



A SOCIO LEGAL STUDY OF FRAUD AND CHEATING: RECENT TRENDS

Dr. Shamsuddin

Assistant Professor, Amity University, Jaipur Rajasthan

Cite This Article: Dr. Shamsuddin, "A Socio Legal Study of Fraud and Cheating: Recent Trends", International Journal of Current Research and Modern Education, Volume 3,

Issue 1, Page Number 72-79, 2018.

Copy Right: © IJCRME, 2018 (All Rights Reserved). This is an Open Access Article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Abstract:

Cheating and fraud are two offences generally can be seen in the personal and professional transactions. Cheating is defined in Indian penal code and different punishment provisions are provided there for various kind of cheating. Fraud is no where defined in Indian penal code but in various sections fraudulent conduct is an essential ingredients of the offence eg. Section 421- of IPC- Dishonest or fraudulent removal or concealment of property to prevent distribution among creditors. A brief definition of fraud is given in the Companies Act 2013, as corporate scams had disheartened to investors many times. Fraud is civil as well as criminal offence. Therefore, some time it is contended before the trial court victim can availed only one remedy either civil or criminal. But the Supreme Court had laid down the principles in various cases. This article contains the concept of fraud and cheating and recent trends of such offences.

Key Words: Fraud, Cheating, Dishonest, Wrongful Gain & Wrongful Loss

Introduction:

Cheating is a dishonest or unfair act done to gain advantage over the other. It is a criminal offence and it has myriad of crimes associated with it. It can be seen in various forms. Section 415 of IPC defines cheating as whoever, by deceiving any person, fraudulently or dishonestly induces the person so deceived to deliver any property to any person, or to consent that any person shall retain any property, or intentionally induces the person so deceived to do or omit to do anything which he would not do or omit if he were not so deceived, and which act or omission causes or is likely to cause damage or harm to that person in body, mind, reputation or property, is said to 'cheat'. A dishonest concealment of facts is a deception within the meaning of this section.¹

Examples

- ✓ A, by exhibiting to Z a false sample of an article, intentionally deceives Z into believing that the article corresponds with the sample, and thereby, dishonestly induces Z to buy and pay for the article. A cheats.
- ✓ A, by pledging as diamonds article which he knows are not diamonds, intentionally deceives Z, and thereby dishonestly induces Z to lend money. A cheats.

Whoever cheats shall be punished with imprisonment of either description for a term which may extend to one year, or with fine, or with both.²

Constituents of Cheating: An act may be consider as cheating when the following constituents is completed-

- ✓ **Acting Dishonestly:** The term 'acting dishonestly' has been defined under section 24 of Indian Penal Code. It is defined as, "when the doing of any act or not doing of any act causes wrongful gain of property to one person or a wrongful loss of property to a person, the said act is done dishonestly."
- ✓ **Property:** Property has a much wider meaning. It does not only include money but other things as well which can be measured in the terms of money. The property should be in a complete ownership of the person and he must have the full right to enjoy its possession.
- ✓ **Fraudulently:** Being fraudulent means which involves deception mainly criminal deception. It is characterized by fraud. According to section 25 "a person is said to do a thing fraudulently if he does that thing with intent to defraud but not otherwise."
- ✓ **Mens Rea:** Mens rea is the intention or action to constitute a crime. It is a mental state of an offender while committing a crime. It has to be proved beyond any doubt that the accused has actively contributed in a crime and that crime has affected another person's property.

The Supreme Court of India on March 17, 2015 in *Vesa Holdings P. Ltd. v. State of Kerala*³ has held that even in a case where allegations are made in regard to failure on the part of the accused to keep his promise, in the absence of a culpable intention at the time of making initial promise being absent, no offence under Section 420 of the Indian Penal Code can be said to have been made out. A bench comprising of Hon'ble Judge *V. Gopala Gowda and C. Nagappan JJ.* Observed that if the intention to cheat has developed later on, the same cannot amount to cheating. In other words for the purpose of constituting an offence of cheating, the

¹ Explanation of Section 415 of Indian Penal Code 1860

² Section 417 of Indian Penal Code 1860

³ (2015). 8 Supreme Court Cases 293

complainant is required to show that the accused had fraudulent or dishonest intention at the time of making promise or representation. The settled proposition of law is that 'every breach of contract would not give rise to an offence of cheating and only in those cases breach of contract would amount to cheating where there was any deception played at the very inception'

