International Journal of Business and Management Invention
ISSN (Online): 2319 – 8028, ISSN (Print): 2319 – 801X
www.ijbmi.org || Volume 5 Issue 7 || July. 2016 || PP—01-09

Frauds in Indian Banking: Aspects, Reasons, Trend-Analysis and Suggestive Measures

Dr. Sukhamaya Swain, Dr. Lalata K Pani

ABSTRACT: *Frauds (basis amount of money involved) in Indian banking have seen a rising trend over the last few years. The statement is just basis the cases reported by member banks in India; the unreported figures could be still higher. Against this backdrop and coupled with rising NPAs and more usage of alternate technological modes of baking, it is essential that banks relook at the time and amount of attention that they normally have been giving to frauds and proactive measures to prevent the same.*
This paper discusses the various aspects of frauds in Indian banking system. It evaluates the statistics involved with fraud basis secondary data available from reliable sources and also analyses the same. Each of the types namely KYC related, loan related and technological aspects are discussed in details along with the reasons. At the end, some suggestions are placed for banks to practice.

I. INTRODUCTION

The banking and financial services, government and public administration, and manufacturing industries were the most represented sectors in the fraud cases that were examined by ***Association of Certified Fraud Examiners*** while preparing the ***Global Fraud Study 2016***. The frequency, complexity type and the money involved in banking frauds have increased manifold resulting in a very serious cause of concern for regulators, such as RBI.
In the last three years, public sector banks (PSBs) in India alone have lost close to Rs. 22,700 Crores on account of banking frauds. This amount has been increasing with each passing year. In most cases we have the staff of the banks involved and in some cases it has been because of technological attempts by outsiders.

Evolution of frauds in banks

In the earlier times, the frauds were limited to fake currency circulation (some of which entered the banking system), forged cheques (again a case of duplicity and printing of fake security items like cheques, Demand drafts and Pay Orders) and advancing loans to known parties without checking the repayment ability and cash-earning proposition in the loan proposal(s).
With the advent of technology, cybercrime has become the new menace of the day. Bankers today have to delve with newer terms with the passage of time. Hawala transactions of yester-years have been replaced by benami accounts wherein the account holder has no clue that he/she has a bank account and if that fact is known, the transactions (volume and nature of the same) are absolutely unknown to the account holder.

Definition

Fraud, under Section 17 of the Indian Contract Act, 1872, includes any of the following acts committed by a party to a contract, or with his connivance, or by his agents, with intent to deceive another party thereto or his agent, or to induce him to enter into the contract:

- The suggestion as a fact, of that which is not true, by one who does not believe it to be true;
- The active concealment of a fact by one having knowledge or belief of the fact;
- A promise made without any intention of performing it;
- Any other act fitted to deceive;
- Any such act or omission as the law specially declares to be fraudulent

RBI as a statutory body has, per se, not defined the term "fraud" in its guidelines on Frauds. A definition of fraud was, however, suggested in the context of electronic banking in the Report of RBI Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds, which reads as: "*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*".
According to the Association of Certified Fraud Examiners (ACFE), fraud is "*a deception or misrepresentation that an individual or entity makes knowing that misrepresentation could result in some unauthorized benefit to the individual or to the entity or some other party*".

Some statistics related to banking frauds
As many as 861 bank advance related fraud cases of Rs 1 lakh and more, involving Rs 4,920 crore, were reported in the first half of 2015-16. During 2014-15, 1,651 such cases were reported that involved an amount of Rs 11,083.11 crore.

