted out, wherever warranted, to the persons found responsible without undue delay.

d) Whether frauds have taken place because of laxity in following the systems and procedures or loopholes in the system and, if so, whether effective action has been taken to ensure that the systems and procedures are scrupulously followed by the staff concerned or the loopholes are plugged.

e) Whether frauds are reported to the local Police / CBI for investigation.

14.3.3. The annual reviews should also, among other things, include the following details:

a) Total number of frauds detected during the year and the amount involved as compared to the previous two years.

b) Analysis of frauds according to different categories detailed and also the different business areas indicated in Paragraphs 6.1 to 6.4 above.

c) Modus operandi of major frauds reported during the year along with their present position.

d) Detailed analyses of frauds of ₹ 1.00 lakh and above.

e) Estimated loss to the bank during the year on account of frauds, amount recovered and provisions made.

f) Number of cases (with amounts) where staff are involved and the action taken against staff.

g) Region-wise / Zone-wise breakup of frauds and amount involved.

h) Time taken to detect frauds (number of cases detected within three months, six months, one year, more than one year of their taking place).

i) Position with regard to frauds reported to the CBI / Police.

j) Number of frauds where final action has been taken by the bank and cases disposed of.

k) Preventive / punitive steps taken by the bank during the year to reduce / minimise the incidence of frauds. Whether systems and procedures have been examined to ensure that weaknesses are addressed.

The broad guidelines regarding constitution and functions of the Special Committee of the Board are given in the following paragraphs.

14.4. Special Committee

14.4.1. Constitution of the Special Committee

While Audit Committee of the Board (ACB) shall monitor all the cases of frauds in general, banks are required to constitute a Special Committee of the Board for monitoring and follow up of cases of frauds (SCBF) involving amounts of ₹ 20.00 lakh and above exclusively. The Special Committee may be constituted with five members of the Board of Directors who will include:

a) Chairman of the bank

b) Two members from Audit Committee of the Board; and

c) Two other members from the Board (may be by rotation) excluding NABARD nominee director / observer, if any.

14.4.2. Functions of Special Committee

The major functions of the Special Committee would be to:

a) Identify the systemic lacunae, if any, that facilitated perpetration of the fraud and put in place measures to plug the same;

b) Identify the reasons for delay in detection, if any, reporting to top management of the bank and NABARD.

c) Monitor progress of CBI / Police Investigation, and recovery position and;

d) Ensure that staff accountability is examined at all levels in all the cases of frauds and staff side action, if required, is completed quickly without loss of time.

e) Review the efficacy of the remedial action taken to prevent recurrence of frauds, such as, strengthening of internal controls.
f) Put in place other measures considered relevant to strengthen preventive measures against frauds.

14.4.3. Meetings

The periodicity of the meetings of the Special Committee may be decided according to the number of cases involved. However, the Committee should meet and review as and when a fraud involving an amount of ₹20.00 lakh and above comes to light.

14.4.4. Review of the functioning of the Special Committee

The functioning of the Special Committee of the Board may be reviewed on a half-yearly basis and the reviews may be put up to the Board of Directors.

14.4.5. The banks shall delineate in a policy document the processes for implementation of the Committee's directions and enable a dedicated outfit of the bank to implement the directions in this regard.

15. Cases of attempted fraud

15.1. Banks need not report cases of attempted frauds to NABARD. However, banks should continue to place the report on individual cases of attempted fraud involving an amount of ₹20.00 lakh and above before the Audit Committee of its Board. The report should cover the following viz.

a) The modus operandi of the attempted fraud.
b) How the attempt did not materialize into fraud or how the attempt failed/ was foiled.
c) The measures taken by the bank to strengthen the existing systems and controls.
d) New systems and controls put in place in the area where fraud was attempted.

15.2. Further, a consolidated review of such cases detected during the year containing information such as area of operations where such attempts were made, effectiveness of new processes and procedures put in place during the year, trend of such cases during the last three years, need for further change in processes and procedures, if any, etc. as on March 31 every year may be put up to the ACB within three months of the end of the relative year.

16. Closure of Frauds Cases

16.1. Banks will report to NABARD through “ENSURE”, the details of the fraud cases closed along with reasons for the closure where no further action was called for.

16.2. Fraud cases closed during the quarter are required to be reported quarterly through FMS 3 return and cross checked with relevant column in FMS 2 return before sending to NABARD.

16.3. Banks should report only such cases as closed where the actions as stated below are complete and prior approval is obtained from the respective Regional Offices of NABARD.

a) The fraud cases pending with CBI/Police/Court are finally disposed of.

b) The examination of staff accountability has been completed

c) The amount of fraud has been recovered or written off.

d) Insurance claim wherever applicable has been settled.

e) The bank has reviewed the systems and procedures, identified as the causative factors and plugged the lacunae and the fact of which has been certified by the appropriate authority (Board / Audit Committee of the Board)

16.4. Banks should also pursue vigorously with CBI for final disposal of pending fraud cases especially where the banks have completed staff side action. Similarly, banks may vigorously follow up with the police authorities and/or court for final disposal of fraud cases.

16.5. Banks are allowed, for limited statistical / reporting purposes, to close those fraud cases involving amounts up to ₹ 1.00 lakh, where:

a) The investigation is on or challan/ charge sheet has not been filed in the Court for more than three years from the date of filing of First Information Report (FIR) by the CBI/Police or

b) The trial in the courts, after filing of charge sheet/challan by CBI / Police, has not started or is in progress.

16.6. The banks are required to follow the guidelines relating to seeking prior approval for closure of such cases from the RO of NABARD under whose jurisdiction the Head Office of the bank is located and follow up of such cases after closure as mentioned below.

16.7. The banks shall have to submit their proposals, case wise, for closure to the Regional Office of NABARD under whose jurisdiction their Head Offices are situated. The cases may be closed after getting the approval of the respective Regional Offices of NABARD. The banks should maintain the record of details of such cases in a separate ledger. Even after closure of the fraud cases for limited statistical purposes, banks should vigorously follow up with the investigating agencies (CBI / Police) to ensure that the investigation process is taken to its logical conclusion. Similarly, the banks should continue to ensure that they are regularly and appropriately represented in the court proceedings as and when required. All the relevant records pertaining to such cases must be preserved till the cases are finally disposed of by CBI/ Police or Courts, as the case may be.