Cheating in a Contract:

A mere breach of contract will not be a cheating. For the offence, prior dishonest intention is required. For example: A singer promised to perform in a certain concert and asked their organizer to arrange for an orchestra. The organizer made all the required arrangement as per the contract. The singer arrived at the concert place and everything was set to go. At the meantime, singer backed out from singing owing to his personal reasons. The organiser filed a case for cheating against the singer. There is a very thin line of difference between cheating and breach of contract. For any sort of cheating, there has to exist a deceiving content right from the beginning of the contract.

Where a Person, Fraudulently or Dishonestly Induces a Person to Deliver any Property:

- ✓ As it is clear by now, mere dishonest intention or deceit will not be sufficient for cheating. Meeting of these two in order to induce the other person to deliver their property and making them do something which they would not have done otherwise, is cheating.
- ✓ A mere breaking of social promises won't amount to cheating.
- ✓ The person being cheated must suffer damage or harm in body, mind, reputation or property and the damage must be a consequential result of cheating and must not be too remote. The loss suffered because of cheating must not be vague.

Cheating is a Criminal Act or Mere Civil Wrong:

A civil wrong is a matter pertaining only between two parties. Eg.- breach of contract, non-repayment of a loan, etc. Civil wrongs are matter which do not harm the society in any way. Act which has the tendencies to harm the society at large is called a criminal wrong. Cheating is both a civil as well as criminal wrong in the same way as defamation is. When a criminal proceeding is set into motion several disabilities arises, for example- difficulty in applying for passport. Therefore, the court sees to it that cheating is not used as a tool to harass the offender. Court applies its brain and in every case of cheating. If the court thinks that the effect of cheating is more civil in nature it sets civil procedure is set into motion. Although, in few cases such as chit fund cases where large stake of people is involved, a cheating is often dealt criminally.

Cheating by Personation:

'A person is said to "cheat by personation"⁴ if he cheats by pretending to be some other person, or by knowingly substituting one person for another, or representing that he or any other person is a person other than he or such other person really is. Explanation - the offence is committed whether the individual personated is a real or imaginary person.

Illustration:

- ✓ A cheats by pretending to be a certain rich banker of the same name. A cheats by personation.
- ✓ A cheats by pretending to be B, a person who is deceased. A cheats by personation.

There must be an essence of cheating along with personating. The cheating is essential ingredient for the offence. Where a person cheats another by deceiving himself to be someone else, he is guilty under section 416 IPC and punished under section 419 IPC. Punishment under this section is imprisonment, which may extend to three year along with fine⁵.

When Does Breach of Contract Amount to Cheating:

Cheating	Breach of Contract
It is mentioned u/s 415 to 420 of Indian Penal Code, 1860.	It is mentioned u/s 73 of Indian Contract Act, 1872.
It is dealt under criminal law.	It is dealt under civil law.
It is a dishonest act done in order to gain advantage over the other.	It is a cause of action which occurs when the binding agreement is not performed.
In its intention to deceive exists at the time when inducement is made. In the beginning, only the person must have fraudulent intention regarding the promise to constitute it as an offence of cheating.	In it the malice intention does not exist from the beginning of the contract. The breach is done due to some reasons at the time when it is about to get binding.

In *S.W. Palanitkar v. State of Bihar*⁶ - the Supreme Court held that to convict a person for the offence of cheating there should be pre-existing dishonest or fraudulent intention of the person from the beginning but in case of Breach of Contract the dishonest intention is not present in the beginning of the agreement.

⁴ Section 416 of Indian Penal Code
⁵ Section 419 of Indian Penal Code
⁶ 2001(10) TMI 1150

Legal Regime for Prohibition of Fraud:

Fraud in IPC: Fraud is nowhere defined in criminal law. It is an act of deliberate deception with the design of securing something by taking unfair advantage of another. It is a deception in order to gain by another's loss. Whenever the term fraud or defraud appears in the context of criminal law, two things are automatically to be assumed.

- ✓ First- deceit or deceiving someone and
- ✓ Second- injury to someone because of such deceit.⁷

An implication of fraud is found in these following sections of IPC namely- Sec. 421, Sec. 422, Sec. 423 and Sec. 424.

