E-COMMERCE: GENERAL CHALLENGES AND STRIVE IN COMBATING E-FRAUDS

A DISSERTATION TO BE SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENT FOR THE AWARD OF DEGREE OF MASTER OF LAWS

SUBMITTED BY

[SUMBUL NAQVI]

[UNIVERSITY ROLL NO.12209900031]

SCHOOL OF LEGAL STUDIES

UNDER THE GUIDANCE

OF

[MS. DR. SANSKRITI SRIVASTAVA]

[ASSISTANT PROFESSOR]

SCHOOL OF LEGAL STUDIES

BBD UNIVERSITY

SESSION 2020-21

CERTIFICATE

This is to certify that the dissertation titled "E-COMMERCE: GENERAL CHALLENGES AND STRIVE IN COMBATING E-FRAUDS" is the work done by Sumbul Naqvi under my guidance and supervision for the partial fulfilment of the requirement for the Degree of Master of Laws in School of Legal Studies Babu Banarasi Das University, Lucknow, Uttar Pradesh.

I wish her/his success in life.

Lucknow
Date

Ms. Dr. Sanskriti Srivastava
Assistant Professor
School of Legal Studies
Babu Banarsi Das University

DECLARATION

Title of Dissertation, E-COMMERCE: GENERAL CHALLENGES AND STRIVE IN COMBATING E-FRAUDS"

I understand what plagiarism is and am aware of the University's policy in this regard.

Sumbul Naqvi,

I declare that:

(a) This dissertation is submitted for assessment in partial fulfilment of the requirement for the award of degree of Master of Laws.

(b) I declare that this DISSERTATION is my original work. Wherever work from other source has been used i.e., words, data, arguments and ideas have been appropriately acknowledged.

(c) I have not permitted, and will not permit, anybody to copy my work with the purpose of passing it off as his or her own work.

(d) The work conforms to the guidelines for layout, content and style as set out in the Regulations and Guidelines.

Lucknow
Date :

SUMBUL NAQVI
ENR. NO. 1220990031
LLM (2022-2023)
(CORPORATE COMPANY LAW)

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to all who guided me and supported me in the completion of this work. Foremost, I am grateful to my supervisor, Ms.Dr. Sanskriti Srivastava for her continuous guidance, patience and support throughout the work. It was for his immense knowledge and expertise that provided due direction to this work and enabled me to understand and appreciate the topic efficiently. Furthermore, I would like to thank my parents for their continuous support and generosity throughout the year. I am also grateful to my classmates for their delightful company throughout this year. I would also like to thank our Dean for providing me an excellent academic environment in Babu Banarsi Das University Lucknow for legal study and research.

Lucknow
Date :

SUMBUL NAQVI
ENR. NO. 1220990031
LLM (2022-2023)
(CORPORATE COMPANY LAW)

LIST OF ABBREVIATIONS

- SCC- Supreme Court Cases
- HC- High Court
- Act - Act of Parliament
- IPC- Indian Penal Code
- PC Act- Prevention of Corruption Act
- NI Act- Negotiable Instrument Act
- BR Act- Banking Regulation Act
- PMLA- Prevention of Money Laundering Act
- IT Act- Information Technology Act
- RBI- Reserve Bank of India
- ADA - Americans with Disabilities Act
- ADR - Alternative Dispute Resolution
- BAR - British Accreditation Registry
- CJ - Chief Justice
- COA - Court of Appeals
- CPC - Code of Civil Procedure
- CRPC - Code of Criminal Procedure
- DUI - Driving Under the Influence
- FIR - First Information Report
- IPO - Initial Public Offering
- LLM - Master of Laws
- M&A - Mergers and Acquisitions
- NGO - Non-Governmental Organization
- OSHA - Occupational Safety and Health Administration

- PTO - Patent and Trademark Office
- SC - Supreme Court
- TRO - Temporary Restraining Order
- USPTO - United States Patent and Trademark Office
- WTO - World Trade Organization

LIST OF CASES

ASIF AZIM CASE

This is the first example of cyber fraud. The most notable development was India's first successful cybercrime conviction in February. On 5 February 1998, 24-year-old Asif Azim was convicted by Delhi Municipal Judge Gulshan Kumar of defrauding Sony India of a 29-inch color TV and wireless headphones worth Rs.500. 27,570. As a first-time offender, he was given a one-year suspended sentence and a personal bail of 20,000 rupees. Mr. Azim, who worked at his I-Energizer, a call center in Noida, stumbled upon the details of his credit card for one of his customers, Mr. Barbara Kampa. Then he decided to shop for free. He created his email address on behalf of Kampa and used it to order on his website of Sony India India using his credit card information for Barbara on May 8 last year. Did. Sony India's credit card company Citibank ruled the transaction legitimate and the product was delivered to Azim's home as early as next week. An email was sent to Campa with a photo of Azim receiving the product.