16.8. The banks shall, with the approval of their respective Boards, frame their own internal policy for closure of fraud cases, incorporating the above norms and other internal procedures / controls as deemed necessary.

16.9. Notwithstanding the fact that banks may close cases of fraud even when Police / CBI investigation is in progress or cases are pending in the court of law, they should complete, within the prescribed time frame, the process of examination of staff accountability or conclude staff side actions.

17. Guidelines for Reporting of Frauds to Law enforcing agencies i.e. Police /CBI

17.1. Cases to be referred to Local Police

Banks should follow the following guidelines for reporting of frauds such as unauthorized credit facilities extended by the bank for illegal gratification, negligence and cash shortages, cheating, forgery, etc. to the State Police authorities :

(a) In dealing with cases of fraud / embezzlement, banks should not merely be motivated by the necessity of recovering expeditiously the amount involved, but should also be motivated by public interest and the need for ensuring that the guilty persons do not go unpunished.

(b) Therefore, as a general rule, the following cases should invariably be referred to the State Police:

(i) Cases of financial fraud involving an amount of ₹ 1 lakh and above, committed by outsiders on their own and / or with the connivance of bank staff / officers should be reported by the Regional Head of the bank concerned to a senior officer of the State CID/Economic Offenses wing of the State concerned.

(ii) Cases of financial fraud committed by bank employees, when it involves banks' funds exceeding ₹ 10,000/- should be reported to the local police station by the bank branch concerned.

(iii) All fraud cases of value below ₹ 10000 involving bank officials, should be referred to the Head office of the bank, who would scrutinize each case and direct the bank branch concerned on whether it should be reported to the local police station for further legal action.

17.2. Cases to be referred to CBI

The banks should report fraud cases involving amount of ₹ 3.00 crore and above to CBI and those below ₹ 3.00 crore to local police, as detailed below:

(a) Cases of ₹ 3.00 crore and above upto ₹ 15.00 crore
* Where staff involvement is prima facie evident - CBI (Anti-Corruption Branch)
* Where staff involvement is prima facie not evident - CBI (Economic Offenses Wing)

(b) All cases involving more than ₹ 15.00 crore - Banking Security and Fraud Cell of the respective centers, which is specialised cell of the Economic Offenses Wing of the CBI for major bank fraud cases.

17.3. Time limit for filing FIR to Police / CBI

FIR should be filed with Police (EOW/CID) & CBI (EOW/ACB/BSFC) as the case may be, **within 30 days** from the date of reporting the incidence as fraud to NABARD and copy thereof should be forwarded to FRMC Cell for record.

17.4. Vetting of FIR *(For Borrowal Frauds and Non Borrowal Frauds)*

a) For the *Fraud Amount*, the complaint with law enforcement agencies should be filed after it is vetted by Legal Department at Head Office.

b) The complaint/FIR to be lodged with law enforcement agencies should be signed by the concerned Regional Manager.

18. Reporting to Financial Intelligent Unit

All frauds where criminal intent is discernible on the part of perpetrators could be both internal and external; Suspicious Transaction Report (STRs) in prescribed format will have to be submitted to the Financial Intelligence Unit – India (FIU-IND) by AML/KYC cell of our Bank.

19. Cheque Related Frauds, Precautions to be taken and reporting to NABARD and the Police

19.1. The rise in the number of cheque related fraud cases is a matter of serious concern. It is evident that many of such frauds could have been avoided had due diligence been observed at the time of handling and/or processing the cheques and monitoring newly opened accounts. Banks are, therefore, advised to review and strengthen the controls in the cheque presenting / passing and account monitoring processes and to ensure that all procedural guidelines including preventive measures are followed meticulously by the dealing staff/officials. Given below are some of the preventive measures banks may follow in this regard. The list is only indicative.

a) Ensuring the use of 100% “CTS – 2010” compliant cheques.

b) Strengthening the infrastructure at the cheque handling Service Branches and bestowing special attention on the quality of equipment and personnel posted for CTS based clearing, so that it is not merely a mechanical process.

c) Ensuring that the beneficiary is KYC compliant so that the bank has recourse to him/her as long as he/she remains a customer of the bank.

d) Examination under UV lamp for all cheques beyond a threshold of say, ₹ 2 lakh.

e) Checking at multiple levels, of cheques above a threshold of say, ₹ 5 lakh.

f) Close monitoring of credits and debits in newly opened transaction accounts based on risk categorization.

g) Sending an SMS alert to payer/drawer when cheques are received in clearing.

h) The threshold limits mentioned above can be reduced or increased at a later stage with the approval of the Board depending on the volume of cheques handled by the banks or it's risk appetite.

19.2. In addition to the above, banks may consider the following preventive measures for dealing with suspicious or large value cheques (in relation to an account's normal level of operations):

a) Alerting the customer by a phone call and getting the confirmation from the payer/drawer.

b) Contacting base branch in case of non-home cheques.

The above may be resorted to selectively if not found feasible to be implemented systematically.

19.3. It has been reported that in some cases even though the original cheques were in the custody of the customer, cheques with the same series had been presented and encashed by fraudsters. In this connection, banks are advised to take appropriate precautionary measures to ensure that the confidential information viz., customer name / account number / signature, cheque serial numbers and other related information are neither compromised nor misused either from the bank or from the vendors' (printers, couriers etc.) side. Due care and secure handling is also to be exercised in the movement of cheques from the time they are tendered over the counters or dropped in the collection boxes by customers.

19.4. To ensure uniformity and to avoid duplication, reporting of frauds involving forged instruments including fake / forged instruments sent in clearing in respect of truncated instruments will continue to be done by the paying banker and not by the collecting banker. In such cases the presenting bank will be required to immediately hand over the underlying instrument to drawee / paying bank as and when demanded to enable it to file an FIR with the police authorities and report the fraud to NABARD. It is the paying banker who has to file the police complaint and not the collecting banker.

