Page 1017 - 1027 **DOI:** *https://doij.org/10.10000/IJLMH.113656*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 5 | Issue 5

2022

Anti-Bank Fraud Regime for NPAs in India

VIJAY CHAUHAN[1]

ABSTRACT

The initial purpose of deposit of money by customers in the banking institutions is to get the sense of security and safety alone. Later, the customer expectations gained new dimensions when the banks started to provide numerous facilities to attain the faith of the depositors. With the rise of the banking business, fraud in banks also came to the limelight. Today, fraudsters are not only individuals but the corporate personalities also. These corporate entities are subject to the lifting of the corporate veil, which ultimately helps in the identification of the culprits. Moreover, the possibility of committing fraud arises from the bank, from the customer or by the connivance of either of the two with an outsider. Therefore, several steps have been taken to address this mounting concern, including the enactment of the Insolvency and Bankruptcy Code 2016. However, this article tries to find out the Anti-Bank fraud regime for such bad loans, which have recently been transformed into fraud committed by corporate entities. The authors have relied on primary and secondary sources of data collection. The primary sources include laws, ordinances, regulations, circulars and various reports (if needed) of panels of experts and cases decided by the courts. Secondary sources include books, commentaries, dictionaries, encyclopaedias, legal reports, magazines, the Internet and newspapers.

I. INTRODUCTION

The methodologies and practises used in Indian banking have undergone a paradigm shift since the second half of the 20th century. The new economic strategy's measures of globalisation, privatisation, and liberalisation had a significant impact on the Indian banking industry. As part of the ongoing reformation process, deregulation has given banks new opportunities to diversify their business portfolios. It has also made a wide range of services available to customers. Customers can now not only store their money in banks for safekeeping, but also enjoy unheard-of services. This transformational process, which enabled the banks to provide a range of services, transformed the way that banking organisations previously worked. The characteristics of financial organisations have altered as a result of service accessibility, the provision of flexible deposit plans, and the liberalised use of operational flexibility.

By utilising the tremendous opportunity and potential, Indian banking institutions have

[1] Author is a LL.M. student at Galgotias University, Greater Noida, India.

 [ISSN 2581-5369]

successfully overcame all challenges to support all economic sectors financially and can now take the initiative to drive the country's competitiveness on the global stage. However, in the absence of effective management, the entire respiratory system as well as the defence mechanism deteriorate the entire system against disease. Banking frauds, to put it simply, are a warning indication of a weakened banking sector that is not responding to corrective actions and poses a serious threat to the stability of the financial system. This is why RBI has prescribed some of the preventive and curative measure, which are discussed further in this chapter.

II. PREVENTION AND DETECTION

Every banking organisation or business either commits fraud or is vulnerable to it. Fraud can result in substantial investment losses as well as a loss of confidence in the capital markets, which eventually causes banking institutions to fail. With the development of banking technology, frauds had a terrifying tendency to grow, which diminished the public's trust in financial institutions as safe havens for deposits and investments. The banks established the "Fraud Risk Management Process" to identify sensitive fraud areas and put in place efficient defences. One of the definite proven reasons of fraud is ignorance of the bank. Therefore, the best preventative technique would be the active staff understanding of the systems and procedures, and when frauds have been committed by outsiders, corrective action must be done to safeguard the Bank's interests. Where employees have knowingly committed fraud, disciplinary procedures must be used as a form of punishment. As a deterrent, certain acts are taken. Although "cure" should always be kept on hand in case of an emergency, "prevention" is still preferred over "treatment" even in the twenty-first century.

(A) EARLY WARNING SIGNS AND RED FLAGGED ACCOUNTS

The concept of accounts with red flag i.e. RFA has its implementation in the today's framework as a critical step in lowering the risk of fraud. When there is an RFA, it means that there are one or more Early Warning Signals that point to possible fraudulent activity (EWS). [2]The bank must be immediately notified of any flaws or misconduct in a loan account that could later turn out to be fraudulent by these warning flags[3].

(B) EARLY DETECTION AND REPORTING OF SUCH ACCOUNTS

A report on the RFA accounts, including, among other things, a summary of the corrective steps

[2] RBI introduces 'red flag' to clamp down on loan frauds, INDIAN EXPRESS, https://indianexpress.com/article/business/business-others/rbi-introduces-red-flag-to-clamp-down-on-loanfrauds/ (Last visited on Aug 14 2022].

