A Research Paper on MISAPPROPRIATION OF BANKING IN INDIA

Dr. Anil Ramteke

G.S. College of Commerce , Wardha Mob. No. 9834635155 / 9673688068

Abstract

The Reserve Bank of India, not to be left behind, played its part in this transformational journey, by issuing regulations and recommendations on banking mechanization and computerization. Financial sector in general and banking industry in Particular is the largest spender and beneficiary from information technology. According to John Finnerty, "Financial Innovation involves the design, the development, and the implementation of innovative financial instruments and processes, and the formulation of creative solutions to problems in finance". The various innovations in banking and financial sector are ECS, RTGS, EFT,

Keywords: Misappropriation, fraud, banking Debit, kycATM, RTGS

NEFT, white label ATM, green channel counter Retail Banking, Debit & Credit cards, free advisory services, implementation of standing instructions of customers, payments of utility bills, fund transfers, internet banking, telephone banking, mobile banking, selling insurance products, issue of free cheque books, travel cheques and many more value added services. Customers in urban India no longer want to wait in long queues and spend hours in banking transactions. This change in customer attitude has gone hand in hand with the development of ATMs, Mobile phone and net banking along with availability of service right at the customer's doorstep. With the emergence of universal banking, banks aim to provide all banking product and service offering under one roof and their endeavor is to be customer centric. While banks are striving to strengthen customer relationship and move towards 'relationship banking,' customers are increasingly moving away from the confines of traditional branch banking and seeking the convenience of remote electronic banking. Information technology and the communications networking systems have revolutionaries the working of banks and financial entities all over the world.

In the context of banking business, 'Bank Fraud' is defined in the Report of Reserve Bank of India (RBI) Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds , 2011 which reads: 'A deliberate act of omission or commission by any person, carried out in the course of a banking transaction or in the books of accounts maintained manually or under computer system in banks, resulting into wrongful gain to any person for a temporary period or otherwise, with or without any monetary loss to the bank.

RBI made it mandatory for scheduled commercial banks (SCBs) to report fraud cases way back in July 1970. In 2005-06, such reporting was extended to urban co-operative banks (UCBs) and deposit taking Non-Banking Financial Companies (NBFCs), registered with RBI. In March 2012, NBFC-NDSIs (systemically important, non-deposit taking NBFCs) having an asset base of Rs. 100 crore and above were also brought under the reporting requirements. According to the data given by RBI in response to an RTI query as on June 13, 2019, of the total 53,334 cases of frauds reported during 2008-09 and 2018-19 fiscal years, involving a whopping Rs 2.05 lakh crore, the highest of 6,811 were reported by the ICICI Bank involving Rs 5,033.81 crore .The state-run State Bank of India (SBI) reported 6,793 fraud cases involving Rs 23,734.74 crore, followed by HDFC Banks which recorded 2,497 such cases involving Rs 1,200.79 crore. Further analysis of fraud related data suggests that, a quantum jump in the amount involved in frauds during 2017-18 was on account of a large-value fraud committed in the gems and jewelry sector, mainly affecting Punjab National Bank. Further, during 2017-18, public sector banks (PSBs) accounted for 92.9 per cent of the amount involved in frauds of more than Rs.1 lakh, as reported to the Reserve Bank; private sector banks accounted for 6 per cent. Public Sector Banks (PSBs) also accounted for about 85 per cent of the cumulative amount involved in frauds during 2017-18 and, private sector banks accounted for a little over 10 per cent. At the system level, frauds in loans, by amount, accounted for more than 75 per cent of frauds involving amounts of Rs.1 lakh and above, while the number of frauds in deposit accounts was at just over 3 per cent. Within the loan category of frauds, PSBs accounted for a major share (87 per cent) followed by the private sector banks (11 per cent).The share of PSBs in frauds relating to 'off-balance sheet items' such as Letter of Credit, Letter of Undertaking, and Letter of Acceptance was higher, at 96 per cent. Of the seven classifications of fraud in alignment with the Indian Penal Code, 'cheating and forgery' was the major component, followed by 'misappropriation and criminal breach of trust'. In 'cheating and forgery' cases, the most common modus operandi was multiple mortgage and forged documents. Further, Mumbai (Greater Mumbai), Kolkata and Delhi were the top three cities in reporting of bank frauds under 'cheating and forgery' category. In respect of staff involvement in frauds, banks reported that it was prominent in the categories 'cash' and 'deposits', though these together had a much smaller share in the overall number of fraud incidents and the amount involved(3).Due to increasing number of frauds, banks reported a total loss of about Rs 70,000 crore during the last three fiscals up to March 2018. The extent of loss in fraud cases reported by scheduled commercial banks (SCBs) for the last three years stood at 16,409 16,652 and 36,694 as on March end, 201516, 2016-17and 2017-18 respectively. While the bulk of banking frauds was loan-related, it is observed that there has been a significant jump in card and internet banking related frauds during 2017-18. A total of 972 such incidents were reported in 2017-18, roughly three per day. The banking sector lost a total of Rs 168.74 crore to organised crimes directed at ATMs in the past three years. With a lot of essential financial services shifting to the digital space, the number of frauds targeting online transactions has also increased. In 2017-18, a total of 911 frauds were committed using debit and credit cards. The sum total of money that went into the wrong hands stands at Rs 65.26 crore.