19.5. However, in the case of collection of an instrument which is genuine but the amount is collected fraudulently by a person who is not the true owner or where the amount has been credited before realisation and subsequently the instrument is found to be fake / forged and returned by the paying bank, the collecting bank, which is defrauded or is at loss by paying the amount before realisation of the instrument, will have to file both the fraud report with the NABARD and complaint with the police.

19.6. In case of collection of altered/fake cheque involving two or more branches of the same bank, the branch where the altered/fake cheque has been encashed, should report the fraud to its Head Office. Similarly in the event of an altered/fake cheque having been paid/encashed involving two or more branches of a bank under Core Banking Solution (CBS), the branch which has released the payment should report the fraud to the Head Office. Thereafter, Head Office of the bank will file the fraud report with NABARD and also file the Police complaint.

20. Authority Deciding Fraud cases (Borrowal / Non-Borrowal)

The Regional Manager will initiate investigation by appointing a senior officer on receiving information about prima facie irregularities/malpractice etc received by way of control returns, audit reports, visit reports or complaints. The investigation report is to be submitted to the competent authority within stipulated time to take a decision on fraud.

The following authorities are competent to decide & declare fraud based on the amount involved in the incidence or outstanding loan facility

Committee	Members of the committee	Authority Deciding Fraud cases (Borrowal / Non-Borrowal)	Delegated Power to declare fraud
RO Regional Manager committee	1-Regional Manager 2-Present Branch Manager 3-Any officer Scale ll from Regional Office	All three are required to complete the quorum for recommendation	Recommending Authority
HO GM Committee	1-General Manager OPR 2-Chief Manager /Senior Manager OPR 3-Chief Manager /Senior Manager DAD 4-Chief Manager/Senior Manager Audit & Inspection	On the recommendation of RO committee. (minimum 4 officials in which General Manager is mandatory to decide & declare fraud)	Up to 25 lac
HO Chairman Committee	1-Chairman 2-General Manager OPR 3-General Manager Other 4-Chief Manager /Senior Manager OPR 5-Chief Manager /Senior Manager DAD 6-Chief Manager/Senior Manager Audit & Inspection	On the recommendation of RO & GM Committee. (minimum 5 officials in which Chairman and one GM are mandatory to decide & declare fraud)	Above 25 lac

21. Staff Accountability for frauds

21.1. As in the case of accounts categorised as NPAs, banks must initiate and complete a staff accountability exercise within six months from the date of classification as a Fraud. Wherever felt necessary or warranted, the role of sanctioning official(s) may also be covered under this exercise. The completion of the staff accountability exercise for frauds and the action taken may be placed before the SCBF and intimated to NABARD at quarterly intervals in FMS.

21.1.1. Banks may bifurcate all fraud cases into vigilance and non-vigilance. Only vigilance cases should be referred to the investigative authorities. Non-vigilance cases may be investigated and dealt with at the bank level within a period of six months.

21.1.2. In cases involving very senior executives of the bank, the Board may initiate the process of fixing staff accountability.

21.1.3. Staff accountability should not be held up on account of the case being filed with law enforcement agencies. Both the criminal and domestic enquiry should be conducted simultaneously.

21.2. In the case of fraud in Non-Borrowal accounts, banks must initiate and complete a staff accountability exercise within six months from the date of classification as a Fraud.

21.3. Staff accountability would be examined by:

a) In Borrowal fraud accounts, staff accountability is to be got examined by Regional Manager, where the loan is sanctioned by Branch Manager.

b) Where the loan is sanctioned by Regional Manager, staff accountability be got examined by General Manager.

c) Where the loan is sanctioned by General Manager, staff accountability be got examined by Chairman .

d) In case of Non-Borrowal frauds, staff accountability be got examined by the Regional Manager.

21.4. Time Line for staff action.

In case staff is found accountable, action will be initiated as per following timeline.

Within 7 working days of receiving staff accountability report, Memo should be issued to the erring Official/s calling for an explanation and advising him/them to submit the reply within 7 working days.

a) After receipt of the reply, if not satisfied, the Charge Sheet
b) should be issued within 15 days after getting views of Internal Advisory Committee (IAC) of Vigilance Department.
c) CSO/CSE will submit reply to chargesheet within 15 days.
d) On receipt of the reply to chargesheet of the CSO/CSE, the final order is to be passed within a period of 2 months, if the case is dealt with minor penalty. In case of major penalty proceedings, the Inquiry should be completed within 2 months from the date of appointment of IA/PO.
e) Inquiring Authority to submit his findings/ report to Disciplinary Authority within 20 days of conclusion of inquiry.
f) Disciplinary Authority to seek comments of the concerned officer on the findings of Inquiring Authority within 15 days.
g) The concerned Officer should submit his reply within 10 days from receipt of the findings of I.A. to Disciplinary Authority.
h) Disciplinary Authority, shall take final decision within 15 days in non-vigilance cases and in case of vigilance cases, he will send his observations to Vigilance Deptt. within 15 days.
i) Disciplinary Authority will pass Final Order within 15 days of receipt of advice of Vigilance Department/CVC.
j) The entire process, right from issuing of chargesheet to passing final order to

be completed within maximum period of 180 days which will also take care of any unforeseen reasons for delay such as adjournments for genuine reasons/natural justice etc.

22. Procedure and delegation power for Fraud amount payment to the customers if fraud committed in customer account

22.1. For quick disposal of the claim for fraud payment to customers if fraud committed in customer account .
Delegation power is under mentioned .