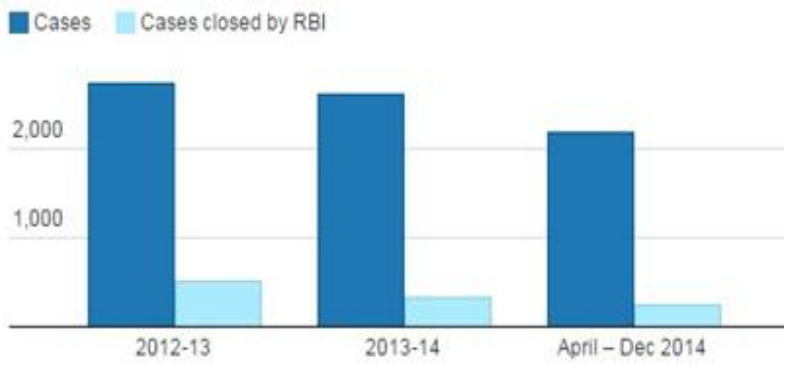

Fig I: Number of bank fraud cases involving Rs. 1 Lac and above

While one sees in isolation, the above statistics does not mean anything. However when one sees the figure below, one observes that the decreasing trend (in number) is primarily attributed to the decrement in the low value cases (less than 1 Lac.). There has been substantial improvement in the large ticket cases (involving Crores.). Needless to say, this is an alarming trend.

(No. of cases in absolute terms and amount involved in Rs. Crore)

Amt Involved	< Rs 1 lakh		> 1 lakh and up to Rs 1 crore		> Rs 1 cr and up to Rs 50 crore		> Rs.50 crore		Total Fraud cases	
FY (Apr–Mar)	No. of cases	Total Amount	No. of cases	Total Amount	No. of cases	Total Amount	No. of cases	Total Amount	No. of cases	Total Amount
Pre-2004	2292	4.24	819	96.65	613	2951.64	13	1244.26	3737	4296.80
2004–05	7553	12.50	2407	287.32	111	584.89	1	53.57	10072	938.29
2005–06	11395	18.63	2334	290.20	192	1009.23	2	135.47	13923	1453.53
2006–07	20415	31.22	3048	325.02	158	791.17	1	78.45	23622	1225.86
2007–08	17691	30.25	3381	383.98	177	662.31	–	–	21249	1076.54
2008–09	19485	33.85	4239	442.94	214	1129.56	3	305.33	23941	1911.68
2009–10	20072	30.36	4494	474.04	222	1129.28	3	404.13	24791	2037.81
2010–11	15284	26.09	4250	494.64	277	1515.15	16	1796.20	19827	3832.08
2011–12	10638	19.05	3751	509.17	327	2113.23	19	1850.08	14735	4491.54
2012–13	9060	22.11	3816	491.13	372	2798.00	45	5334.75	13293	8646.00
Total	**133885**	**228.31**	**32539**	**3795.10**	**2663**	**14684.46**	**103**	**11202.25**	**169190**	**29910.12**

Fig. II: Year wise fraud cases reported by commercial banks

What is more alarming is the below mentioned cases which shows the number of cases closed by RBI. If the increment of number of such cases were not enough, Fig III goes on to show that the said cases are not closed. The authors are not aware of the reasons of the same but this for sure is not a good sign.

(No. of cases in absolute terms and amount involved in Rs. Crore)

Amt Involved	< Rs 1 lakh		> 1 lakh and up to Rs 1 crore		> Rs 1 cr and up to Rs 50 crore		> Rs.50 crore		Total Fraud cases	
FY (Apr–Mar)	No. of cases	Total Amount	No. of cases	Total Amount	No. of cases	Total Amount	No. of cases	Total Amount	No. of cases	Total Amount
Pre-2004	1661	2.85	568	36.33	11	94.64	1	85.66	2241	219.48
2004–05	6047	8.47	470	33.27	13	99.68	–	–	6530	141.42
2005–06	11611	9.47	154	10.86	11	75.93	1	55.28	11777	151.54
2006–07	14291	9.46	248	17.53	4	34.30	–	–	14543	61.29
2007–08	12861	11.23	374	26.79	3	32.05	–	–	13238	70.07
2008–09	6796	9.25	420	20.84	10	49.28	–	–	7226	79.37
2009–10	5828	8.99	636	38.03	4	21.18	–	–	6468	68.20
2010–11	13526	13.47	649	42.88	7	14.26	–	–	14182	70.61
2011–12	38330	23.58	756	49.80	10	33.04	–	–	39096	106.42
2012–13	11198	8.45	556	35.83	14	78.51	–	–	11768	122.79
Total	**122149**	**105.22**	**4831**	**312.16**	**87**	**532.87**	**2**	**140.94**	**127069**	**1091.18**

Fig. III: Year wise details of fraud cases closed

As per Fig IV, the number of cases and the value involved with SBI, its associates and the Public sector banks are less than that of private sector banks. The amount involved is however the reverse. The private banks have more number of small cases.

