

## Banking Industry Frauds in India : An Analysis

<sup>1</sup>Rajneesh Kumar, <sup>2</sup>Sanjeev Kumar

<sup>1</sup>Assistant Professor Govt. Degree College Rakkar Teh. Rakkar Distt. Kangra HP India

<sup>2</sup>Teacher, Govt. Primary School Balh, Nadaun, Hamirpur, 177042, HP, India,

Email - <sup>1</sup> rajneesh.ndn@gmail.com <sup>2</sup> sanjeevmnature@gmail.com.

**Abstract:** The technology have used in financial services of course, which has given a tremendous impetus to their development. However, due to heavy dependency on electronic and digital tools to carry out business and payment transactions, a serious threat has also been imposed to the safety and reliability of financial operations. The frauds with online payments, ATM machines, electronic cards and net banking transactions have become a serious issue. Huge loss of money of people and institutions is caused every year due to these cyber frauds in the banking sector, even after tight security measures in electronic transactions. The banks themselves have been found to be involved in fraudulent practices in a big way causing their customers enormous losses.

**Key Words:** bank frauds, preventive measures, internal control, compliance, and security controls.

### 1. INTRODUCTION:

The fraud can loosely be defined as “any behavior by which one person intends to gain a dishonest advantage over another in other words, the fraud is an act or omission which is intended to cause wrongful gain to one person and wrongful loss to the other, either by way of the concealment of facts or otherwise. The 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. The Bank fraud is the use of potentially illegal means to obtain money, assets, or other property owned or held by the financial institution, or to obtain money from the depositors by fraudulently posing as a bank or other financial institutions. The bank fraud is a criminal offence, while the specific elements of particular banking fraud laws vary depending on jurisdictions. The bank frauds apply to actions that employ a scheme or artifice, as opposed to the theft & bank robbery. For this purpose, sometime the bank fraud have considered a white-collar crime. The banks are dealing with public’s money and hence it has imperative that employees should exercise due care and diligence in handling the transactions in the banks. The recent rise in the bank frauds calls for tightening of security mechanism. The strong system of internal control is the most effective way of the fraud prevention. The banks should increase their efforts to raise the level of security awareness in their organizations to combat the frauds.

#### 1.1. Areas of Bank Frauds:

The bank frauds mainly describe into four areas such as deposits, cyber, trade & depository and loans & advances frauds, which also depicts in the following figure 1.

#### 1.2. Review of Literature:

Albrecht (1996), has observed that, the symptoms of poor internal controls increase the likelihood 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. Bologna (1994), Calderon and Green (1994) and Beirstaker, Brody, Pacini (2005), have observed in their studies that the cites the environmental factors that enhance the probability of embezzlement, they are: inadequate rewards; inadequate internal controls; no separation of duties or audit trails; ambiguity in job roles, duties, responsibilities, and areas of accountability; failure to counsel and take administrative action when performance levels or personal behaviour fall below acceptable levels; inadequate operational review; lack of timely or periodic review, inspections, and follow-up to assure compliance with company goals, priorities, policies, procedures, and governmental regulations and failure to monitor and enforce policies on honesty and loyalty. The study also observed that the various techniques include fraud policies, telephone hotlines, employee reference checks, fraud vulnerability reviews, vendor contract reviews and sanctions, analytical reviews

(financial ratio analysis), password protection, firewalls, digital analysis and other forms of software technology, and discovery sampling.