Committee	Members of the committee	Sanction/Recommended by	Delegated Power
RO Regional Manager committee	1-Regional Manager 2-Present Branch Manager 3-Any officer Scale ll from Regional Office	All three are required to complete the quorum for sanction/recommendation	50000 Per Customer
HO GM Committee	1-General Manager OPR 2-Chief Manager /Senior Manager OPR 3-Chief Manager /Senior Manager DAD 4-Chief Manager/Senior Manager Audit & Inspection	On the recommendation of RO committee. (minimum 4 officials in which General Manager is mandatory to complete the quorum for sanction/ recommendation)	Above 50000 up to 2.0 lac
HO Chairman Committee	1-Chairman 2-General Manager OPR 3-General Manager Other 4-Chief Manager /Senior Manager OPR 5-Chief Manager /Senior Manager DAD 6-Chief Manager/Senior Manager Audit & Inspection	On the recommendation of RO & GM Committee . (minimum 5 officials in which Chairman and one GM are mandatory to complete the quorum for sanction .)	Above 2.0 lac

22.2. Sanctioning/Recommanding committee will verify and obtain followings .

a. Fraud amount must be declared by competent authority.
b. Origional Passbook,vouchers, and other relevent papers must be obtained .
c. Obtain Indemnity with two Surities .
d. Obtain financial worth of the surities .worth must be double the amount of claim
e. Obtain Money receipt with declatation ‘‘I/we have received full and final payment“
f. Tally the fraudlent amount with declared amount by competent authority .
g. Payment will be made by debiting CD (N) Fraud head .
h. Any recovery received later will be kept in CD(N) Creditor Fraud head.
i. All origional papers will be kept in custody of the Bank.

23. Write Off

When all avenues available for recovery are exhausted, Bank will arrange for writing off the likely loss with the approval of the appropriate authority. With a view to ensuring that all relevant aspects are given focused attention before writing off of loss in a fraud case, the process of seeking administrative clearance for the proposed write off will be followed. Civil/criminal cases and recovery proceedings and other issues, if pending, would be followed up for their logical conclusion.

24. Provisioning:

a) In case of accounts classified as 'fraud', banks are required to make provisions to the full extent of amount involved in the fraud, irrespective of the value of security.

b) However, final provision figure of Non-Borrowal Frauds will be arrived after taking into account the amount of recovery, expected recovery and insurance claim received.

25. LOAN FRAUDS – NEW FRAMEWORK

25.1 The increasing incidence of frauds in general and in loan portfolios in particular in RRBs is a matter of serious concern. There is a need for implementing a framework for fraud risk management in banks.

25.2. The objective of the framework is to direct the focus of banks on the aspects relating to prevention, early detection, prompt reporting to NABARD (for system level aggregation, monitoring & dissemination) and the investigative agencies (for instituting criminal proceedings against the fraudulent borrowers) and timely initiation of the staff accountability proceedings (for determining negligence or connivance, if any) while ensuring that the normal conduct of business of the banks and their risk taking ability is not adversely impacted and no new and onerous responsibilities are placed on the banks. In order to achieve this objective, the framework has stipulated time lines with the action incumbent on a bank. The time lines / stage wise actions in the loan life-cycle are expected to compress the total time taken by a bank to identify a fraud and aid more effective action by the law enforcement agencies. The early detection of Fraud and the necessary corrective action are important to reduce the quantum of loss which the continuance of the Fraud may entail.

25.3. Early Warning Signals (EWS) and Red Flagged Accounts (RFA)

25.3.1. A Red Flagged Account (RFA) is one where a suspicion of fraudulent activity is thrown up by the presence of one or more Early Warning Signals (EWS). These signals in a loan account should immediately put the bank on alert regarding a weakness or wrong doing which may ultimately turn out to be fraudulent. A bank cannot afford to ignore such EWS but must instead use them as a trigger to launch a detailed investigation into a RFA.

25.3.2. An illustrative list of some EWS is given for the guidance of banks in **Annexure I** of this circular**.** Banks may choose to adopt or adapt the relevant signals from this list and also include other alerts/signals based on their experience, client profile and business models. The EWS so compiled by a bank would form the basis for classifying an account as a RFA.

25.3.3. The threshold for EWS and RFA is an exposure of ₹ 20.00 lakh or more at the level of a bank irrespective of the lending arrangement (whether solo banking, multiple banking or consortium).

25.3.4. The modalities for monitoring of loan frauds below ₹ 20.00 lakh threshold is left to the discretion of banks. However, banks may continue to report all identified accounts to CFMC, NABARD as per the existing cut-offs.

25.3.5. The tracking of EWS in loan accounts should not be seen as an additional task but must be integrated with the credit monitoring process in the bank so that it becomes a continuous activity and also acts as a trigger for any possible credit impairment in the loan accounts, given the interplay between credit risks and fraud risks. In respect of large accounts it is necessary that banks undertake a detailed study of the Annual Report as a whole and not merely of the financial statements, noting particularly the Board Report and the Managements' Discussion and Analysis Statement as also the details of related party transactions in the notes to accounts. The officer responsible for the operations in the account, by whatever designation called, should be sensitised to observe and report any manifestation of the EWS promptly to the Fraud Monitoring Group (FMG) or any other group constituted by the bank for the purpose immediately. To ensure that the exercise remains meaningful, such officers may be held responsible for non-reporting or delays in reporting.

25.3.6. The FMG should report the details of loan accounts of ₹ 20.00 lakh and above in which EWS are observed, together with the decision to classify them as RFAs or otherwise to the CEO of the bank every month.

25.3.7. A report on the RFA accounts may be put up to the Board for monitoring and follow-up of Frauds, a synopsis of the remedial action taken together with their current status.

25.4. Early Detection and Reporting

25.4.1. At present the detection of frauds takes an unusually long time. Banks tend to report an account as fraud only when they exhaust the chances of further recovery. Among other things, delays in reporting of frauds also delays the alerting of other banks about the modus operandi through various measure that may result in similar frauds being perpetrated elsewhere. More importantly, it delays action against the unscrupulous borrowers by the law enforcement agencies which impact the recoverability aspects to a great degree and also increases the loss arising out of the fraud.