At the end of June, when Mr. Kampa realized he had been charged for an item he didn't buy and called his bank, the situation turned into panic. After consulting with her, Citibank reported that the transaction was fraudulent and void. In other words, Sony had to pay for the transaction. The matter was then reported to her CBI. The CBI team determined that the Internet Protocol her address from which the message originated was in Noida, not the United States. They then identified the source computer he was using. When the CBI confronted him, Azim confessed everything. He said he did it just to get something for free. Azim was convicted under Sections 418, 419 and 420 of the Indian Penal Code. The CBI arrested Arif Azim on online fraud charges and registered the case under IPC Article 420. The conviction boosted public confidence in law enforcement's ability to detect cybercrime and the resilience of India's justice system to meet the new challenges of the cyber age.

HARSHAD MEHTA SCAM (1992)

Harshad Mehta, a stockbroker, orchestrated a massive securities scam in the early 1990s. The case involved fraudulent practices in the banking sector, such as manipulating stock prices, issuing fake bank receipts, and exploiting loopholes in the banking system. The scam led to significant losses for banks and investors. Harshad Mehta was convicted and sentenced to imprisonment.

SATYAM SCANDAL (2009)

The Satyam Computer Services scandal was a corporate fraud case that exposed fraudulent financial reporting by the company's management. The scam involved inflating profits, creating fictitious assets, and manipulating financial statements. Satyam's chairman, Ramalinga Raju, admitted to the fraud, and several executives were charged. The case highlighted the need for improved corporate governance and auditing standards.

VIJAY MALLYA AND KINGFISHER AIRLINES (2012 ONWARDS)

Vijay Mallya, the former chairman of Kingfisher Airlines, was involved in a high-profile case of loan default and financial irregularities. Kingfisher Airlines amassed substantial debt and failed to repay loans taken from various banks. Mallya was accused of diverting funds, misusing loans, and non-disclosure of assets. He was declared a wilful defaulter, and legal proceedings are ongoing.

PUNJAB NATIONAL BANK (PNB) FRAUD (2018)

One of the largest banking frauds in India, the PNB fraud involved jeweler Nirav Modi and his companies. Nirav Modi and his associates fraudulently obtained Letters of Undertaking (LoUs) from PNB, which were used to secure credit from other banks abroad. The scam amounted to billions of dollars, and Nirav Modi fled the country. Several bank officials were implicated, and the case highlighted the need for stricter oversight and risk management in the banking sector.

TABLE OF CONTENTS

- **Easier to Retarget Customers**

- **DISADVANTAGES**

  - **Limited Customer Service**
  - **Lack of Instant Gratification**
  - **Inability to Touch Products**
  - **Reliance on Technology**
  - **Higher Competition**

PERFECT EXAMPLE OF E-COMMERCE

E-COMMERCE: A CHANCE TO EXECUTE FRAUD

BANKING

- **Business to Consumer (B2C)**
- **Business to Business (B2B)**
- **Consumer to Consumer (C2C)**
- **Consumer to Business (C2B)**

RISK AT BANKING

- **Credit risk**
- **Market risk**
- **Liquidity risk**
- **Operational risk**
- **Cyber security risk**
- **Compliance and regulatory risk**
- **Reputation risk**

MODES OF PAYMENT IN BANKING SYSTEM AND ITS RISKS

- **Credit Cards**
- **Secure Electronic Transaction (SET)**
- **Confidentiality**
- **Integrity**
- **Authentication**
- **Non-Repudiation**