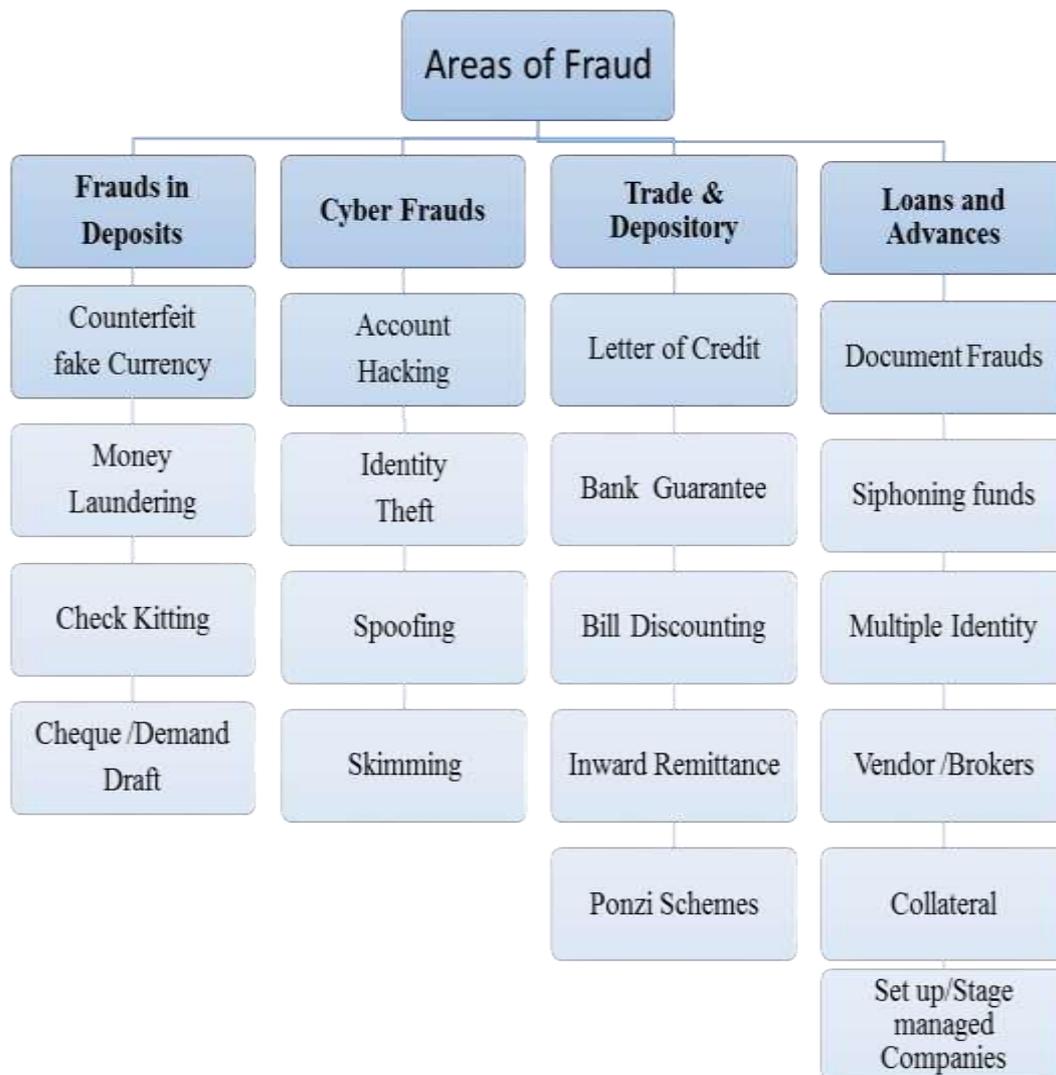


Figure -1

1.3. Objectives :

- To study the different types of the Bank frauds.
- To analyse the Technology and advances related bank frauds.
- To study & identify the frauds prevention and detection and advance suggestions to remove the banking frauds.

2. RESULTS AND DISCUSSION

The objectives of the study are based upon the following results & discussion.

A) Different Types of the Bank Frauds

The different types of bank frauds illustrated are as under:

**Stolen Checks Fraud**

The fraudsters may seek access to facilities such as mailrooms, post offices, offices of a tax authority, a corporate payroll or a social or veterans' benefit office, which process cheques in large numbers. Then the fraudsters may open bank accounts under assumed names and deposit the cheques. Thereafter, they may first alter in order to appear legitimate, so that they can subsequently withdraw unauthorised funds is known as stolen checks fraud.

**Cheques kiting Fraud**

In the Cheque kiting frauds, a cheque is deposited to a bank account and the money is made available immediately, even though it is not removed from the account on which the cheque is drawn until the cheque actually clears.

### **Forgery and altered cheques Fraud**

When the person have altered cheques in the name (in order to deposit cheques intended for payment to someone else) or the amount on the face of cheques, simple altering can change Rs. 100.00 into Rs. 100,000.00.

### **Accounting fraud**

The fraudsters hide serious financial problems, known to use fraudulent bookkeeping to overstate sales and income, inflate the worth of the company's assets, or state a profit when the company is operating at a loss. These tampered records are then used to seek investment in the company's bond or security issues or to make fraudulent loan applications in a final attempt to obtain more money to delay the inevitable collapse of an unprofitable or mismanaged firm.

### **Demand draft fraud**

The bank employees remove a few DD leaves or DD books from stock and write them like a regular DD. Since they are insiders, they know the coding and punching of a demand draft. The fraudulent demand drafts are usually drawn payable at a distant city without debiting an account. The draft is cashed at the payable branch.