- ✓ Fraudulent removal or concealment of property to prevent distribution among creditors (Section 421 IPC)
- ✓ Fraudulently preventing debt being available for creditors. (Section 422 IPC)
- ✓ Fraudulent execution of deed of transfer containing false statement of consideration. (Section 423 IPC)
- ✓ Fraudulent removal or concealment of property. (Section 424 IPC)

Fraud in Contract Act: 'Fraud' means and includes any of the following acts committed by a party to a contract, or with his connivance, or by his agent, with intent to deceive another party thereto or his agent, or to induce him to enter into the contract⁸:-

- ✓ 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.

Explanation: Mere silence as to facts likely to affect the willingness of a person to enter into a contract is not fraud, unless the circumstances of the case are such that, regard being had to them, it is the duty of the person keeping silence to speak, or unless his silence, is, in itself, equivalent to speech. Illustrations: A sells, by auction, to B, a horse which A knows to be unsound. A says nothing to B about the horse's unsoundness. This is not fraud in A.

In order to amount to Fraud, an act must be confined to acts committed by a party to contract with an intention to deceive another party or his agent or to induce him to enter into a contract. Fraud, which vitiates the contract, must have a nexus with the acts of the parties entering into the contract. This definition highlights the precondition to prove the intention of the person who has committed Fraud. If that person has willingly committed a Fraud, then he will be punished. Here the person means himself or his agent. The acts which include fraud are wrong suggestions or concealment of facts or false promises or any fraudulent act to deceive others.

Fraud in Company Act 2013: The financial/ corporate frauds and scams which have taken place in India, required the attention of the Law makers. It was high time to evaluate the high standards in corporate governance and implement stringent provisions to tackle corporate Fraud. The problem was on the rise both in its frequency and severity. The increasing rate of white-collar crimes demanded stiff penalties, exemplary punishments and effective enforcement of law with the right spirit. Examples: Our country has witnessed several corporate Frauds, till date e.g. Rs. 5,000 crore Harshad Mehta scam in 1992, Rs. 7,000 crore Satyam fiasco in 2009, the Rs. 27,000 crore Sahara fraud case which started in 2010 and is sub-judice at the Supreme Court currently.

The new Companies Act, 2013, focuses on the issues related to corporate Fraud. It is defined in Explanation of Section 447 of the Act. "Fraud" in relation to affairs of a company or anybody corporate, includes any act, omission, concealment of any fact or abuse of position committed by any person or any other person with the connivance in any manner, with intent to deceive, to gain undue advantage from, or to injure the interests of, the company or its shareholders or its creditors or any other person, whether or not there is any wrongful gain or wrongful loss. Where 'Wrongful Gain' means the gain by unlawful means of property to which the person gaining is not legally entitled; and 'Wrongful Loss' means the loss by unlawful means of property to which the person losing is legally entitled. To fall under this definition, these actions, omissions, concealment of the facts, should be done to deceive or to gain undue advantage which shall result in loss to the company or its shareholders or its creditors or any other person associated with the company and it may result in wrongful gain or wrongful loss. Any person who is found guilty of fraud shall be punishable with imprisonment for a term which shall not be less than six months but which may extend to ten years and shall also be liable to fine which shall not be less than the amount involved in the fraud, but which may extend to three times the amount involved in the fraud. Where the fraud in question involves public interest, the term of imprisonment shall not be less than three years.⁹As the punishment for Fraud is both imprisonment and fine, it is considered a

⁷ Fraud as a crime is nowhere defined in the Indian Penal Code

⁸ Section 17 of the Contract Act-1872

⁹ Section 447 of the Companies Act 2013

non-compoundable offence. It shows that, the commission of Fraud has become a serious offence in the eyes of law. The Act has provided punishment for fraud under section 447 and around 20 sections of the Act talk about fraud committed by the directors, key managerial personnel, auditors and/or officers of company.

Fraud/ Cheating	
Cheating	Fraud
It is mentioned u/s 415 to 420 of Indian Penal Code, 1860.	Implications of fraud are mentioned in section 421, 422, 423, 424 of Indian Penal Code, 1860.
It is a dishonest act done in order to gain advantage over the other.	It is a deliberate deception to secure unfair advantage over of the other. It is done to gain by another's loss.
In order to maintain suit for cheating there are two situations which are necessary subscribed in section 415 i.e. deception and inducement.	In order to maintain the suit for fraud intention to deceive is sufficient.
Cheating is not limited only to contracts.	Fraud basically relates more to contracts.