FRAUDS

NATURE OF ELECTRONIC FRAUD IN INDIA

TYPES OF ELECTRONIC FRAUDS VIZ A VIZ BANKING SECTOR

- **Phishing**
- **Identity theft**
- **Online fraud**
- **Credit card fraud**
- **Account takeover**
- **Investment and Trading Fraud**

MODERN AREAS OF FRAUDS

LAW RELATED TO BANKING FRAUDS IN INDIA

- **Indian Penal Code (IPC)**
- **Prevention of Corruption Act, 1988**
- **Negotiable Instruments Act, 1881**
- **Banking Regulation Act, 1949**
- **Prevention of Money Laundering Act, 2002 (PMLA)**
- **Information Technology Act, 2000 (IT Act)**
- **Reserve Bank of India (RBI) Guidelines and Circulars**

DIRECTIVES BY THE RESERVE BANK OF INDIA REGARDING REPORTING OF BANKING FRAUDS:

DETAILED STUDY AND COVERING OF LAWS RELATED TO BANKING FRAUDS IN INDIA

- **INDIAN PENAL CODE**
    - **Section 420**
    - **Section 406**
    - **Section 409**
    - **Section 415**
- **PREVENTION OF CORRUPTION ACT 1988**
    - **Bribery Offenses**
    - **Illegal Gratification**
    - **Abuse of Official Position**
    - **Criminal Misconduct**
- **NEGOTIABLE INSTRUMENTS ACT, 1881**
    - **Section 138**
    - **Section 139**
    - **Section 140**
    - **Section 141**
    - **Section 143**
- **BANKING REGULATION ACT, 1949**
    - **Section 5(b)**
    - **Section 10**
    - **Section 35A**
    - **Section 46**

- **Section 46A**

- **PREVENTION OF MONEY LAUNDERING ACT 2002**
    - **Money laundering crime**
    - **Reporting and recordkeeping requirements**
    - **Penalties**
- **INFORMATION TECHNOLOGY ACT, 2000 (IT ACT)**
    - **Electronic Documents and Digital Signatures**
    - **Secure Electronic Records and Secure Digital Signatures**
    - **Electronic Funds Transfer**
    - **Cyber Frauds and Offenses**
    - **Cybersecurity and Data Protection**

DETERRENT EFFECT OF BANKING LAWS ON SOCIETY

CASE LAWS

COMPARISON OF INDIA BANKING LAWS WITH FOREIGN BANKING LAWS

INDIAN BANKING LAWS AND ITS IMPLEMENTATION:

TRADITIONAL AND MODERN AREAS OF FRAUDS

- **Traditional Areas of Banking Frauds:**
- **Modern Areas of Banking Frauds**

PREVENTIVE AND CURATIVE MEASURES VIS-A-VIS

- **Preventive Measures**
- **Curative Measures**

BANKING FRAUDS AND CYBER CELL

LINE OF INVESTIGATION BY CYBER POLICE IN E COMMERCE AND BANKING FRAUDS

MEASURES IF CYBER POLICE FAILS TO REGISTER COMPLAINT IN BANKING FRAUDS

FOREIGN BANKING LAWS AND ITS IMPLEMENTATION IN FOREIGN COUNTRIES

KEY REASONS OF FRAUDS IN INDIAN BANKING SYSTEM AND INTERNATIONAL BANKING SYSTEM

CROSS BORDER CASE LAWS ON BANKING LAWS

IMPORTANT PREVETIVE WAYS TO COMBAT BANKING FRAUDS AND SAFEGUARDS

GRAPHICAL INDICATION OF BANKING FRAUD CASES

CONCLUSION

RECOMMENDATIONS

- **Independent expert executives**
- **Know your market**
- **Internal Rating Agencies**
- **Monitoring of vandalism at the local level**
- **Strong punitive measures against third parties**
- **Strict Laws to Prevent Fraudulent Financial Reporting**
- **Means of Ground Reconnaissance**
- **Dedicated departments dealing with fraud cases**
- **Financial Education**
- **Transparent Recruitment and Appropriate Compensation**
- **Interagency coordination**

CHAPTER 1

INTRODUCTION

Cyber law broadly refers to all forms of electronic communication as well as other distinct online elements of internet technology. The area of law that governs legal issues when accessing the internet is known as cyber law. It implies that everything pertaining to, connected with, or any legal action taken by an internet user in cyberspace is covered by cyber law.