### **Fraudulent loans**

The fraudulent loan is one in which the borrower is a business entity controlled by a dishonest bank officer or an accomplice; the "borrower" then declares bankruptcy and the money is gone. The borrower may even be a non-existent entity and the loan merely an artifice to conceal a theft of a large sum of money from the bank.

### **Fraudulent loan applications**

The bank employees take a number of forms varying from individuals and using false information to hide a credit history filled with financial problems. Then unpaid loans to corporations using accounting fraud to overstate profits in order to make a risky loan appear to be a sound investment for the bank.

### **Forged or fraudulent documents**

The documents claiming that a sum of money has been borrowed as a loan, withdrawn by an individual depositor, transferred or invested. Therefore can be valuable to someone who wishes to conceal the minor detail that the bank's money has in fact been stolen.

### **Wire transfer fraud**

In the wire transfer system the funds takes a few days for the transfer to "clear" and be available to withdraw. The other person may still be able to withdraw the money from the other bank. A new teller or corrupt officer may approve withdraw since it is in pending status, which then the other person cancels the wire transfer and the bank institution takes a monetary loss.

### **Bill discounting fraud**

The fraudster uses a company at their disposal to gain confidence with a bank, by appearing as a genuine, profitable customer. The company regularly and repeatedly uses the bank to get payment from one or more of its customers to give the illusion of being a desired customer. These payments are always made actively paying any and all bills raised by the bank. After a period of time, the bank is happy with the company. The company requests that the bank settles its balance with the company before billing the customer, again business continues as normal for the fraudulent company. Only when the outstanding balance between the bank and the company is sufficiently large. The company takes the payment from the bank and thereafter the company and its customers disappear or leaving no-one to pay the bills issued by the bank.

### **Payment card fraud**

The Credit card fraud is widespread as a means of stealing from banks, merchants and clients.

### **Stolen payment cards**

The simplest form of this theft involves stealing the card itself and charging a number of high-ticket items to it in the first few minutes or hours before it is reported as stolen.

The fraudsters have attached fraudulent card stripe readers to publicly accessible ATMs, to gain unauthorised access to the contents of the magnetic stripe, as well as hidden cameras to illegally record users' authorisation codes. The data recorded by the cameras and fraudulent card stripe readers are subsequently used to produce duplicate cards that could then be used to make ATM withdrawals from the victims' accounts.

### **Empty ATM envelope deposits**

A criminal overdraft can result due to the account holder making a worthless or misrepresented deposit at an automated teller machine in order to obtain more cash than present in the account or to prevent a check from being returned due to non-sufficient funds.

### **Impersonation**

The scam operates by obtaining information about an individual, then using the information to apply for identity cards, accounts and credit in that person's name. Often little more than name, parents' name, date and place of birth are sufficient to obtain a birth certificate; each document obtained then is used as identification in order to obtain more

identity documents. Government-issued standard identification numbers such as "social security numbers" are also valuable to the fraudster.

**Phishing and Internet fraud**

The Phishing fraud operates by sending forged e-mail, impersonating an online bank, auction or payment site; the e-mail directs the user to a forged web site, which is designed to look like the login to the legitimate site. Which claims that the user must update personal info. Then stolen information is used in other frauds, such as theft of identity or online auction fraud.

**Money laundering**

The Money laundering is the process by which large amounts of illegally obtained money (from drug trafficking, terrorist activity or other serious crimes) is given the appearance of having originated from a legitimate source.

**B) Technology and Advances related Bank Frauds**

The technology and advances related bank frauds are exhibited as under:

**Technology related frauds**

The Banks are increasingly nudging their customers to adopt newer service delivery platforms like mobile, internet and social media, for enhanced efficiency and cost-cutting. There have been several instances of low value frauds wherein the fraudsters have employed hostile software programs or malware attacks, phishing, Vishing (voicemail), SMSishing (text messages), Whaling (targeted phishing on High Networth Individuals) techniques apart from stealing confidential data to perpetrate frauds. Bank group-wise detail of the number of technology related fraud cases with the amount involved therein over the last 4 years is as under in Table 1.

It can be inferred from the table that the large number of the bank frauds have been done by the new private sector banks as well as foreign banks. The mean score of the bank frauds is also support the same.