Recent Trends of Frauds:

Frauds can be seen in different modes in financial institutions, educational institutions, medical services and others as well. Eg. hawala transactions (1991), ponzi schemes, fake currency, cheque forgery, advancing loans without adequate due diligence, siphoning of investors' money through fictitious companies, use of fictitious government securities, tax evasion and money laundering, black money stashed abroad, cybercrime-debit/credit card fraud, identity theft, fake demat accounts, benami accounts, collusive frauds emanating kickbacks to employee of financial institutions, use of forged instruments such as stamp papers and shares, violation of know your customer (KYC) norms, manipulation circular trading and stock etc.

Bribery and Corruption: Corruption is one of the biggest challenges faced by the Indian economy. Various surveys and studies conducted by industry bodies like Transparency International have identified corruption as a key risk for Indian corporates. India ranked 79 among the 176 countries included in Transparency International's Corruption Perceptions Index - 2016.¹⁰ Some of the key reasons for high corruption in India are the lack of a strong legal framework and enforcement of anticorruption laws, red-tapism and a result-oriented approach.

Terrorist Financing: It involves the raising and processing of assets to supply terrorists with resources to pursue their activities. While money laundering and terrorist financing differ in many ways, they often exploit the same vulnerabilities in financial systems that allow for an inappropriate level of anonymity and non-transparency in the execution of financial transactions.

Money Laundering: The goal of a large number of criminal acts is to generate a profit for the individual or group that commits the act. Money laundering is the processing of these criminal proceeds to disguise their illegal origin. This process enables the criminal to enjoy profits without jeopardizing their source.

Tax Evasion: The general modus operandi to evade tax include wrongly availing TDS, non-registration, short payment of taxes, wrong classification and undervaluation of services.

Cybercrime: Financial cybercrime in India has been steadily increasing over the years. For the year 2015-16, the Reserve Bank of India (RBI) reported 16,468 cyber crimes related to ATM, debit card, credit card and net banking frauds. The number of frauds reported by the RBI were 13,083 in the year 2014-15 and 9,500 in the year 2013-14.¹¹

Type of case	2013	2014	2015	% Increase / Decrease in 2014 since 2013	% Increase / Decrease in 2015 since 2014
Cheating using computer as a medium or target.	-	1115	2255	-	102.2
Forgery using computer as a medium or target	747	63	45	-91.5	-28.6
Criminal breach of trust/fraud using computer as a medium or target	518	54	42	-89.6	-22.2
Counterfeiting using computer as a medium or target	59	10	12	-83.0	20.0

Table: Report of National Crime Record Bureau (NCRB) on financial cybercrime in India

¹⁰ Corruption Perception Index 2016. Available at - https://www.transparency.org/news/feature/corruption_perceptions_index_2016

¹¹ Medianama. (April, 2017). RBI reported 16,468 instances of financial cyber crime in 2015-16. Available at - <https://www.medianama.com/2017/04/223-rbi-cyber-crime-fraud/>. Retrieved on - 12.12.2017

The RBI set up the Reserve Bank Information Technology Pvt Ltd (ReBIT) to take care of its IT requirements, including the cyber security needs of the bank and its regulated entities. ReBIT will focus on IT and cyber security including research for the financial sector and assist in IT systems audit and assessment of RBI regulated entities, in addition to implement and manage internal or system wide IT projects. The agency will have four main verticals it will work in-cyber security, research and innovation, systems audit and project management.

A legal framework is required for security of digital wallets operating in the country as with digital payments on the rise, and digital heists and frauds becoming common. In India, most notably, over 3.2 million debit card details were likely stolen by hackers from ATMs and POS machines in October 2016. The National Payments Corporation of India (NPCI) said that the complaints of fraudulent withdrawal are limited to cards of 19 banks and 641 customers. The total amount involved is Rs. 1.3 crore. More recently, Bank of Maharashtra reported a loss of Rs 25 crore in March as frauds exploited a bug in their UPI application and core banking software.¹²

Data Security: In addition to website defacement and distributed denial of service, hackers have been making use of social media to launch more sophisticated attacks. Hacking attacks are tailored to target a particular organisation or entity and are often focussed on gathering valuable sensitive data.