25.4.2. The most effective way of preventing frauds in loan accounts is for banks to have a robust appraisal and an effective credit monitoring mechanism during the entire life-cycle of the loan account. Any weakness that may have escaped attention at the appraisal stage can often be mitigated in case the post disbursement monitoring remains effective. In order to strengthen the monitoring processes, based on an analysis of the collective experience of the banks, inclusion of the following checks / investigations during the different stages of the loan life-cycle may be carried out:

a) Pre-sanction: As part of the credit process, the checks being applied during the stage of pre-sanction may consist of the Risk Management Group (RMG) or any other appropriate group of the bank collecting independent information and market intelligence on the potential borrowers which could be used as an input by the sanctioning authority. Banks may keep the record of such pre-sanction checks as part of the sanction documentation.

b) Disbursement: Checks by RMG during the disbursement stage may focus on the adherence to the terms and conditions of sanction, rationale for allowing dilution of these terms and conditions, level at which such dilutions were allowed, etc. The dilutions should strictly conform to the broad framework laid down by the Board in this regard. As a matter of good practice, the sanctioning authority may specify certain terms and conditions as 'core' which should not be diluted. The RMG may immediately flag the non-adherence of core stipulations to the sanctioning authority.

c) Annual review: While the continuous monitoring of an account through the tracking of EWS is important, banks also need to be vigilant from the fraud perspective at the time of annual review of accounts. Among other things, the aspects of diversion of funds in an account, adequacy of stock vis-a-vis stock statements, stress in group accounts, etc., must also be commented upon at the time of review. Besides, the RMG should have capability to track market developments relating to the major clients of the bank and provide inputs to the credit officers. This would involve collecting information from the grapevine, following up stock market movements, subscribing to a press clipping service, monitoring databases on a continuous basis and not confining the exercise only to the borrowing entity but to the group as a whole.

25.5. Staff empowerment: Employees should be encouraged to report fraudulent activity in an account, along with the reasons in support of their views, to the appropriately constituted authority, under the Whistle Blower Policy of the bank, who may institute a scrutiny through the FMG. The FMG may 'hear' the concerned employee in order to obtain necessary clarifications. Protection should be available to such employees under the whistle blower policy of the bank so that the fear of victimisation does not act as a deterrent.

25.6. Role of Auditors: During the course of the audit, auditors may come across instances where the transactions in the account or the documents point to the possibility of fraudulent transactions in the account. In such a situation, the auditor may immediately bring it to the notice of the top management and if necessary to the Audit Committee of the Board (ACB) for appropriate action.

25.7. Bank as a sole lender

25.7.1. In cases where the bank is the sole lender, the FMG will take a call on whether an account in which EWS are observed should be classified as a RFA or not. This exercise should be completed as soon as possible and in any case within a month of the EWS being noticed. In case the account is classified as a RFA, the FMG will stipulate the nature and level of further investigations or remedial measures necessary to protect the bank's interest within a stipulated time which cannot exceed six months.

25.7.2. The bank may use external auditors, including forensic experts or an internal team for investigations before taking a final view on the RFA. At the end of this time line, which cannot be more than six months, banks would either lift the RFA status or classify the account as a fraud.

25.7.3. A report on the RFA accounts may be put up to the Board with the observations/decision of the FMG. The report may list the EWS/irregularities observed in the account and provide a synopsis of the investigations ordered / remedial action proposed by the FMG together with their current status.

25.8. Lending under Consortium or Multiple Banking Arrangements (MBA)

25.8.1. Certain unscrupulous borrowers enjoying credit facilities under “multiple banking arrangement (MBA)” after defrauding one of the financing banks, continue to enjoy the facilities with other financing banks and in some cases avail even higher limits at those banks. In certain cases the borrowers use the accounts maintained at other financing banks to siphon off funds by diverting from the bank on which the fraud is being perpetrated. This is due to lack of a formal arrangement for exchange of information among various lending banks/FIs. In some of the fraud cases, the securities offered by the borrowers to different banks are the same.

25.8.2. In view of this, all the banks which have financed a borrower under 'multiple banking' arrangement should take coordinated action, based on commonly agreed strategy, for legal / criminal actions, follow up for recovery, exchange of details on modus operandi, achieving consistency in data / information on frauds reported to Reserve Bank of India. Therefore, bank which detects a fraud is required to immediately share the details with all other banks in the multiple banking arrangements.

25.8.3. In case of consortium arrangements, individual banks must conduct their own due diligence before taking any credit exposure and also independently monitor the end use of funds rather than depend fully on the consortium leader. However, as regards monitoring of Escrow Accounts, the details may be worked out by the consortium and duly documented so that accountability can be fixed easily at a later stage. Besides, any major concerns from the fraud perspective noticed at the time of annual reviews or through the tracking of early warning signals should be shared with other consortium / multiple banking lenders immediately as hitherto.

25.8.4. The initial decision to classify any standard or NPA account as RFA or Fraud will be at the individual bank level and it would be the responsibility of this bank to report the RFA or Fraud status of the account to alert the other banks. Thereafter, within 15 days, the bank which has red flagged the account or detected the fraud would ask the consortium leader or the largest lender under MBA to convene a meeting of the Joint Leaders Forum (JLF) to discuss the issue. The meeting of the JLF so requisitioned must be convened within 15 days of such a request being received. In case there is a broad agreement, the account would be classified as a fraud; else based on the majority rule of agreement amongst banks with at least 60% share in the total lending, the account would be red flagged by all the banks and subjected to a forensic audit commissioned or initiated by the consortium leader or the largest lender under MBA. All banks, as part of the consortium or multiple banking arrangement, would share the costs and provide the necessary support for such an investigation.

25.8.5. The forensic audit must be completed within a maximum period of three months from the date of the JLF meeting authorizing the audit. Within 15 days of the completion of the forensic audit, the JLF will reconvene and decide on the status of the account, either by consensus or the majority rule as specified above. In case the decision is to classify the account as a fraud, the RFA status would change to Fraud in all banks and reported to NABARD within a week of the said decision. Besides, within 15 days of the NABARD reporting, the bank commissioning/ initiating the forensic audit would lodge a complaint with the CBI on behalf of all banks in the consortium/MBA.

25.8.6. It may be noted that the overall time allowed for the entire exercise to be completed is six months from the date when the first member bank reported the account as RFA or Fraud.