[3] Reserve Bank of India, Master Directions on Frauds – Classification and Reporting by commercial banks and select FIs, RBI/DBS/2016-17/28, DBS.CO.CFMC.BC.No.1/23.04.001/2016-17 (Issued on July 01, 2016). See; Master direction 8.3, Chapter VIII.

 [ISSN 2581-5369]

taken and their current status, will be given to the Special Committee of the Board for monitoring and follow-up of Frauds (SCBF)[4]. Currently, fraud detection takes an unreasonably long time. Banks often don't report a bogus account until all other recovery options have been exhausted. Delays in reporting frauds, among other things, prohibit the RBI from issuing Caution Advice/ CFRs to other banks about the modus operandi, which can discourage other banks from disclosing frauds of a similar sort. More importantly, it hinders law enforcement from prosecuting dishonest borrowers, which has a detrimental impact on elements of recoverability and increases the damage brought on by fraud. The simplest method for preventing fraud on loan accounts is for banks to maintain a solid evaluation and a trustworthy credit monitoring system over the course of the loan account[5]. Any shortcomings that might have gone undiscovered during the evaluation process can frequently be mitigated if the post-disbursement monitoring is still successful. In order to strengthen the monitoring systems, it is advised that the following inspections and investigations be conducted at different stages of the loan life cycle based on a study of the banks' collective experience.

i. Pre-approval:

As part of the credit process, The Risk Management Group (RMG) or another appropriate bank group collects market intelligence and unbiased data about potential borrowers from the public domain, including information on their background, involvement in legal issues, and business raids, restrictions imposed on them by governmental agencies, validation of sui generis information, and other factors. Banks are required to keep a record of these presanction assessments as part of the sanction record.

ii. Dispersion

The focus of RMG's audits at the payout stage should, among other things, be on ensuring that the terms and conditions of the sanction are being followed, the rationale for approving a weakened these terms and conditions, the extent of such dilutions, etc. The general rules established by the Board in this regard must be completely followed by the dilutions. A collection of terms and conditions may be designated as "core" by the sanctioning body and should not be changed. When core requirements are not being observed, the RMG may immediately notify the sanctioning authority.

[4] Reserve bank of India, Master Directions on Frauds – Classification and Reporting by commercial banks and select FIs, RBI/DBS/2016-17/28, DBS.CO.CFMC.BC.No.1/23.04.001/2016-17 (Issued on July 01, 2016). See; Master direction 8.4, Chapter VIII.

[5] Reserve bank of India, Master Directions on Frauds – Classification and Reporting by commercial banks and select FIs, RBI/DBS/2016-17/28, DBS.CO.CFMC.BC.No.1/23.04.001/2016-17 (Issued on July 01, 2016). See; Master direction 8.4.2, Chapter VIII.

 [ISSN 2581-5369]

iii. Annual review:

While EWS tracking should be used to continuously monitor an account, banks should also keep an eye out for fraud during these evaluations. At the time of review, it is necessary to talk about issues such money being taken from an account, having enough stock compared to stock statements, stress in group accounts, etc. The RMG should also be able to track market developments involving the bank's major customers and make suggestions to the credit officers. This would include gathering rumours, monitoring stock market trends, purchasing a press clippings subscription, regularly reviewing databases, and not only focusing on the borrowing entity but the entire group in the exercise.

(C) EMPLOYEE EMPOWERMENT AND ACCOUNTABILITY

According to the bank's whistleblower policy, employees should be motivated to inform the appropriate authorities about fraudulent activity in an account so that they can initiate an investigation utilising the FMG (Fraud Monitoring Group) and the relevant documentation.[6] In order to obtain the information it need, the FMG may "hear" the involved employee. Such employees ought to be covered by the bank's whistleblower policy in order to prevent the possibility of reprisal from acting as a deterrent.[7]

The role of the sanctioning official(s) may, where deemed appropriate or essential, also be covered by this exercise. The SCBF must be informed of the findings of the staff accountability exercise for frauds, as well as any follow-up steps, using the FMR.