Reasons of Bank Misappropriation

A study conducted at IIM Bengaluru identifies causes of bank frauds. Accordingly, bank frauds are primarily due to lack of adequate supervision of the top management; collusion between the staff, corporate borrowers and third party agencies; weak regulatory system; lack of appropriate tools and technologies in place to detect early warning signals of a fraud; lack of awareness of bank employees and customers; and lack of coordination among different banks across India and abroad. Further, delays in legal procedures for reporting, and various loopholes in system are the reasons of frauds. Also, lack of specialized forensic audit as well as a good legal understanding of frauds is one of the reasons. For detection and prevention of bank frauds, it is necessary to understand about the modus operandi of frauds.

Modus of Operandi of Frauds

Bank frauds can be divided into three main sub-groups related to: Technology, Advances and KYC (mainly in deposit accounts). Nearly, 65 percent of total fraud cases were technology related covering frauds committed through /at interne banking channel, ATMs and other alternate payment channels like credit/ debit/prepaid cards. Frauds related to deposits are relatively less in number and in value. But, the frauds in advances portfolio accounted for a major proportion (64%) of the total amount involved in frauds. Relatively speaking, large value advances related frauds (>Rs. 1 crore) have increased both in terms of number and amount involved over the years. Modus operandi in these frauds and preventive &mitigation strategies are discussed as under :

(1) Technology Related Frauds

The cumulative total of number of cases and the amount involved in technology related frauds as at March end, 2013 stood at 1,11,655 and Rs. 357.33 crore respectively. Though the average amount involved in frauds is less than Rs.31,000, banks should be constantly on the guard to provide a secure environment for customers to conduct banking transactions. While banks' customers have now become tech-savvy and started using online banking services and products, fraudsters are devising newer ways of perpetrating frauds by exploiting the loopholes in technology systems and processes. Fraudsters have employed hostile software programs or malware attacks, phishing, Vishing (voicemail), SMS is hing (text messages) and Whaling (targeted phishing on high net worth Individuals) techniques apart from stealing confidential data to perpetrate frauds. With cyber-attack becoming more frequent, the RBI has advised banks in February 2013 to introduce certain minimum checks and balances like introduction of two factor authentication in case of 'card not present transactions, converting all strip based cards to chip based cards for better security, issuing debit and credit cards only for domestic usage unless soughtspecifically by the customer, putting threshold limit on international usage of debit/ credit cards, constant review of the Pattern of card transactions in coordination with customers, sending SMS alerts in respect of card transactions etc. to minimize the impact of such attacks on banks as well as customers. Regarding the electronic modes of payment like NEFT and RTGS, it is the responsibility of the user to ensure that his unique ID and password are properly secured and do not get misused due to his laxity. And, banks, on their part, should also ensure that these payment channels are safe and secure. Towards this end, RBI has advised banks to introduce preventive measures such as putting a cap on the value/number of beneficiaries, introducing system of issuing alert on inclusion of additional beneficiary, velocity checks on number of transactions effected per day/per beneficiary, considering introduction of digital signature for large value payments, capturing internet protocol check as an additional validation check for any transaction, etc.