On the other side, the IT revolution has created a digital world, which is the biggest threat to the global legal system, for instance. Online transactions, digital signatures, and paperless contracts have forced the legal community to consider new issues and completely ignore geographical limits. Cybercrime is the name given to the new generation of crimes that have been made possible by the advent of the digital age. Without revealing his name, a person seated anywhere in the world can interact with another person. Because of this, the internet presented a number of difficulties for the government, as well as for business and individuals.

As we can see from the previous few decades, computing and communication have undergone a huge transformation, and utilisation of this information technology is growing quickly. New, quicker, and better technologies are occasionally introduced to the market. There was no such awareness of these technologies in earlier times, but as time went on, society began to become more and more interested in them because they were more affordable and dependable.

Moreover, the rate of technological advancement accelerated even further following the development of E-commerce, and individuals began utilising it more frequently. Second, the era of digital banking, where it is possible to transfer large sums of money quickly between accounts. In addition, the most significant development to be discussed is the proliferation of online employment opportunities, which allow people to earn money while relaxing at home in front of computers rather than working demanding field jobs that are even harder to obtain.

A system of electronic banking where banks claim that their systems are fool proof, and we're often hearing about online fraud as well as forgery in millions of Indian rupees.

Our privacy has been compromised by various social media citations, including issues such as leaking personal photos and confidential information, and obtaining other information through fake IDs.

Taking the recent trend of 'Phishing' the most unethical and fraudulent way of getting someone's personal information with the intention to blackmail that person by just giving him an unauthorised pop up and to hack his computer.

Cyber activities of all kinds are the largest platform for criminals to carry out vast amounts of criminal activity, and tracking such activities is the most difficult task. Cybercrime and computer crime are the same concept, but they are slightly different as the type of electronic means is the most important part of hacking an electronic device.

For example if one has a mobile phone or PC or laptop and there is no such network system in it such as Bluetooth, W-Fi, internet (2G, 3G or 4G) or infrared etc. then it is not possible to hack any electronic devices as hacking is impossible without the network. Thus, the cybercrime can be classified on the basis of victim in the following manner:

- Crime affecting Individual
- Crime affecting economy
- Crime affecting national security

CRIME AFFECTING INDIVIDUAL:

This is the main reason of cybercrime that has been initiated throughout the world. It is cybercrime that affects individuals. In this cybercrime, the victim is the computer user or someone who uses the computer in the victim's name. Criminals use her private access by gaining access to the victim's computer or account and violating the victim's privacy rights.

Computers are a common and important source for storing personal data and information. The Internet and computers have developed techniques to recover vast amounts of personal data in a very short time. Because of its capacity and ease of use, the technology is used everywhere from schools to hospitals, and used or abused by businesses to government and non-government banks.[1] Criminal privacy breaches can occur when certain data becomes available in cyberspace through hacking attacks or other accessible

[1] Laws on Cyber Crime: P .K. Singh, (2007) Book Enclave, Jaipur, Page 48.

methods.[2] This is also the case for violations of the right to privacy, which is now considered a fundamental right by the Supreme Court of India. Wireless service providers now use computers or the Internet to store and transmit their customers' personal information. This kind of data can be affected by this kind of cybercrime. This privacy invention is one of the most important forms of cybercrime.

In this form of cybercrime, criminals masquerade as identity theft and commit crimes under the guise of fraud and misrepresentation. As a result of such crimes, trust in the integrity of business transactions may be compromised. Because the victim is totally innocent and he is unaware of the crime he has committed, he remains shocked and surprised when the police approach him during the investigation of a particular case. The nature of this crime is cyber stalking. Stalking on the Internet refers to the act of harassing or contacting others without permission by using electronic media such as the Internet. The term "cyberstalking"[3] refers only to the use of electronic communication means such as the Internet, email, SMS, MMS as a means of stalking.

CRIME AFFECTING ECONOMY:

Information technology is growing rapidly and is used in all sectors of the economy, including industry, trade and services. The use of internet for economic and trade development is the need of the times. Using the Internet and computers in business is known as e-commerce. It is an electronic commerce that provides various procedures in high-tech business quickly and inexpensively. In this way, e-commerce can now cross borders without any problems. Merchants and businessmen were attracted to this mode of transferring large amounts of funds because the process was inexpensive. However, this method is not without its drawbacks.