All fraud instances may be divided by banks into vigilance and non-vigilance categories. The investigating authorities should only be notified in situations needing monitoring. Cases of non-vigilance may be looked into and dealt with at the bank level in a six-month period[8]. During an audit, auditors might find instances where the account's transactions or the records indicate that the account may have had fraudulent transactions. The auditor must quickly notify top management of such an event so that the proper course of action can be implemented.[9]

---

[6] Reserve bank of India, Master Directions on Frauds – Classification and Reporting by commercial banks and select FIs, RBI/DBS/2016-17/28, DBS.CO.CFMC.BC.No.1/23.04.001/2016-17 (Issued on July 01, 2016). See; Master direction 8.5, chapter VIII.

[7] RBI asks banks to install detection systems to check frauds, THE ECONOMIC TIMES, https://economictimes.indiatimes.com/news/economy/policy/rbi-asks-banks-to-install-detection-systems-tocheck-frauds/articleshow/47202515.cms (Last visited on August 14, 2022).

[8] Reserve bank of India, Master Directions on Frauds – Classification and Reporting by commercial banks and select FIs, RBI/DBS/2016-17/28, DBS.CO.CFMC.BC.No.1/23.04.001/2016-17 (Issued on July 01, 2016). See; Para 8.10.2, Chapter VIII.

[9] Reserve bank of India, Master Directions on Frauds – Classification and Reporting by commercial banks and select FIs, RBI/DBS/2016-17/28, DBS.CO.CFMC.BC.No.1/23.04.001/2016-17 (Issued on July 01, 2016). See; Master direction 8.6, Chapter VIII.

 [ISSN 2581-5369]

(D) WHEN A BANK ACTS AS THE EXCLUSIVE OR SOLE LENDER.

The FMG (Fraud monitoring group) will determine whether or not to label an account where EWS are discovered as RFA when the bank is the only lender. This process needs to be finished as soon as is practical, ideally within a month of the EWS being identified. The FMG will outline, within a time frame no more than six months[10], the kind and scope of any investigations or corrective actions necessary to protect the bank's interest if the account is identified as RFA.

The bank may seek advice from a team of internal investigators or external auditors, including forensic experts, before making a final decision regarding the RFA. After this time, which cannot exceed six months, banking institution must either remove the red flagged status or announce such profile to be sham. An assessment report on the red flagged profiles should be sent to the SCBF (Special Committee of the Board for monitoring and follow up of cases of frauds) together with the FMG's observations and conclusions. The report should include a description of the EWS and abnormalities that were discovered in the account, as well as a summary of the inquiries that were ordered and the corrective measures that the FMG recommended, as well as an update on how those measures are progressing.

(E) IN THE CASE OF A CONSORTIUM OF BANKS OR NUMEROUS LENDING ARRANGEMENTS

Some dishonest borrowers using "multiple banking arrangements"[11] continue to take use of the granting facilities of other banking institution and, in particular cases, receive the increased limits at other banks after defrauding one of the financing banks. This is because of the reason of the lack of an organised system for exchange of information among different lending banks and financial institutions. In particular fraud cases, the borrowers secured their same assets/securities to other institutions.

Thus, in order to pursue legal or criminal action, assessment (before and after granting of loan) for recovery, exchanging information on mode of operation, and to achieve uniformity in data and information collection on frauds reported to the Reserve Bank of India, all banks that have provided financing to a borrower under a "multiple banking" arrangement should act jointly based on a mutually agreed-upon strategy. Because of this, the first bank to discover of a fraud must immediately alert the other banks in the different financial arrangements. Individual banks

[10] Reserve bank of India, Master Directions on Frauds – Classification and Reporting by commercial banks and select FIs, RBI/DBS/2016-17/28, DBS.CO.CFMC.BC.No.1/23.04.001/2016-17 (Issued on July 01, 2016). See; Para 8.8.1, Chapter VIII.

[11] Aishwarya, Banking Consortium And It's Legal Aspects - Financial Services, MONDAQ (2020), available at https://www.mondaq.com/india/financial-services/965138/banking-consortium-and-it39s-legal-aspects

 [ISSN 2581-5369]

participating in the consortium or group agreements are required to use their own due diligence. It should be conducted before incurring any default risk related to credit and to independently and critically monitor the usage of money rather than relying solely on the leader of group or consortium. However, the consortium may work out the intricacies and accurately document them with regard to escrow account monitoring so that accountability may be promptly demonstrated in the future. Like in the past, any substantial fraud-related issues should also be quickly disclosed with other consortia / numerous banking lenders if they are discovered during annual evaluations or through the monitoring of early warning signals. Exercise due care, for instance, by creating Standard Operating Processes with checklists for the operating functionaries to follow, updating any printed manuals, and training staff to strictly adhere to such procedures.