25.9. Filing Complaints with Law Enforcement Agencies

25.9.1. Banks are required to lodge the complaint with the law enforcement agencies immediately on detection of fraud. There should ideally not be any delay in filing of the complaints with the law enforcement agencies since delays may result in the loss of relevant 'relied upon' documents, non-availability of witnesses, absconding of borrowers and also the money trail getting cold in addition to asset stripping by the fraudulent borrower.

25.9.2. It is observed that banks do not have a focal point for filing CBI / Police complaints. This results in a non-uniform approach to complaint filing by banks and the investigative agency has to deal with dispersed levels of authorities in banks. This is among the most important reasons for delay in conversion of complaints to FIRs. It is, therefore, enjoined on banks to establish a nodal point / officer for filing all complaints with the CBI on behalf of the bank and serve as the single point for coordination and redressal of infirmities in the complaints.

25.9.3. The complaint lodged by the bank with the law enforcement agencies should be drafted properly and invariably be vetted by a legal officer. It is also observed that banks sometimes file complaints with CBI / Police on the grounds of cheating, misappropriation of funds, diversion of funds etc., by borrowers without classifying the accounts as fraud and/or reporting the accounts as fraud to NABARD. Since such grounds automatically constitute the basis for classifying an account as a fraudulent one, banks may invariably classify such accounts as frauds and report the same to NABARD.

25.10. Penal measures for fraudulent borrowers

25.10.1. In general, the penal provisions as applicable to wilful defaulters would apply to the fraudulent borrower including the promoter director(s) and other whole time directors of the company insofar as raising of funds from the banking system or from the capital markets by companies with which they are associated is concerned, etc. In particular, borrowers who have defaulted and have also committed a fraud in the account would be debarred from availing bank finance from Scheduled Commercial Banks, Development Financial Institutions, Government owned NBFCs, Investment Institutions, etc., for a period of five years from the date of full payment of the defrauded amount. After this period, it is for individual institutions to take a call on whether to lend to such a borrower. The penal provisions would apply to non-whole time directors (like nominee directors and independent directors) only in rarest of cases based on conclusive proof of their complicity.

25.10.2. No restructuring or grant of additional facilities may be made in the case of RFA or fraud accounts.

25.10.3. No compromise settlement involving a fraudulent borrower is allowed unless the conditions stipulate that the criminal complaint will be continued.

26. Reporting Cases of Theft, Burglary, Dacoity and Bank Robberies

26.1. Banks should report instances of bank robberies, dacoities, thefts and burglaries immediately on their occurrence to NABARD through "ENSURE" portal, in the format given in DoS – FMS-4a.

The report should include details of modus operandi and other information as at columns 1 to 11 of DoS-FMS - 4.

26.2. Banks should also submit a **quarterly** consolidated statement in the format given in DoS-FMS-4 in "ENSURE" covering all cases pertaining to the quarter. This may be submitted within 30 days of the end of the quarter to which it relates.

26.3. Banks which do not have any instances of theft, burglary, dacoity and / or robbery to report during the quarter, may submit a nil report.

27. Legal Audit of Title Documents in respect of Large Value Loan Accounts

27.1. Banks should subject the title deeds and other documents in respect of all credit exposures of ₹ 1.00 crore and above to periodic legal audit and re- verification of title deeds with relevant authorities as part of regular audit exercise till the loan stands fully repaid.

27.2. Banks shall furnish a review note to their Board / Audit Committee of the Board at quarterly intervals on an ongoing basis giving therein the information in respect of such legal audits which should cover aspects, inter alia, like number of loan accounts due for legal audit for the quarter, how many accounts covered, list of deficiencies observed by the auditors, steps taken to rectify the deficiencies, number of accounts in which the rectification could not take place, course of action to safeguard the interest of bank in such cases, action taken on issues pending from earlier quarters.

28. Systems and Controls

Compliance of prescribed systems and procedures and control functions are critical to the organization in prevention of frauds. Hence, a review mechanism is to be undertaken on a regular basis to ensure that frauds of similar nature do not occur. An illustrative list of areas demanding focused attention of Controllers, at every level, to ensure prevention of frauds, is given below:

a) Stress on KYC compliance and due diligence standards.

b) Alert Reports, other control reports and verification of slips/ vouchers are to be meaningfully reviewed on daily basis. Branch Heads and Controlling Offices shall be accountable in case of any violation leading to perpetration of frauds.

c) Control Returns submitted by branches/ sanctioning authorities of different levels should be scrutinized meaningfully.

d) Nominal accounts, BGL accounts and Internal accounts, Inoperative accounts are to reconciled and checked regularly as these a/cs are easy target of fraudsters.

e) Control of system access and verification of system generated reports like Supplementary and daily critical reports are to be reviewed/ scrutinized by Branch Heads.

f) Paying branches to seek clear confirmation from issuing branches, if manually prepared drafts are presented for payment.

g) Involvement of staff through concepts like 'Preventive Vigilance Committee', 'whistle blower, 'alertness awards scheme' etc.

h) Identity of the whistle blower is not to be revealed.

i) Imparting training to operating staff to update their job knowledge and skill sets.

j) Following Best Practices Code adopted by the Bank.

k) Action against third party vendors who are found to have committed professional improprieties.

l) Job rotation and transfer policy.

m) Scrutiny of staff accounts and keeping watch over life styles of members of staff.

The aforesaid systems and controls are illustrative and not exhaustive. All the branches / offices and dealing groups / verticals of the Bank are advised to read the same in conjunction with the related operational guidelines / circulars issued by the Bank from time to time.

29 FRAUD RISK MANAGEMENT CELL (FRM CELL)

FRM Cell will lend the necessary sharpness and penetrative edge required in controlling frauds and consequent risk arising there from.

29.1. Role & Responsibilities of FRM Cell

The FRM Cell would have the following duties:

29.1.1 Collect investigation reports in respect of all frauds, analyze the frauds for root causes, compile common characteristics observed and suggest preventive steps.