Incorrect KYC Details: KYC details are collected and assessed by the institution at the time of customer onboarding as well as during re-KYC. A fraudster can find an opportunity to use incorrect KYC details during the customer lifecycle to commit fraud. Some examples:- Tampering of KYC details; Fraudulent KYC details such as a fake PAN being provided by the investor, change in name and other personal details not being updated, leading to opportunities for fraudsters to remit money to incorrect bank accounts and dummy customers; Units of different account holders with the same or similar name getting consolidated despite varying bank details and addresses in different folios; Mismatch between folios (schemes) consolidated vis-à-vis those requested for consolidation as per the customer application etc.

Misappropriation, Siphoning of Funds by Brokers or Intermediaries: The broker cheating the investor or account holder by taking a blank cheque and later misusing the same, Dormant accounts such as mutual fund investments with long-term maturity or redemption not being monitored by investors regularly, making them susceptible to fraud, Employees taking undue advantage of the lack of segregation of duties and manipulating the settlement or clearing account reconciliations.

Incorrect Commission or Incentives: Lax internal controls may give way to malpractices such as creation of agent or broker codes in the system and collusion in order to avail of extraneous commission and incentives. For example:- Employees creating fictitious agent or broker identities with a motive of personal profiteering and misappropriating the commission or incentives passed on to the other agents or brokers.

Front Running and Insider Trading: In order to pass on the benefit of windfall gains of the stock market to investors, the broker may resort to unethical practices such as front running and insider trading. For example:- Broking house being paid 'under the table' in order to portray the company's stock as the favorite, causing the investor to buy the stock; A broker buying shares based on insider information from companies, without any structured information that recommends the purchase; Analysts and brokers buying shares in a company just before the broking house recommends the stock as a strong buy etc.

Missing Dividend Payments or Discrepancies: The investor may be lured by a broker or other intermediaries to put money in stocks with supposedly attractive returns. These intermediaries may collude with sham companies and cause a discrepancy in dividend payments to investors. For examples: Diversion of dividend payments to dummy customers, Incorrect intimation of record date, dividend percentage and ex-dividend NAV by the AMC excess or short payouts to investors, Dividend pay-out files not being verified with dividend registry excess or short pay-outs to investors.

Risk in Mobile Banking: There are two types of mobile financial services that are currently offered in the Indian market- mobile banking and mobile wallets. Being an easy and convenient mode of transacting it has been rising in value usage & volume of transactions by mobile banking. This move, on one hand, enhances the convenience and adoptability of a mobile wallet and on the other, makes it more susceptible to fraud risks.

✓ 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.

✓ Creating fake and non-existent users on the mobile financial services platform: Most of the banks appoint a third party vendor to develop a mobile application to be integrated with their core banking system. The vendor may create two unauthorized users with rights to initiate and verify transactions, and transfer funds from the organisation to his associates' wallets, effectively stealing money from the bank.

¹² Medianama. (April, 2017). RBI reported 16,468 instances of financial cyber crime in 2015-16. Available at- <https://www.medianama.com/2017/04/223-rbi-cyber-crime-fraud/>. Retrieved on – 12.12.2017

- ✓ Malware: The increase in the number of mobile banking users is accompanied by a rise in attacks through malware.
- ✓ Data theft: Mass attacks are possible through the theft of credentials which can be used for personal benefits.
- ✓ SIM swap: SIM swap means replacing the old SIM with a new one, when the old gets lost or damaged, or when one needs a differently sized SIM card. If a fraudster manages such a swap, he can carry out numerous fraudulent transactions using the mobile number of the victim. For instance, the valid mobile station international subscriber directory number (MSISDN) is moved to another handset. The user has no access to their account and receives no notification. The user with the other handset, on knowing the PIN, can transact in the account.

✓ Fake or similar interface apps: Fake applications, with exactly the same user interface as the original application, are being created to steal confidential information shared by the user.

Risk in Mobile Wallets: Increased risk of money laundering: Transfer of money into and out of a mobile wallet 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.