Any normal or NPA account will first be categorised at the individual bank level as RFA or Fraud. It is the obligation of such bank to disclose the account's red flagged status on the CRILC platform in order to alert other banks. If the specific bank decides to classify the account as fraudulent at this point, it must notify RBI of the fraud within a period of 21 days of discovery and then submit the matter to the Police or CBI, as it did in the past.[12] Additionally, within 15 days period after the fraud classification or RFA categorisation, the bank that raised a red flag on the loan account or identified the fraud would ask the leader of the consortium to conduct a meet up of the JLF to assess the situation. Such a JLF meeting shall be held within fifteen (15) days after receipt of such request.[13] The account should be classified as fraudulent if there is widespread agreement; otherwise, the loan account must be tagged by all banks and later on subjected to an audit (forensic) that is initiated or ordered by the head of consortium. Each bank must cover the expenses and shall provide the required aid for such an investigative procedure as a member of the consortium or multiple banking arrangement.

The forensic audit shall be completed within three months of the JLF meet that approved the audit. But, within a period of 15 days of the conclusion of audit, JLF must re-join to establish the loan account's status, by consensus or by using the majority rule. Within one week of the decision to label the loan account as fraudulent, the red flagged status must be changed to 'Fraud' in all banks then it must also be disclosed to RBI, and displayed at the CRILC forum. Additionally, within thirty (30) days of disclosing the matter to RBI, the bank ordering or initiating the audit must file a written complaint to the CBI as a representative of all banks in

[12] Reserve bank of India, Master Directions on Frauds – Classification and Reporting by commercial banks and select FIs, RBI/DBS/2016-17/28, DBS.CO.CFMC.BC.No.1/23.04.001/2016-17 (Issued on July 01, 2016). See; Master Direction 8.9, chapter VIII.
[13] Ibid

 [ISSN 2581-5369]

the MBA or consortium.

III. REPORTING MECHANISM

Banks should be driven by the interests of public and the requirement of ensuring that the guilty parties are held accountable when dealing with fraud or embezzlement situations, in addition to the need to quickly recover the sum at issue.

(A) POLICE/CBI FRAUD REPORTING

All fraud instances involving bank employees that are less than Rs. 10,000 shall be reported to the head institution of the bank in a region, who will investigate the case and advise the affected institutional branch on whether to submit it to the local police station for further legal action.[14]

As a result, the following situations[15] should always be reported to the State Police or the CBI, as shown below;

Category of bank	Amount involved in the fraud	Agency to whom complaint should be lodged	Remarks
Private Sector/ Foreign Banks	₹ 10000 and above	State Police	If committed by staff
	₹ 0.1 million and above	State Police	If committed by outsiders on their own and/or with the connivance of bank staff/officers.
	₹ 10 million and above	In addition to State Police, SFIO, Ministry of Corporate Affairs, Government of India. Second Floor, Paryavaran Bhavan, CGO Complex, Lodhi Road, New Delhi 110 003.	Details of the fraud are to be reported to SFIO in FMR Format.
Public Sector Banks	Below ₹ 30 million 1. ₹ 10,000/- and above but below ₹ 0.1 million	State Police	If committed by staff.[2]
	2. ₹ 0.1 million and above but below ₹ 30 million	To the State CID/Economic Offences Wing of the State concerned	To be lodged by the Regional Head of the bank concerned
	₹ 30 million and above and up to ₹ 250 million	CBI	To be lodged with Anti Corruption Branch of CBI (where staff involvement is prima facie evident) Economic Offences Wing of CBI (where staff involvement is prima facie not evident)
	More than ₹ 250 million and up to ₹ 500 million	CBI	To be lodged with Banking Security and Fraud Cell (BSFC) of CBI (irrespective of the involvement of a public servant)
	More than ₹ 500 million	CBI	To be lodged with the Joint Director (Policy) CBI, HQ New Delhi

(B) REPORTING TO RBI

Banks must electronically submit Fraud Monitoring Returns (FMR) for each specific fraud

[14] Reserve bank of India, Master Directions on Frauds – Classification and Reporting by commercial banks and select FIs, RBI/DBS/2016-17/28, DBS.CO.CFMC.BC.No.1/23.04.001/2016-17 (Issued on July 01, 2016). See; Master Direction 6, Chapter VI.