29.1.2 Develop scenarios for data mining such as:

- Large value operations in inoperative accounts.
- Quick mortality of retail advances etc.

29.1.3 Consult and co-ordinate with other departments in developing such scenarios.

29.1.4 Report to the Managing Director & CEO on regular basis about the root cause analysis of cases reported to it.

29.1.5 Provide updates and report to the Top Management for maintaining, improving and refining the Fraud Risk Management policy

29.1.6 Conduct regular training programs within the Bank for upgrading skills of officers in Fraud Risk Management.

29.1.7 Collect data relevant to the frauds and record in a systematic, disciplined manner in a central data repository, which is retrievable in case of future reference.

29.1.8 Address the fraud prevention techniques on the basis of root cause analysis of high impact of frauds.

29.1.9 Implement the FRM policy and be responsible for reviewing it.

29.1.10 The FRM cell within itself would also have independent team which would be constantly engaged into data mining and research for advanced tools and techniques to ferret out the possibilities of fraud.

29.1.11 Creating fraud awareness amongst all employees.

29.1.12 FRM cell shall coordinate with other departments for prevention of frauds and risk mitigation.

29.2. Fraud Risk Management Process

In order to have singular focus on fraud prevention and management function, Fraud Risk Management policy has been devised. The fraud risk management approach is one that is focused on three objectives:

a) Prevention: controls designed to reduce the risk of fraud and misconduct from occurring in the first place.

b) Detection: controls designed to discover fraud and misconduct when it occurs due to unwarranted departure from norms, carelessness & abuse of authority.

c) Response: controls designed to take corrective action and remedy the harm caused by fraud or misconduct.

30. FRAUDS COMMITTED BY UNSCRUPULOUSBORROWERS

30.1. It is observed that a large number of frauds are committed by unscrupulous borrowers including companies, partnership firms/proprietary concerns and/or their directors/partners by various methods including the following:

(i) Fraudulent discount of instruments or kite flying in clearing effects.

(ii) Fraudulent removal of pledged stocks/disposing of hypothecated stocks without the bank's knowledge/inflating the value of stocks in the stock statements and drawing excess bank finance.

(iii) Diversion of funds outside the borrowing units, lack of interest or criminal neglect on the part of borrowers, their partners, etc. and also due to managerial failure leading to the unit becoming sick and due to laxity in effective supervision over the operations in borrowal accounts on the part of the bank functionaries rendering the advance difficult to recover.

30.2. In respect of frauds in borrowal accounts, additional information as prescribed under Annexure 1 of FMS should also be furnished.

30.3. Branches should exercise due diligence while appraising the credit needs of unscrupulous borrowers, borrower companies, partnership/ proprietorship concerns and their directors, partners and proprietors etc. as also their associates who have defrauded the banks.

31. Third Party Entities (TPE) – Reporting to IBA

Third parties such as builders, warehouse/cold storage owners, motor vehicle/tractor dealers, travel agents etc. and professionals such as architects, valuers, chartered accountants, advocates etc. are also to be held accountable if they have played a vital role in credit sanction/disbursement or facilitated the perpetration of frauds. The Bank is required to report to IBA the details of such third parties involved in frauds. Before reporting to IBA, the Bank has to satisfy itself of the involvement of third parties concerned and also provide them with an opportunity of being heard. In this regard the Bank should follow due process of natural justice. The same should be suitably recorded. On the basis of such information, IBA would, in turn, prepare caution lists of such third parties for circulation among the Banks.

31.1. Law Deptt., HO is the authority to inform the name of such advocates to IBA for inclusion of their names in IBA caution list.

31.2. Credit Deptt. HO Is the authority to inform the name of such architects/valuers/chartered accountants to IBA for inclusion of their names in IBA caution list.

32. Reporting Requirements

Fraud Flagging in CBS:-

Once an account is declared as fraud by competent authority and reported to NABARD the account should be FRAUD FLAGGED in CBS (as per new functionality on fraud flagging in CBS)

33. RECOVERY OF FRAUD LOSSES

33.1. The operating units should put in vigorous efforts, immediately after detection of a fraud, to recover the entire amount involved. Generally maximum recovery in fraud case is possible when recovery effort is put immediately after the occurrence of fraud. Hence, it is necessary to reduce the time gap between occurrence of fraud and its detection. This will help bank to initiate faster recovery steps. A systematic approach should be adopted in recovery of fraud losses, as illustrated below:

- Money trail should be traced so as to identify the assets created out of defrauded money to ensure recovery of the amount.
- Trace other assets, if any, available with the fraudsters.
- Take urgent and effective steps for enforcing security available
- Civil suits would be filed against the fraudsters.
- Close follow-up with the Bank's advocates to ensure prompt and logical conclusion of the cases.
- Co-ordinated approach with Collecting Bank in respect of frauds involving forged instruments paid through clearing.
- Recourse to arbitration/ legal action shall be considered if the expected coordination is not forthcoming from the counter-party bank.
- The Police may also recover some amount during their investigation. This shall be deposited in Court pending final adjudication. The bank should liaise with the Police and keep track of such amounts.
- Retired police officials (SP/DSP) may be engaged as retainer consultants to help in recovery process.

Further, bank needs to develop suitable MIS for monitoring progress in the recovery efforts. Additionally, bank should fix recovery targets in fraud related events and quarterly reviews be placed before ACB.

32.2. Recovery Process:

a) In order to recover defrauded amount, Bank will file recovery suit in Court/DRT apart from tracing other assets of the borrowers & guarantors & attaching the same through Court.

b) The attachment of staff property should be made by following the due process of Law where staff involvement is established.

33.3 OTS Proposal in respect of fraudulent accounts

Bank is considering the settlement proposals submitted by the borrowers who have obtained facility by making fraudulent representation or otherwise committing fraud. As the progress in these cases takes very long time for any logical conclusion, Bank has to consider each case on its merits as the frauds are dealt with all severity and state laws are to be meticulously followed.

It is to be noted here that General Manager committee at HO *will be Sanctioning Authority of OTS proposal.*

OTS proposals in fraud accounts, issue of No Dues Certificate and release of security in such accounts will be governed by Recovery Policy.