Businessmen and ordinary people use this technology to save time, but criminals use this technology, unknown to ordinary Internet users, and use more advanced technology to more easily carry out their criminal activities. Technology. Criminal activities such as hacking and IP spoofing are common crimes that target businesses.[4] Fraud generally takes place on the Internet. Software piracy is a common crime today, but the purpose of

[2] https://www.business-standard.com/article/finance/sbi-ex-chief-pratip-chaudhuriarrested-sent-to-14-day-judicial-custody-121110200055_1.html

[3] https://www.verywellmind.com/what-is-cyberstalking-5181466

[4] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2741013

software piracy is simply to save money. Cybersquatting is also a way to commit cybercrime. The main purpose of these crimes is to obtain illicit profit. This is a new form of traditional crime, known as cybercrime.[5]

CYBER CRIME AFFECTING NATIONAL SECURITY:

Illegal acts in cyberspace that affect entire societies and nations are called cybercrimes against national security. Today the internet is used to spread ideas. If used by terrorist organizations to propagate such ideas, it not only poses a threat to national security, but also poses a great risk of destroying the telecommunications and information technology equipment itself in a terrorist attack. This form of cybercrime poses a threat both domestically and internationally. Cyber terrorism is a prime example of this crime. Terrorists use modern information technology to plan, raise money, propaganda, and communicate with each other to carry out their plans. [6]

Cyber warfare, on the other hand, is another way to carry out cyber crimes that adversely affect national security. First and foremost, computers and the Internet are an integral part of the military strategies of various nations around the world. When a country uses an enemy's intelligence, it poses a threat to that country, and this kind of activity undermines global peace and security.

LITERATURE REVIEW:

The Information Technology Act, 2000, Information technology is rapidly growing and used in all sectors of the economy including industry, commerce and services. The use of internet for the use of development of business and commerce is the need of the hours. The use of internet and computer in business is call e-commerce. This e-commerce provides various speedy and less expensive procedures in the high- tech business. Thus ecommerce has removed the national boundaries without any problem. Due to this, less expensive process attracted the traders and businessperson to use this mode for transferring the huge amount of money. However, this process is also not without disadvantages.

The businessman and common man uses this technology to save their time, but criminals use the technology which is unknown to the general user of the internet and the

[5] Chapter III; The Law Relating to Cyber Crime in India.
[6] Laws on Cyber Crime: P .K. Singh, (2007) Book Enclave, Jaipur, Page 58.

technology is more sophisticated technology which is more easier way to commit the criminal activities. The criminal activity as like hacking and IP spoofing are the common offence, which are going to commit against the economy. Generally, the frauds are going to be committed by using internet. Software piracy is the common offence in a day, the object behind software piracy is nothing but to save the money. Cybersquatting is another mode to commit the cyber-crime. The main object behind these offences is nothing but to gain wrongfully. This is new mode to commit conventional crime though, it is known as a cyber-crime.

SCOPE OF STUDY:

The scope of the study is to reach the very roots of the complex issues relating to the Cyber Crime and what are the issues that an individual face in the present scenario.

STATEMENT OF THE PROBLEM :

Firstly, the present research shall focus on some relevant facts and circumstances i.e.

E- Commerce and the trading through the Internet has become a reality and it will be there for a long. Any deal involving the transmission of electronic signals can be classified as E-Commerce. The unique ability of the internet to allow a company's marketing message to have a global reach and selectively target those consumers already predisposed towards actual purchase of the product, has spurred a rush among corporations both large and small, to set up shop on the internet.

CONCEPTUAL FRAMEWORK:

The findings of the present research would be based on the overall framework which includes the findings and rising issues of E-Commerce and the system to deal with and lastly as per law the present concept and scenario to deal with crimes related to E-Commerce. The concept would be made clearer with the help of other examples and laws.

OBJECTIVE OF THE STUDY:

1. The electronic commerce is all about commercial transactions, whether between the private individuals or commercial entities, which take place in or over electronic networks

2. Challenges face by individuals at present scenario to lead their lives on daily basis

3. To understand the legal Perspective of an individuals who are victim to the said crime.

4. To identify and study the safeguards for those victims from these criminals and cyber mafias.

HYPOTHESIS

The General Public is not aware about and it is one of the most controversial topic which we hardly see or heard. Secondly, the trauma that these individual face is in huge form. Lastly, as we know that being a victim there is no any deterrent effect of the law established with regards to the Cyber Crime and E-Commerce.