Table 1: Bank Group wise Technology Related Frauds								
(No. of cases in absolute terms and amount involved in Rs. Crore)								
	2009–10		2010–11		2011–12		2012–13	
Bank Group	No. of cases	Amount involved						
Nationalized Banks including SBI Group	118	1.82	143	3.39	172	7.26	190	9.85
Old Private Sector Banks	9	0.15	4	0.46	9	0.06	6	1.09
New Private Sector Banks	14387	34.53	9638	21.41	6552	16.54	3408	33.97
Sub Total	14396	34.68	9642	21.87	6561	16.6	3414	35.06
Foreign Banks	5273	26.88	4486	14.77	3315	14.60	5161	22.45
Grand Total	19787	63.38	14271	40.03	10048	38.46	8765	67.36

**3. ADVANCE FRAUDS:**

The closer examination of the reported fraud cases has revealed that around 65% of the total fraud cases reported by banks were technology related frauds (covering frauds committed through /at internet banking channel, ATMs and other alternate payment channels like credit/ debit/prepaid cards) while the advances portfolio accounted for a major proportion (64%) of the total amount involved in frauds. Table 1 shows that relatively large value advances related frauds (> Rs. 1 crore) have increased both in terms of number and amount involved over the last four years.

The mean value of the bank frauds in advances is also support the above analysis.

Table 2: Bank Group wise Advance Related Frauds (Rs. 1 Crore & above in value)								
(No. of cases in absolute terms and amount involved in Rs. Crore)								
	2009–10		2010–11		2011–12		2012–13	
Bank Group	No. of cases	Amount Involved						
Nationalised Banks including	152	736.14	201	1820.12	228	2961.45	309	6078.43

SBI Group								
Old Private Sector Banks	16	99.10	20	289.31	14	63.31	12	49.87
New Private Sector Banks	10	63.38	18	234.18	12	75.68	24	67.47
Sub-total	26	162.48	38	523.49	26	138.98	36	117.34
Foreign Banks	4	45.26	3	33.20	19	83.51	4	16.75
Grand Total	182	943.87	242	2376.81	273	3183.94	349	6212.51

#### 4. CONCLUSION AND SUGGESTIONS:

From the forgoing analysis it can be concluded that the impact of frauds on entities like banks, which are engaged in financial activities, is more significant as their operations involve intermediation of funds. The economic cost of frauds can be huge in terms of likely disruption in the working of the markets, financial institutions, and the payment system. The vulnerability of banks to fraud has been heightened by technological advancements in recent times. The prevention and detection of bank frauds are given as under:-

- A well-defined governance structure which including Board of Director, Executives committees, Internal policies, Guidelines & control, Fraud risk management strategies etc.
- The Periodic reviews and transparent management reporting.
- Develop the policies and the procedures to provide guidance to the business, The Policies to be structured in layers to cover all the products and services across locations.
- The Effective technology solutions to be implemented for the business to run in sync and data to be available consistently.
- The Data capturing to be consistent and adequate. The data flow from various systems to be unhindered as well as the data sanctity to be preserved.
- The employ qualified and experienced staff to enable supervision and monitoring, internal audit, independent review, and investigation.

#### 5. SOME SUGGESTIONS AS HEREUNDER:

- The number of frauds reported each year is actually coming down, the amount involved is going up substantially. The increase in amount involved is largely attributable to the few large value advance related frauds that come to light each year.
- The small value technology related and other transactional frauds, as a proportion to the number of daily banking transactions, are very miniscule and are manageable.
- The large value advance related frauds, which pose a significant challenge to all stakeholders, are mainly concentrated in the public sector bank.
- 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.
- The Board oversight of the audit processes and the internal systems and control must be able to identify vulnerable areas, raise red flags and plug loopholes quickly and effectively.
- The Society should demand stringent action against the perpetrators of financial frauds and should socially ostracize them.
- The Banking system should collectively ensure that the fraudsters do not have access to banking facilities.

#### REFERENCES:

1. Bierstaker J., Brody R.G. and Pacini C., Accountants perception regarding fraud detection and prevention methods, *Managerial Auditing Journal*, 21(5), 520-535 (2006) .
2. Khanna Ashu and Arora Bindu, A study to investigate the reasons for bank frauds and the implementation of preventive security controls in Indian banking industry, *Int. J. Bus. Sci. & App. Mgmt.*, 4(3), (2009).
3. Saini Hemraj, Rao Yerra Shankar and Panda T.C., Cyber- Crimes and their Impacts: A Review', *IJERA*, 2(2), 202-209 (2012).
4. Singh B., *Online Banking Frauds In India*, Report, Retrieved from <http://perry4law.org>, March 24, (2013) at 8:17 am *Details of Calendar Year wise Cyber Frauds in Banks*, Retrieved from [www.rbi.org.in](http://www.rbi.org.in) (2013).
5. Sharma B.R., *Bank Frauds- Prevention & Detection*, Universal law Publishing Co. Pvt .Ltd. (2003).