33.4 Sale of Financial Assets of Doubtful Standard / Fraudulent Origin to Securitization Company (SC)/ Reconstruction Company (RC)

It is to be ensured that while packaging and selling performing or non-performing assets, it is properly ascertained that the pool of assets being sold does not contain any loan originated fraudulently or has been classified as fraud as on the date of sale.

34. Causative Factors and Reporting Obligation

Some of the known symptoms or 'fraud opportunities' are:

a) Lack of awareness of procedures among staff members, customers, etc.

b) At times, lack of awareness of consequences of fraud.

c) Financial Pressures coupled with vices of need & greed.

d) Excessively friendly relationships with fraudsters (internal or external)

e) Temptations from inducing borrowers / others.

f) Delayed detection of frauds and delayed conviction of culprits.

It is obligatory for all staff members of the Bank to report to the superiors, or through the options available through the whistleblower route, known or suspected fraud or 'red flags' or symptoms or indicators of fraud.

35. Prevention of frauds

Following are the important instructions for prevention of frauds.

a) The branches should strictly follow KYC norms while opening deposit as well as loan accounts.

b) Visit borrowers / guarantor's residence / property sites proposed to be purchased and their office / place of business to ascertain their genuineness. Discreet enquiries are to be made to ascertain their credentials and antecedents, information about their loans, if any, availed by them from other branches / Bank / Institutions, etc. at the time of pre-sanction efforts.

c) The branches should make an intelligent scrutiny of the lawyer's report and valuation report instead of solely relying on them.

d) Meaningful and regular checking of alert reports and voucher verification are to be done. The Branch Heads / Region Heads should be held responsible for non-monitoring of checking of such reports.

e) Reconciliation / squaring off System Suspense Account(s) on a regular basis.

f) Staff accounts should be monitored by Branch Head at regular intervals.

g) The capability level permitted to officials in the system should not exceed the powers delegated to them.

h) The fraud prevention and other instructions issued / laid down by DIT and RBI guidelines should be meticulously followed.

i) Caution list(s), Defaulter's list and CIBIL Report, should be referred regularly at the time of sanction of loans, etc.

j) Whistle blowing concept / alertness award scheme should be promoted / encouraged.

k) Password sanctity should be maintained and never be shared among staff members.

36. **Customer and Employee Awareness**

36.1. Customer Awareness

Customer awareness is one of the pillars of fraud prevention. It has been seen that alert customers have enabled prevention of several frauds and in case of frauds, which could not be avoided, helped in bringing the culprit to book by raising timely alerts. The bank should thus aim at continuously educating its customers and solicit their participation in various preventive/detective measures. It is the duty of all the groups in the bank to create fraud risk awareness amongst their respective customers.

The following are some of the recommended measures to create awareness amongst customers:

a) Publications in leading newspapers
b) Detailed 'do's and don'ts' on the web site of the bank
c) Messages along with statement of accounts, either physical or online
d) Messages printed on bank's stationery such as envelopes, card covers, etc.
e) SMS alerts (for debit transactions in the customer account)
f) Message on phone banking when the customer calls
g) As inserts or on the jackets of cheque books
h) Posters in branches and ATM centres

It should be ensured that the communication to the customer is simple and aimed at making them aware of fraud risks and seeking their involvement in taking proper precautions aimed at preventing frauds.

36.2 Employee Awareness

Employee awareness is crucial to fraud prevention. Training on fraud prevention practices should be provided. Bank may use the following methods to create employee awareness:

a) Class room training programmes at the time of induction or during risk related training sessions
b) Publication of newsletters on frauds covering various aspects of frauds and containing important message on fraud prevention from senior functionaries of the Bank
c) E-learning module on fraud prevention

d) Online games based on fraud risks in specific products or processes

e) E-tests on prevention practices and controls

f) Detailed 'do's and don'ts' put up on the worksite of the employee

g) Safety tips flashed at the time of logging into Core Banking System (CBS), screen savers, etc.

h) Emails sent by the respective business heads

i) Posters on various safety measures at the work place

j) Messages/discussions during daily work huddles

---xxxxxxxxxxxxxx---

ANNEXURE I

Early Warning Signals

Some Early Warning signals which should alert the bank officials about some wrong doings in the loan accounts which may turn out to be fraudulent:

1. Default in payment to the banks / sundry debtors and other statutory bodies, etc., bouncing of the high value cheques
2. Under insured or over insured inventory
3. Invoices devoid of TAN and other details
4. Dispute on title of the collateral securities
5. Funds coming from other banks to liquidate the outstanding loan amount
6. Request received from the borrower to postpone the inspection of the godown for flimsy reasons
7. Financing the unit far away from the branch
8. Frequent invocation of BGs and devolvement of LCs
9. Funding of the interest by sanctioning additional facilities
10. Same collateral charged to a number of lenders.
11. Concealment of certain vital documents like master agreement, insurance coverage.
12. Large number of transactions with inter-connected companies and large outstanding from such companies.
13. Significant movements in inventory, disproportionately higher than the growth in turnover.
14. Significant movements in receivables, disproportionately higher than the growth in turnover and I or increase in ageing of the receivables.
15. Disproportionate increase in other current assets.
16. Significant increase in working capital borrowing as percentage of turnover.
17. Critical issues highlighted in the stock audit report.
18. Increase in Fixed Assets, without corresponding increase in turnover (when project is implemented).
19. Increase in borrowings, despite huge cash and cash equivalents in the borrower's balance sheet.
20. Substantial related party transactions.
21. Poor disclosure of materially adverse information and no qualification by the statutory auditors.
22. Frequent change in accounting period and I or accounting policies.
23. Frequent request for general purpose loans.
24. Movement of an account from one bank to another.
25. Frequent ad hoc sanctions.
26. Non- routing of sales proceeds through bank
27. LCs issued for local trade I related party transactions
28. High value RTGS payment to unrelated parties.
29. Heavy cash withdrawal in loan accounts.
30. Non submission of original bills.