Regarding duplicate debit/ credit cards, banks need to improve the peripheral and system security in ATM locations and, at the same time, educate their customers about using their payment cards with due caution. Similarly, cases of circulation of fraudulent e-mails and SMS messages conveying winning of prize money have become matter of a concern in recent times. Many a times, innocent people fall prey to such e-mails and pay money in designated accounts, which is then quickly siphoned off through ATMs located in far flung areas of the country. For this purpose, the fraudsters generally use deposit accounts in banks with lax KYC drills or accounts which remain inoperative for long. Banks, therefore, not only need to caution their customers to guard against such temptations for easy money. In fact, inadequacy of KYC drill would render any subsequent investigation process meaningless. RBI, as a part of its financial literacy programme, constantly seeks to caution the general public through print media, electronic media and on its web-site not to get enamored by the false promises made in such e-mails. Apart from enlisting active co-operation from their technology vendors, banks must look to build a close rapport with other banks, investigative agencies and regulators to ensure that there is prompt and coordinated exchange of information, whenever required. With the spread of mobile banking, banks would need to closely engage with the telecom service providers for reducing the technology related fraud risk. Banks could also consider seeking insurance coverage as a risk transfer tool and a mitigate for the financial losses arising from technology induced fraudulent customer transactions.

(2) Advances Related Frauds

Majority of the credit related frauds are on account of deficient appraisal system, poor post-disbursement supervision and inadequate follow up. In this regard, RBI in its circular of August 07, 2004highlighted major deficiencies observed in credit area which shall lead to frauds. These are observed at both at sanction and post sanction stage. At the sanction stage, there are major deficiencies noticed. For Instance, sanctions are made deviating from the laid down policy / lending norms. Ad-hoc limits are sanctioned frequently even if the company has regular limits and, the same are running irregularly. Credit limits are sanctioned by branch/Zonal Office/Central Office level functionaries in excess of their delegated powers. The sanctioning authorities overlook the irregularities pointed out by the lower level functionaries in the borrowal account. The sanctioning authorities are not given full facts about the borrowers and the project by the officials in controlling office/branch. Sanctioning authorities overlook the fact at the time of takeover of accounts that the borrowing company has irregular accounts with the previous bank/s. There have been instances where some of professionals like chartered accountants, valuers and advocates involved in the loan assessment and, sanctioning processes have also facilitated the perpetration of frauds by colluding with the borrowers to fabricate fudged financial statements, inflated security valuation reports and defective search reports for title deeds of mortgaged property based on which banks have been led to overestimate the funding requirements and security cover for the same. Cases of multiple financing against the same security are also observed. In the same way, there are major deficiencies at post-sanction stage. For instance, the terms and conditions prescribed at the time of sanction of loan facilities are subsequently relaxed without justification by the sanctioning authorities themselves while disbursing funds. In respect of high valued advances, cases of diversion of funds are not reported to the bank's Board for their information and action in the matter. As regards working capital limits, failure to detect disappearance of stock given as security has resulted into misappropriation of funds/sale of stock and receivables without the knowledge of banks. Further, there could be failure to ensure adequacy of the security offered by the borrowers, and to verify whether the same asset is mortgaged to another bank. Periodical review of accounts is not undertaken after the funds are lent by the banks. Excess drawings, permitted by the branch/Regional Office level functionaries in the borrowal accounts, are ratified by the Head Office in a routine manner without examining the need for such permissions, at times, frequently. Lastly, limits sanctioned are allowed to be interchanged indiscriminately by the branch officials without proper authority.

For prevention of frauds in credit area, Certain measures are suggested. To mention few of them, in cases of diversion of funds, the lending bank should obtain a certificate from the borrowers on a quarterly basis furnishing details of accounts opened with other banks. Generally, banks rely on the certificates of valuation given by the external valuers which in some cases are found to have shown grossly inflated values. It is, therefore, suggested that banks shall set up of independent 'Valuation Cell' within banks themselves.. Immediate action should be taken where the malafide /gross negligence on the part of dealing officials are noticed. Wherever there is a prima-facie case against the dealing officials, appropriate action in terms of CVC guidelines for their inclusion in the list of officers with doubtful integrity, should be initiated by banks in consultation with the CBI. Banks should evolve a process of check listing which enables them to examine any deficiencies while releasing the funds to the borrowers or monitoring the end use of funds. Lastly, there is a need for building up a cadre of officials with proper educational background and training to take care of larger projects financed by the banks.