E-commerce frauds can vary based on the specific context and research focus. Hypothesis: The lack of robust security measures and weak authentication processes in e-commerce platforms contributes to an increase in fraudulent transactions. E-commerce platforms that do not prioritize strong security measures and fail to implement effective authentication processes may be more susceptible to fraudulent activities. The absence of stringent security measures creates opportunities for fraudsters to exploit vulnerabilities and engage in fraudulent transactions.

The increasing popularity and growth of e-commerce platforms lead to a corresponding rise in e-commerce fraud incidents. As e-commerce becomes more prevalent and widely used, the hypothesis suggests that the sheer volume of transactions and the expanding customer base provide a larger pool of potential targets for fraudsters. The growth in e-commerce activities creates a favorable environment for fraudsters to carry out their illicit activities. Insufficient consumer awareness and lack of education about online security contribute to a higher incidence of e-commerce frauds.

The lack of awareness and understanding among consumers regarding online security practices and common fraud schemes can make them more vulnerable to e-commerce frauds. Consumers who are not well-informed about the risks associated with online transactions may unknowingly engage in activities that expose them to fraudulent schemes. Inadequate regulatory oversight and enforcement of e-commerce platforms result in a higher prevalence of fraud incidents.

Further the weak regulatory oversight and lax enforcement of regulations pertaining to e-commerce platforms create an environment where fraudulent activities can flourish. Insufficient monitoring, failure to implement stringent compliance measures, and limited consequences for non-compliance may contribute to a higher occurrence of e-commerce frauds.

Technological advancements, such as the proliferation of mobile devices and increased connectivity, contribute to the growth of e-commerce frauds.

Explanation: This hypothesis proposes that technological advancements, while facilitating the convenience and accessibility of e-commerce, also create new avenues for fraudsters to exploit. The increasing use of mobile devices for online transactions and the expanding interconnectedness of devices and platforms may result in an elevated risk of e-commerce fraud incidents. Conducting thorough investigations, analyzing trends, and gathering empirical evidence are essential steps in evaluating the prevalence and underlying factors of e-commerce frauds.

RESEARCH QUESTIONS:

In the above stated objectives, the following questions are formulated.

1. Whether laws made on these crimes are more effective one and are people aware about it?
2. Whether the existing laws and the procedure established by Law is achieving its objectives?

AWARENESS IN SOCIETY ON BANKING AND E COMMERCE FRAUDS

Raising awareness in society about banking and e-commerce frauds is crucial to help individuals protect themselves and minimize the risk of falling victim to fraudulent activities. Here are some key aspects of awareness that can be promoted in society:

- Education and Information: Conducting educational campaigns and disseminating information about common types of banking and e-commerce frauds is essential. This includes providing information on phishing scams, identity theft, fake websites, email and phone scams, and other fraudulent practices. Public

awareness programs, workshops, and online resources can help individuals understand the risks and learn how to identify and prevent fraud.

- Safe Online Practices: Promoting safe online practices is vital in preventing e-commerce fraud. This includes advising individuals to use secure and trusted websites, protect their login credentials, regularly update their software and antivirus programs, and avoid clicking on suspicious links or downloading unknown attachments. Emphasizing the importance of strong passwords, multi-factor authentication, and safe browsing habits can significantly reduce the risk of fraud.
- Secure Payment Methods: Educating individuals about secure payment methods is crucial. Encouraging the use of reputable payment gateways, secure online banking platforms, and encrypted payment systems can help individuals make transactions with confidence. Promoting awareness about the risks associated with sharing credit card or bank account details and advising caution when making online payments can protect individuals from fraudulent activities.
- Verification and Vigilance: Creating awareness about the importance of verifying the credibility of sellers, websites, or service providers before making transactions is essential. Individuals should be encouraged to research and read reviews, check for security certificates, and be cautious of deals that appear too good to be true. Being vigilant about suspicious emails, messages, or phone calls and reporting any potential fraud attempts can contribute to early detection and prevention.
- Reporting Mechanisms: Encouraging individuals to report incidents of banking and e-commerce fraud is crucial. Publicizing and promoting the availability of reporting mechanisms such as dedicated helplines, complaint portals, or contacts for cybercrime units can ensure that victims have an avenue to report fraudulent activities. This helps law enforcement agencies and regulatory bodies gather data, investigate cases, and take appropriate action against fraudsters.
- Collaboration with Financial Institutions: Collaborating with banks, financial institutions, and e-commerce platforms is essential in raising awareness. These organizations can play a significant role in educating their customers, implementing robust security measures, and providing guidelines for safe online transactions. Collaborative efforts can include joint awareness campaigns, sharing