(No. of cases in absolute terms and amount involved in Rs. Crore)

Amt Involved	< Rs 1 lakh		> 1 lakh and up to Rs 1 crore		> Rs 1 cr and up to Rs 50 crore		> Rs.50 crore		Total Fraud cases	
Bank Group	No. of cases	Total Amount	No. of cases	Total Amount	No. of cases	Total Amount	No. of cases	Total Amount	No. of cases	Total Amount
Nationalised Banks including SBI Group	7622	31.97	19753	2847.11	2184	11867.24	94	10081.69	29653	24828.01
Old Pvt. Sector Banks	622	2.38	1463	225.09	181	1001.56	5	478.68	2271	1707.71
New Pvt. Sector Banks	83850	112.36	6984	510.18	225	1445.82	1	72.11	91060	2140.47
Sub Total (Private Banks)	84472	114.74	8447	735.27	406	2447.38	6	550.79	93331	3848.19
Foreign Banks	41791	81.60	4339	212.72	73	369.84	3	569.76	46206	1233.92
Grand Total	133885	228.31	32539	3795.10	2663	14684.46	103	11202.25	169190	29910.12

Fig. IV: Bank Group wise fraud cases reported as of 31-Mar 2013

While the number of frauds and the amount involved, when seen in isolation, may seem large, it is important to view the incidence of frauds in the banking sector in the context of the massive increase in the number of deposit and credit accounts in banks and the huge volumes (number as well as value) of transactions that are processed by the banks every day. To put figures in the right perspective, the number of deposit accounts in the banks over ten years (between end 2002 and end 2012) has gone up from 43.99 crore to 90.32 crore while the number of loan accounts in the same period has also more than doubled from 5.64 crore to 13.08 crore. A quick estimate puts the average number of all transactions that happen every day in the banking system at approximately 10 crore, which is enormous. The number of frauds per million banking transactions was about 0.4, which is not a very high figure.

The alternate Channels usage has also been improving over the years. Table I shares the data for March months of 2012 and 2016. Number of POS transactions has grown 3 times in the period. The number of debit cards outstanding as of the last date of that month has also doubled. A study on e-commerce in India by Accel Partners estimated that shopping through mobile phones grew 800 per cent in 2013. It is expected to show a compounded annual growth rate (CAGR) of 150 per cent by 2016.

	Mar-16	***Mar-12***	***Multiplying factor***
No. of ATMs	199099	95686	2.08
No. of ATM transactions	732334936	471233729	1.55
Amount of ATM Transactions (In INR Cr.)	224862.4	131837.6	1.71
No. POS Terminals	1385668	660920	2.10
No. of POS transactions	185088730	59413631	3.12
Amount of POS transactions (In INR Cr.)	36157.4	13490.7	2.68
No. of Credit cards	24505219	17653818	1.39
No. of Debit Cards	661824092	278282839	2.38

Table I: Statistical figures for POS, ATMs, Credit Cards and Debit Cards

Coming to the discussion point on number of frauds, on a standalone basis the quantum of frauds, both in terms of number and amount involved, may appear to be very high, but when one weighs it against the sheer magnitude of accounts and transactions handled by the banking system, they are not alarming.

Various aspects of bank frauds

Broadly, the frauds reported by banks can be divided into three main sub-groups:

II. KYC RELATED

After the international focus on KYC, RBI brought a paradigm shift in the approach to KYC by banks in India. It moved away from *introduction to document based identification* - hence introduction is no more required. It also shifted the focus from *financial loss* (from frauds) to the banks to the *loss of reputation* to the banks (by non-compliance). The other principles are that the KYC information collected is to be consistent with risk perception and other information to be collected only with consent of the customer and the KYC related information is confidential - not to be divulged for cross-selling or any other purpose.

RBI has prescribed that the KYC policy of banks should have the following key elements:

(i) Customer Acceptance Policy
(ii) Customer Identification Procedures
(iii) Monitoring of Transactions, and
(iv) Risk Management

If one were to carefully observe, each of the elements is intended to make the *customer-bank* relationship a fraud-free one.