Unauthorized deductions from the wallet of a customer (especially a dormant or infrequent customer account): Employees of the mobile wallet service provider may misuse the balance stored in the wallet of a customer by making unauthorized deductions. Moreover, in case of a mis-happening to a customer with no nomination facility, the balance in the customer's account is not passed on to his family members and remains with the service provider, which ultimately becomes a low-hanging fruit for the fraudsters.

Failure to conduct proper due diligence of 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 rotated with minimum transaction fees.

No auto log off facility: An individual usually opens the application on his mobile device for availing of the services and closes the application, instead of logging out. If the mobile device is stolen or lost and a fraudster opens the application, he can misuse the remaining balance in the service provider's wallet.

Fraud Risks in Insurance Companies:

Large accumulations of liquid assets make insurance companies attractive for loot schemes. These companies are under great pressure to maximize the returns on investing the reserve funds, making them vulnerable to high-yielding investment schemes.

The insurance industry has witnessed an increase in the number of fraud cases over the last couple of years. A growing number of organizations are realizing that frauds are driving up the overall costs of insurers and premiums for policyholders, which may threaten their viability and also have a bearing on their profitability. To keep these risks under check, a detailed framework for insurance fraud monitoring has been laid down with effect from 2013 -14 and is applicable to all insurers and reinsurers.

- ✓ Policy holder and claims fraud: Policy holder committing fraud against the insurer at the time of purchase and/or execution of an insurance product
- ✓ Intermediary fraud: Intermediaries committing frauds against the insurer and/or policyholders
- ✓ Internal fraud: Employees commit fraud suo moto or in collusion with external parties or amongst themselves against the insurer

Broad Categories of Fraud Risks in the Insurance Sector:

Misrepresentation: Misrepresenting critical information relating to a profile (incorrect income, educational qualification, occupation, etc). For example: The proposal form mentioned that the client had a shop in the market, whereas investigations revealed that the client was a small-time vendor sitting on a footpath.

Forgery or tampering documents: Forging the customer's signature in any document, proposal or any supporting document. For example: The client (staying in one city) and working as a surgeon was required to countersign the application form for some corrections. The form came back and it was found that the signatures were forged by the advisor, who was the client's brother.

Bogus Business: Proposal forms submitted for non-existent customers. For example: A sales manager or broker logs in the proposal of a non-existing client.

Cash Defalcation: Agent collecting the premium but not remitting the cheque to the insurance company, owing to which the insured has no coverage. For example: The advisor had collected the premiums from the customer and had not deposited the same for almost a month; it came to the insurer's notice when the customer was sent the lapsed letter.

Mis-Selling: A selling practice wherein the complete, detailed and factual information of a product is not given to the customer (also called product misinformation); can include incomplete or incorrect representation of the terms and conditions such as guaranteed returns, rider features, charges, linked product vs endowment, facility of top-up vs regular premium, premium holiday, etc. For example: The customer was given a cover of 1 lakh INR and the premium was 5 lakh INR. This was a clear case of mis-selling as even the facility of a top-up was not explained to the client.

Pre-Signed Forms: Obtaining pre-signed blank forms and filling the address change request (ACR)/contact number change (CCR) without actually physically seeing the client or satisfying oneself about the client. For example: While the proposal form mentioned that the customers were working in an electronic agency, in reality they were working in some other business.

Doctor's Nexus: Doctor being involved with the perpetrators in committing life insurance fraud. For example: A doctor gave clean medical reports, while the fraudster influenced the doctor to conceal the information.

Conclusion: Regulatory and Legislative Landscape

The RBI issued a master circular in year 2015 on 'Frauds – Classification and Reporting'¹³. The circular has fixed the responsibility of preventing frauds on banks, exposing them to a completely new horizon of financial risks. Further, banks are now required to report to the RBI the 'complete information about frauds and the follow up action taken thereon'. With the shift from traditional ways of responding to frauds to new ways of robust reporting and risk monitoring systems, banks can now control financial and reputational risks more efficiently.

With the rapid growth in users and wider coverage of mobile phone networks, mobile banking is increasingly coming up as a significant delivery channel for extending banking services to customers. Putting the onus on banks, the RBI has issued operative guidelines to regulate this channel, suggesting reporting of suspicious transactions to its financial intelligence unit. Owing to the heavy reliance on telecom operators for its services, the prevention and detection of frauds in mobile banking have become even more complex. To keep a check on frauds, banks need to incorporate a greater level of scrutiny, by deploying advanced tools and technology capable of protecting the customers against unethical activities.