[15] Chart. Available at; https://m.rbi.org.in/scripts/BS_ViewMasDirections.aspx?id=10477#11

incident to the RBI using the FMR Application (in XBRL system) that was issued to them within a period of three weeks of the detection, regardless of the amount of money at risk. The bank must submit a monthly certificate in accordance with Annex I to CFMC, Bengaluru, within seven days at the end of the month. A copy must be given to each SSM in the bank (noting that a soft copy of each FMR has been provided to RBI). Fraud reports shall also be provided in situations where central investigative agencies have started criminal proceedings on their own and/or the RBI has ordered that such incidents be disclosed as frauds.

For frauds perpetrated by their joint ventures, affiliates, and subsidiaries, banks may also file FMR reports in paper copy alone. If the subsidiary, affiliate, or joint venture is an entity governed or regulated by the RBI and is directly required to report the matters related to fraud to RBI in accordance with guidelines operative on that subsidiary, affiliate, or joint venture, the parent bank is not required to provide the printed statement of the FMR sheet in relation to fraud cases discovered at such subsidiary, affiliate, or joint venture. All banks are required to notify the RBI of any frauds carried out at their international branches or offices (other than foreign banks).

If the fraud involves Rs. 50 million or more, banks are additionally required to submit a Flash Report (FR) within a week of the scam being known to the institution's main office. The flash report should be provided in the form of a DO letter with a copy to the CFMC in Bengaluru and an address for the PCGM/CGM-in-Charge, DBS, RBI, Central Office, Mumbai. The officials from each bank and financial institution who are in responsibility of reporting fraud and other crimes would be listed by the Central Fraud Monitoring Cell (CFMC), which is located in the Department of Banking Supervision's Central Office in Bengaluru. Banks should make sure that all matters of frauds totaling $0.1 million or more are immediately disclosed to their boards after being discovered[16]. In such reports, negligence on behalf of the competent branch officials and the central authorities should be noted, among other things, and information of the actions taken against the fraud-related officials should be provided.

IV. VIGILANCE

In response to the suggestions provided by the Committee on Prevention of Corruption or Santhanam Committee[17], the Government of India established the Central Vigilance

[16] Reserve bank of India, Master Directions on Frauds – Classification and Reporting by commercial banks and select FIs, RBI/DBS/2016-17/28, DBS.CO.CFMC.BC.No.1/23.04.001/2016-17 (Issued on July 01, 2016). See; Para 3.2, Chapter III.

[17] Central Vigilance Commission, Report of the Committee on Prevention of Corruption (Ministry of Home Affairs). Available at; https://cvc.gov.in/sites/default/files/scr_rpt_cvc.pdf

 [ISSN 2581-5369]

Commission by a resolution on 11.2.1964. Additionally, the CVO was given statutory character with effect from 25.8.1998 with the help of the "The Central Vigilance Commission Ordinance, 1998," in accordance to the directives of the Hon'ble SC in the matter of *Vineet Narain vs. Union of India*[18]. While the CVC Bill was being considered by the Parliament, it was somehow backed by the CVC (Amendment) Ordinance of October 27, 1999, the CVC Ordinance of November 8, 1999. Then the bill was subsequently approved by both the Houses in 2003, and the Indian President granted his approval on September 11th of that same year. As a result, starting on that day, the Central Vigilance Commission Act, 2003 (No. 45 of 2003) went into effect.

The Chairperson (Central Vigilance Commissioner) and not more than two Vigilance Commissioners shall constitute the Commission in accordance with the requirements of Sections 3 and 4 of the CVC Act, 2003. The President appoints the Central Vigilance Commissioner & the Vigilance Commissioners through a warrant affixed with his seal for a period of four (4) years beginning on the day they take office or until they reach the age of sixty-five, whichever comes first. A Secretary who is chosen by the Central Government assists the Commission.