(3) Frauds related to Deposits

There are several ways of perpetrating frauds in deposits area. These include: opening of new fictitious deposit accounts by persons not properly identified by the bank followed by depositing of fake/stolen/forged instruments in such accounts and then withdrawing proceeds, manipulation in inward/outward clearing, by passing unauthorized entries in the books accounts, giving free access to unidentified so called middlemen/ agents of the original depositor and withdrawing the amount, debiting impersonal accounts such as Imprest Clearing Account/ Suspense account, laxity in the safe custody of critical stationary etc. In these regards, banks should ensure that deposit accounts maintained with them are fully KYC compliant. Newly opened accounts with unusual banking operation should be under check. Further, timely rectification of entries in Suspense Accounts, and Reconciliation of entries in Clearing Adjusted Account should be ensured, adequate safeguards should be in place in respects of TTs, DDs and Pay Orders. Operations in dormant accounts should be under watch. The banks should also have a system of generating alerts to monitor transactions in accounts which are inoperative for long or where transactions are not in conformity with general trend and customer risk profile

Suggestions

1) The government shall consider an independent specialized cadre of officers in banks who are capable of carrying out an effective and time bound investigation of such scams. In respect of mega frauds and technology based frauds, this arrangement is needed. For this purpose, selection of such officers shall be on the lines of recruitment of IAS/ IES officers. But, in short term, the government shall consider forming this cadre with a pool of commercial bankers, RBI and CBI officials through lateral recruitment. Further, there should be a dedicated department/cell in banks equipped with legal assistance which serves as a single point of contact with investigating agencies and facilitates easy access to relevant documents.

2) There needs to be effective coordination between banks and agencies such as the Central Board of Direct Taxes (CBDT) to share vital information on personal wealth of promoters. In case of any information that may raise a red flag, the CVC and the RBI should jointly investigate the promoters for fraudulent activities..

3) Banks have to ensure corporate governance at the highest levels. The top management needs to set guidelines and policies for ethical practices and standard procedures to maintain zero tolerance to negligence and fraudulent activities.

4) Various types of audits are _undertaken by banks such as statutory audit, risk-based internal audit, concurrent audit, information systems audit and special audits. These need to be tightened for the purpose of obtaining early warning signals of frauds. In particular, the concurrent audit has to be carried out on a real-time, or near-real time basis.

5) There is a need to improve exchange of information between all stakeholders to instill and maintain financial discipline among the users of funds and prevent negative information arbitrage to the detriment of the system. Bank Board should ensure that the audit processes and the internal systems and control are capable to identify vulnerable areas, raise red flags and plug loopholes quickly and effectively.

6) Delays should be avoided in reporting frauds to appropriate authorities, conducting investigation and fixing staff accountability, which in effect leads to shielding of the main culprit while the blame is generally shifted to the junior level officials. More importantly, it is necessary that a strong foundation is built by leveraging robust IT systems, framing effective policies and procedures, laying down strict compliance processes, setting high integrity standards, developing efficient monitoring capabilities and initiating strict punitive action against the culprits in a time bound manner. This is necessary not just for the safety of banks but for ensuring the stability and resilience of the overall financial system and sustaining the confidence that various stakeholders have in its strength and integrity.

7) Job rotation in critical areas of banking operations and branches should be strictly followed. Compulsory leave should be granted at regular intervals to the staff operating in critical areas banking and also to a branch manager. Star performers as identified in banks should be kept under watch. Further, posting of senior officers to Inspection department should be made compulsory for higher promotion. In addition, the alert staff member should be suitably honored.

8) Investigation team members should be given an opportunity to undergo a training programme to acquire necessary skills to conduct investigation timely & objectively and initiate staff action within a given time limit. Similarly, banks should regularly reorient and train their personnel so that they fully understand the importance of internal controls in their respective work place. Besides class room training, there shall be regular e-modules with e-certifications and updates made available to the officers at large.

References

1. Report of the Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds, 2012
2. Financial Express, June 14, 2019.
3. Economic Times, August 29, 2018.
4. Fraud Risk Management, SIB Students Corner, Theme No 322, South Indian Bank, Thissur
5. Report on Analysis of Top 100 bank Frauds, Central Vigilance Commission, October 2017.
6. Report to the Nation on Occupational Fraud and Abuse, Association of Certified Fraud Examiners (ACFE), 2012Frauds in the Indian Banking Industry,
7. WORKING PAPER NO: 505, Charan Singh & Others, IIM, Bengaluru, March 2016.
8. Deficiencies in Credit, Reserve Bank of India Circular , August 10, 2004
9. Speech delivered by Shri R. Gandhi, Deputy Governor at "2nd National Conference on Financial Frauds Risks & Preventions" organized by ASSOCHAM on June 26, 2015 at New Delhi.
10. Indian Banking Sector: Current Status and the Way Forward ,Address by Shri Shaktikanta Das, Governor, Reserve Bank of India Delivered at the National Institute of Bank Management.
11. Dr. V.S. Kaveri , "Journal of Commerce & Management Through:" Aug. 2019