The Insurance Regulatory and Development Authority (IRDA) has issued an Insurance Fraud Monitoring Framework (IFMF) in order to guide the implementation of measures to minimize the vulnerability against frauds in the insurance sector. IFMF mandates for the insurance companies to set up a risk management committee, followed by disclosure of adequacy of the systems in place to safeguard against frauds. In order to reduce the exposure, the IRDA has mandated that insurance companies have fraud risk management systems for reinsurers. Proficiently designed processes, continuous monitoring and management of fraud risk will go a long way in keeping a check. In addition to this, a well-established fraud risk management system will answer key questions related to complicated threats.

The NBFC sector has evolved considerably in terms of its size, operations, technological sophistication, as well as entry into newer areas of financial services and products. NBFCs are now deeply interconnected with entities in the financial sector, on both sides of their balance sheets. Being financial entities, they are as exposed to these risks as banks. Acknowledging the risk factors applicable to NBFCs, the RBI has issued a master circular on reporting of frauds. The circular lays down a road map similar to the one for banks. Akin to the banking sector, the circular has fixed the responsibility of preventing frauds on NBFCs, subjecting them to uncertain financial risks. The RBI has further mandated the reporting of frauds by NBFCs in a prescribed format. This is expected to pose certain challenges to NBFCs and may require many to re-visit their business model. These regulations call for NBFCs to invest in upgrading their systems and processes and equip them with advanced tools to prevent as well as detect frauds in parlance with the emerging threats by way of technology.

References:

1. How a breach of contract would amount to cheating. (2015). Available on- <https://www.lawkam.org/criminal/breach-contract-amount-cheating/6179/>
2. Anubhav Pandey. (2017). Indian Penal Code on fraud and cheating. Available on- <https://blog.ipleaders.in/cheating-fraud/>
3. Dr. Ashok Dhamija. (2015). Breach of contract will not be cheating unless deception played at the very inception. Available on - <http://tilakmarg.com/answers/breach-of-contract-will-not-be-cheating-unless-deception-played-at-the-very-inception/>
4. The Companies Act 2013. Available at- http://www.mca.gov.in/MCAsearch/search_table.html
5. Fraud and Companies Act 2013. Available at- <http://www.rna-cs.com/fraud-and-the-companies-act-2013/>
6. Pandey. A. (2017). Cheating – Constituents, punishment and other legal issues related to cheating. Available at – <https://blog.ipleaders.in/cheating-constituents-punishment-legal-issues-related-cheating/>
7. ASSOCHAM. (June 2015). Current fraud trends in financial sector. Available at <http://rbidocs.rbi.org.in/rdocs/Speeches/PDFs/DGKCAF290713.pdf>. Accessed on 12.01.2018
8. Association of Certified Fraud Examiners. (2014). Reports on the nations on occupational fraud and abuse. Available at - <http://www.acfe.com/rtnn/docs/2014-report-tonations.pdf>

¹³ RBI Circular- Frauds – Classification and Reporting'. Available at- https://www.rbi.org.in/scripts/BS_ViewMasCirculardetails.aspx?id=9878. Accessed on 14.01.2018

9. Frauds in the Banking Sector: Causes, Concerns and Cures. Available at- https://www.rbi.org.in/scripts/BS_SpeechesView.aspx?Id=826. Accessed on 13.01.2018
10. Business Standards. About Rs 8,000 cr service tax evasion detected during 2013-14 Available at- http://www.business-standard.com/article/pf/about-rs-8-000-cr-service-tax-evasion-detected-during-2013-14-114040600173_1.html
11. Taxman. (2017). Companies Act with Rules.
12. Uma Shankar Gopalika Vs. State of Bihar and Another [(2005) 10 SCC 336]
13. All Cargo Movers (India) Private Limited Vs. Dhanesh Badarmal Jain (2007)14SCC 776
14. V.Y. Jose and Another Vs. State of Gujarat and another [(2009)3 SCC 78]
15. Vijayander Kumar and others Vs. State of Rajasthan and another [(2014) 3 SCC 389]