Fraudulent documentation involves altering, changing or modifying a document to deceive the bank. It can also involve approving incorrect information provided in documents knowingly (cases of connivance of bank staff with fraudsters). Deposit accounts in banks with lax KYC drills/ inoperative accounts are vulnerable to fraudulent documentation.

Some typical examples:

- To evade taxes, an individual routes savings transactions through multiple bank accounts
- An individual illegally obtains personal information/ documents of another person and takes a loan in the name of that person.
- He/she provides false information about his/her financial status, such as salary / IT return and other assets, and takes a loan for an amount that exceeds his / her eligible limits with the motive of non-repayment.
- A person takes a loan using a fictitious name and there is a lack of a strong framework pertaining to spot verifications of address, due diligence of directors/promoters, pre-sanction surveys and identification of faulty/incomplete applications and negative/criminal records in client history.
- Fake documentation is used to grant excess overdraft facility and withdraw money.
- A person may forge export documents such as airway bills, bills of lading, Export Credit Guarantee Cover and customs purged numbers/orders issued by the customs authority.

In each of these examples, there is possible laxity in checking documents. KYC is not just checking the documents submitted but ensuring that whatever has been submitted pertains to the same person / applicant.

III. ADVANCES RELATED

Frauds related to the advances portfolio accounts for the largest share of the total amount involved in frauds in the Indian banking sector. Increase in the cases of large value fraud (involving amount of Rs. 50 crore and

above) in accounts financed under consortium or multiple banking arrangements involving even more than 10 banks at times, is an unwelcome trend in the banking sector. Another point that needs to be highlighted here is that public sector banks account for a substantial chunk of the total amount involved in such cases.
Majority of the credit related frauds are on account of deficient appraisal system, poor post disbursement supervision and inadequate follow up.

a. Siphoning of funds takes place when funds borrowed from banks are utilised for purposes unrelated to the operations of the borrower.

b. Diversion of funds includes any one of the following occurrences:

- Use of short-term working capital funds for long-term commitments not in conformity with the terms of sanction
- Using borrowed funds for creation of assets other than those for which the loan was sanctioned
- Transferring funds to group companies
- Investment in other companies by acquiring shares without the approval of lenders
- Shortage in the usage of funds as compared to the amounts disbursed/ drawn, with the difference not being accounted for

c. Over-valuation or absence of requisite collaterals

Absence of extant guidelines on the due diligence of professionals (Chartered Accountants or financial advisors) assisting borrowers at the time of disbursement of loans may result in valuation agencies or advocates facilitating the perpetration of frauds by colluding with the borrowers to inflate security valuation reports. Some examples:
Concealing liabilities: Borrowers concealing obligations such as mortgage loans on other properties or newly acquired credit card debts in order to reduce the amount of monthly debt declared on the loan application
Misstatement: Deliberately overstating or understating the property's appraised value
Shot gunning: Multiple loans for the same property being obtained simultaneously for a total amount greatly in excess of the actual value of the property
Another aspect which needs to be discussed in this context is considerable delay in declaration of frauds by various banks in cases of consortium/ multiple financing. RBI on many occasions has observed more than 12–15 months lag in declaration of the same case as fraud by different banks, which not only enables the borrower to defraud the banking system to a larger extent, but also allows him considerable time to erase the money trail and change the pitch for the investigative agencies and statutory authorities.
Although RBI has advised banks to ensure proper and transparent exchange of information between lenders on the borrowers financed under multiple banking arrangements / consortium arrangements, cases of multiple financing against the same security still come up indicating utter disregard in conforming to the basic safeguards as advised by RBI.

IV. TECHNOLOGY RELATED

In 2014, around 65% of the total fraud cases reported by banks were technology-related frauds (covering frauds committed through / at an internet banking channel, ATMs and other payment channels like credit/debit/prepaid cards).
Business and technology innovations that the banking sector is adopting in their quest for growth are in turn presenting heightened levels of cyber risks. These innovations have probably introduced new vulnerabilities and complexities into the system. For example, the continued adoption of web, mobile, cloud, and social media technologies has increased opportunities for attackers. Similarly, the waves of outsourcing, offshoring, and third-party contracting driven by a cost reduction objective may have further diluted institutional control over IT systems and access
points. These trends have resulted in the development of an increasingly boundary-less ecosystem within which banking companies operate, and thus a much broader "attack surface" for the fraudsters to exploit.