The Chief Vigilance Officer (CVO), who oversees the organization's vigilance section, advises the organisation and its executive on all matters related to vigilance. Additionally, he creates a connecting chain between his group and the Central Vigilance Commission and the CBI. The CVO's vigilance responsibilities are extensive and include gathering information about corrupt practises used by, or likely to be used by, employees of his organisation; investigating verifiable allegations made to him; processing investigation reports for the disciplinary authority in question to consider; and, as necessary, referring the situation to the Commission for guidance. As a result, the CVO's responsibilities can be loosely divided into three groups: I. Punitive vigilance; II. Preventive and proactive vigilance; and III.

Surveillance and detection.

(A) VIGILANCE ANGLE WITH RESPECT TO BANKS:

As it is in every organisation, management in financial institutions must include vigilance work. By taking such action, the organization's level of managerial effectiveness and efficiency is being increased rather than decreased. In banking institutions, taking risks is an essential part of doing business.[19] Therefore, a vigilance inquiry does not necessarily need to concentrate on every loss experienced by the company, whether it be financial or otherwise. Disregarding

[18] Vineet Narain vs. Union of India, (1996) 2 SCC 199

[19] Reserve Bank of India, The RBI Master Circular on 'Frauds-Classification and Reporting, RBI/2012-13/59 UBD.CO.BPD.MC.No.17/12.05.001/2012-13 (Issued on July 02, 2012).

 [ISSN 2581-5369]

motivated or negligent decisions that have jeopardised the organization's goals would be harsh, nevertheless.

Therefore, it is important to distinguish between a business loss brought on by a wise business decision and an extreme loss brought on by any dishonest, selfish, or sloppy task performance. While the former must be seen adversely and dealt with in line with the present disciplinary procedures, the latter must be treated as a routine component of business and ignored from the perspective of vigilance. If a reasonable person acting within the confines of the specified rules, regulations, and instructions would have taken the decision under the circumstances in the commercial interests of the organisation, that is one relevant condition for proving the case's legitimacy.

An yes answer to this question may imply the presence of bonafides. A negative answer, on the other hand, might imply that they aren't there. As a result, a vigilance investigation into a complaint based on a minor difference in perspective or perception, a small error in judgement, a lack of effectiveness, or a failure to complete assignments with exceptional devotion would not be required[77]. Such failures may cause the organisation serious issues, but not from a vigilance perspective. They require distinct treatment..

In addition, the following behaviours[20] blatantly show a lack of attention to detail:

- Demanding or accepting payment other than justifiable wages in exchange for fulfilling official responsibilities or using his position or influence to gain favour with another official
- Acquiring costly items from a person with whom he has or is likely to have official transactions, his subordinates have official interactions, or where he can wield influence, without due care or without proper consideration.
- Using unethical or unlawful means, or abusing his authority as a public servant, to gain something of value or a financial benefit for himself or for anybody else.
- Possessing assets that are excessive compared to his established sources of income
- Incidents involving theft, forgery, fraud, or other similar offences.

(B) CVO AND BANKS:

The Commission has mandated that every banking institution has to set up an IAC (Internal advisory committee) of three (3) members in which the members are preferred to have the rank of General Managers and not below the rank of Deputy General Managers, to investigate

[20] Central Vigilance Commission, Vigilance angle – definition of (partial modification regarding), Office Order No.74/12/05 (Issued on December 21, 2005).

received complaints at the bank as well as cases arising from routine inspections, audits, and staff accountability issues, etc., and to determine whether or not angle of vigilance was to be applied to those transactions. The Committee shall set forth its findings and conclusions in writing. The committee's recommendations will be given to the CVO. The CVO will consider the recommendations of the Committee before deciding on each matter. When the Commission visits the bank for the purpose of a vigilance audit, an officer or team of officers will have access to these records, which the CVO is responsible for maintaining.

The committee will always vote unanimously on whether or not to include the vigilance angle. The position held by the majority of the members may be communicated if there is disagreement. The CVO would communicate its suggestions to the DA. Concerning any officials who do not fall under the purview of the Commission, the issue should first be brought up with the CMD/MD&CEO in the event of a disagreement between the DA and the CVO. If the dispute persists, it can be sent to the Commission to be decided by it.

*****

 [ISSN 2581-5369]