Hacking: Hackers/fraudsters obtain unauthorized access to the card management system of the respective bank. Counterfeit cards are then issued for the purpose of money laundering.

Phishing: A technique used to obtain your card and personal details through a fake email

Pharming: A similar technique where a fraudster installs malicious code on a personal computer or server. This code then redirects clicks you make on a Website to another fraudulent Website without your consent or knowledge

Vishing*:* Fraudsters also use the phone to solicit your personal information.

Smishing*:* It uses cell phone text messages to lure consumers in. Often the text will contain an URL or phone number. The phone number often has an automated voice response system. And again just like phishing, the smishing message usually asks for your immediate attention.

Debit card skimming: A machine or camera is installed at an ATM which picks up card related information and PIN numbers when customers use their cards.

Computer viruses: With every click on the internet, a company's systems are open to the risk of being infected with nefarious software that is set up to harvest information from the company servers.

Counterfeit instruments: Fake cheques / Demand Drafts that look too good to be true are being used in a growing number of fraudulent schemes, including foreign lottery scams, cheque overpayment scams, internet auction scams and secret shopper scams.

With the growing business of mobile banking, it is essential that we devote exclusive space and time to this aspect / mode of banking. The risks associated with Mobile Banking have to be studied on a two pronged base i.e. ***Transactions through Mobile*** and ***Mobile Wallets***. Why Mobile Wallets? The reason is that at the backend of every e-Wallet we either have a bank account, banks' credit card or debit card.
According to RBI, in 2014-2015, 22 million of the 589 million bank account holders were using mobile banking apps. The volume of mobile banking transactions has also risen from around Rs.1,819 crore in 2011–12 to about Rs.1.02 trillion in 2014–15, as per a PwC report. Possible frauds with Mobile Banking:

Fake apps: The first step in stealing money online is to steal information. This can be done by creating a fake app outside a play store. Hackers create fake apps which will looks exactly as the original one and the usage & interface is similar to the original app.

Mobile banking application being mapped to an incorrect mobile number: For bank customers who do not use mobile banking, an employee of the bank could attach an associate's mobile number to the bank account and install a mobile application on his mobile device. The customer's account is compromised by the associate and he or she does not get any notification about the same.

SIM Swap: The fraudsters shall first collect the personal banking information through phishing, vishing, smishing or any other means. Once they have the same, they manage to have the SIM card blocked, and obtain a duplicate one by visiting the mobile operator's retail outlet with fake identity proof. The mobile operator deactivates the genuine SIM card, which was blocked, and issues a new SIM to the fraudsters. It is now simple to generate a one-time password (OTP) required for transactions using the stolen banking information. This OTP is received on the new SIM held by the fraudsters and they can now transact before the bank customer realizes the theft and alerts the bank.
Possible frauds with Mobile Wallets:

Increased risk of money laundering: Transfer of money into and out of a mobile wallet (with open and semi-open wallet option available) from or to a bank account is now possible. Cash-in from the bank account of an individual and cash-out to a different bank account of another individual can be used as a platform for laundering unaccounted money.

Fake merchants: If the merchant on-boarded by the service provider is a fraudster, and the payment is made by the customer for fictitious goods or services from the merchant, cash can be debited from the account.
Adoption of mobile commerce is dependent on customers' perceptions about how safe their virtual money is from fraud. Over time, the ability to successfully counter frauds can become a key business differentiator for mobile wallet companies. Fraud, therefore needs to be considered as a critical business risk rather than just a one-off financial loss.

Reasons for bank frauds

i. Lack of oversight by concerned officer's w.r.t. deviation management: With existing systems and procedures clearly defined, it is the onus on the senior management to allow specific deviations. Lack of seriousness and knowledge regarding the same may create havoc and lead to a fraud.

ii. Non adherence to KYC guidelines as prescribed by RBI: In the haste of increasing the CASA base of respective branches (or any unit), KYC requirements are compromised. RBI has recently fined banks for non-adherence to KYC norms. The concurrent auditor, who visits the branch once in a month, points out those KYC guidelines which are not followed by the branch and asks it to obtain proof and confirm. This takes another month or so. During this lean period, fraudsters open deposit accounts, deposit forged stolen cheques and withdraw the amount.
iii. Increasing business pressure on staff: Margins, profitability and shareholders expectations being under strain, the management passes on to the middle management who in turn have the same transmitted to the line staff. Staff may use unscrupulous methods to achieve their respective targets.
iv. Lack of tools to identify potential red flags: Some organisations even if they have the correct, agile and educated managers, there may be absence of suitable systems to give the necessary signals during the course of a loan turning bad or a KYC being violated et al.
v. The symptoms of poor internal control systems increase the chances of frauds. Internal control symptoms include a poor control environment, lack of segregation of duties, lack of physical safeguards, lack of independent checks, lack of proper authorizations, lack of proper documents and records, the overriding of existing controls, and an inadequate accounting system.
vi. Changes in technology: The new technologies adopted by banks are making them increasingly vulnerable to various risks such as phishing, identity theft, card skimming, vishing, SMSishing, viruses and Trojans, spyware and adware, social engineering, website cloning and cyber stalking. Banking transactions today have moved to debit/ credit cards and to electronic channels like ATMs, RTGS/ NEFT, ECS/NECS, Internet banking and Mobile banking. This has given a happy hunting ground to fraudsters. Infact all these alternate channels are being promoted by each of the commercial banks to reduce the pressure on branch banking.
vii. Collusion between employees and external parties: Insider fraud, whether arising from coercion, collusion, or otherwise, are increasingly considered to be one of the most serious fraud threats faced by banks in India. Infact it does not require sophisticated learning to decipher that the frauds happening today are not an act of an individual.
viii. Inexperienced staff: People with no or little experience or exposure to loans/advances are posted to branches which have large advances portfolio and are compelled to process loan proposals.

Silver Linings

- RBI has set up fraud monitoring cell (June 2016).
- RBI has instructed all banks that fraud risk management, fraud monitoring and fraud investigation function must be owned by the bank's CEO, Audit Committee of the Board and the Special Committee of the Board, at least in respect of large value frauds.
- RBI has asked banks to disclose fraud cases and make provisions for them not exceeding four quarters from the date during which it has been detected. Banks as per the notification must scrupulously adhere to the extant guidelines on classification and reporting of the frauds. Banks should normally provide for the entire amount due to the bank or for which the bank is liable (including in case of deposit accounts), immediately upon a fraud being detected.
- Reporting structure is clearly defined by RBI

Category of bank	Amount involved in the fraud	Agency to whom complaint should be lodged	Other Information
Private Sector/ Foreign Banks	Rs.1 lakh and above	State police	
	Rs.10000 and above if committed by staff	State police	
	Rs.1 crore and above	Serious fraud investigation office (Ministry of Corporate Affairs)	In addition to state police
Public Sector Banks	Below Rs. 3 crore	State police	
	Rs.3 crore and above and up to Rs.25 crore	CBI	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 Rs.25 crore	CBI	Banking Security and Fraud Cell (BSFC) of CBI (irrespective of the involvement of a public servant)

Fig V: Current Structure for filing Police/CBI complaints; defined by RBI

V. SUGGESTIONS

a. Adherence to all the guidelines of RBI w.r.t. KYC and loan proposals.
b. There should be a dedicated cell within each bank to monitor the company/firm to which they are lending and the macro-economic environment of the concerned industry or market where products are marketed. This is independent of the credit officers. The job should be to constantly evaluate and not just check the same during the time of on-boarding.
c. Re-KYC, if done diligently can also help check any fraudulent activities particularly on the liability side. Infact, staff may be incentivized to do the same.
d. Triggers should be designed for all transactions. These should be for both liability as well as borrowal customers. The triggers should alert concerned officials upon deviation. Typically, banks have such alert mechanism for loan customers but liability is not a no-risk area.
e. The government should consider examining the role of third parties such as chartered accountants, advocates, auditors, and rating agencies that figure in accounts related to bank frauds, and put in place strict punitive measures for future deterrence. There is also a case to be made to question the certification/credentials of third parties like auditors to decide their competence in evaluating accounts containing potentially fraudulent entries.
f. A new case of fraud should be informed to all officials of the bank. Nowadays with each bank having their own intranet system for communication, a simple mailer with the names of the officers / parties morphed may be circulated.
g. Feeding of information by various govt. agencies to banks should be made. Agencies / authorities like Home Ministry, CBI, CBDT, CBEC, CVC, RBI atleast should regularly feed banks with information if at all they get on an apriori basis.
h. Banks have traditionally focused their investments on becoming secure. However, this approach is no longer adequate in the face of a rapidly changing threat landscape. Banks should consider building cyber risk management programs to achieve three essential capabilities namely: the ability to be secure, vigilant, and resilient.

VI. CONCLUSION

While fraud is not a subject that any bank wants to deal with, the reality is that most organizations experience fraud to some degree. It should be recognized that the dynamics of any organization (why only bank) requires an ongoing reassessment of fraud exposures and responses in light of the changing environment an organization encounters. Especially given the unrelenting pace of regulatory change within the banking sector, these stricter regulatory requirements are demanding more attention from management, affecting the profitability of different lines of business, and increasing costs of compliance.

a. The frauds may be primarily due to lack of adequate supervision of top management, faulty incentive mechanism in place for employees, 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.
b. The minds of officers cannot be read during the time of recruitment. Mindset of some private and some public sector bank employees shall be to intentionally defraud the organisation. What the organisations can do is to establish and recheck systems which shall raise the timely alert on deviations.
c. Online banking is the new trend and it is here to stay. Banks must realize that the customers who use online banking services is a very powerful group capable of launching scathing attacks using the social media, which can irreparably tarnish the reputation of banks. Banks would need to constantly monitor the typology of the fraudulent activities in such transactions and regularly review and update the existing security features to prevent easy manipulation by hackers, skimmers, phishes, etc. Banks have traditionally planned for resilience against physical attacks and natural disasters; cyber resilience can be treated in the same way. Banks should consider their overall cyber resilience capabilities across several dimensions.
d. Society and media should demand stringent action against the perpetrators of financial frauds
e. As new regulations such as the Companies Act, 2013, place greater emphasis on the presence of a vigil mechanism to mitigate fraud risks, banks must ensure that their employees are aware of their organization's whistleblower policy and should socially ostracize them. They could be borrowers, lenders, staff or any other stakeholder in the scheme of frauds.

Early detection, through the implementation of requisite programs / software's / system to detect both emerging threats and the fraudster's moves, can be an essential step towards containing and mitigating losses. Incident detection that incorporates sophisticated, adaptive, signaling, and reporting systems can automate the correlation and analysis of large amounts of IT and business data, as well as various threat indicators, on an enterprise-wide basis. Banks' monitoring systems should work 24/7, with adequate support for efficient incident handling and remediation processes.

REFERENCES

[1]. Report to the Nations on Occupational Fraud and abuse, part of Global Fraud Study 2016 by Association of Certified Fraud Examiners.
[2]. Current fraud trends in the financial sector, report by ASSOCHAM and PwC (June 2015)
[3]. "RBI sets up fraud monitoring cell", news article of Economic Times (22-Jun 2016).
[4]. Master Circular on Frauds- Classification and Reporting: RBI (01-Jul 2015)
[5]. Frauds – Classification and Reporting: RBI (01-Jul 2014).
[6]. Singh, Charan, "Frauds in the Indian Banking Industry" published in Mar 2016.
[7]. "India Banking Fraud Survey - Edition II", Deloitte Consulting, April 2015.
[8]. "KYC – compliance vs convenience", speech by Mr R Gandhi, Deputy Governor of the Reserve Bank of India, at the Federation of Andhra Pradesh Chambers of Commerce and Industry, Hyderabad on 23-May 2014.
[9]. "Fraud in the banking sector – causes, concerns and Cures", speech by Dr K C Chakrabarty, Deputy Governor of the Reserve Bank of India, during the National Conference on Financial Fraud organised by ASSOCHAM, New Delhi, 26 July 2013.