best practices, and providing resources to customers to enhance their knowledge and protection against fraud.

- Continuous Updates: Awareness programs should keep pace with evolving fraud techniques and trends. Regularly updating individuals with information on new types of frauds, emerging risks, and preventive measures ensures that they are equipped to tackle the evolving challenges in the digital landscape.
- By promoting awareness on banking and e-commerce frauds, individuals can develop a better understanding of the risks involved and adopt safe practices to protect themselves. It also creates a more vigilant society that is less susceptible to fraudulent activities and contributes to the overall security of the online ecosystem.

EXISTING LAWS AND THE PROCEDURE ESTABLISHED BY LAW IN BANKING LAWS AND E COMMERCE ACHIEVING ITS OBJECTIVES

Existing laws and the established legal procedures in banking and e-commerce aim to achieve several objectives related to consumer protection, fraud prevention, and maintaining the integrity of financial transactions. While the effectiveness of these laws and procedures may vary across jurisdictions, they generally serve the following purposes:

Consumer Protection: Banking and e-commerce laws provide a framework to protect the rights and interests of consumers. They establish rules and regulations that financial institutions and e-commerce platforms must follow to ensure transparency, fair practices, and the provision of adequate services to customers. These laws typically include provisions related to disclosure of terms and conditions, protection against unauthorized transactions, dispute resolution mechanisms, and avenues for seeking remedies in case of fraud or malpractice.

Fraud Prevention and Detection: Laws governing banking and e-commerce activities include provisions aimed at preventing and detecting fraudulent practices. They outline obligations for financial institutions and e-commerce platforms to implement robust security measures, conduct customer due diligence, monitor transactions for suspicious activities, and report fraudulent incidents to relevant authorities. These laws also

empower law enforcement agencies to investigate and prosecute offenders involved in banking and e-commerce frauds.

Regulatory Oversight: Legal frameworks establish regulatory bodies or authorities responsible for overseeing banking and e-commerce activities. These regulators enforce compliance with the applicable laws and regulations, conduct inspections, issue guidelines and directives, and take enforcement actions against entities that violate the rules. They play a crucial role in ensuring the soundness, stability, and integrity of the financial system and e-commerce ecosystem.

Dispute Resolution Mechanisms: Banking and e-commerce laws often provide mechanisms for resolving disputes between consumers and financial institutions or e-commerce platforms. These mechanisms may include alternative dispute resolution processes, such as mediation or arbitration, as well as access to courts for legal recourse. The objective is to provide a fair and efficient means for consumers to seek redress in case of disputes or fraudulent activities.

International Cooperation: In the globalized world of banking and e-commerce, laws and procedures are designed to facilitate international cooperation and information sharing. Cross-border fraud and financial crimes require collaboration between jurisdictions, and legal frameworks establish mechanisms for extradition, mutual legal assistance, and cooperation with international organizations to combat transnational fraud effectively.

Assessing the extent to which existing laws and procedures achieve their objectives requires an evaluation of their implementation, enforcement, and adaptation to evolving technological advancements. It also involves monitoring their effectiveness in deterring fraud, protecting consumers, and promoting a secure and trustworthy banking and e-commerce environment. Ongoing evaluation, periodic updates of laws and regulations, and continuous collaboration between stakeholders are necessary to ensure that these frameworks remain effective in achieving their intended objectives.

CHAPTER 2

CYBER LAW AND CONSTITUTION:

Cyber law refers to the legal framework that governs activities conducted in the digital realm, including the internet, computers, networks, and electronic devices. The constitution, on the other hand, serves as the fundamental law of a country, outlining the rights, responsibilities, and powers of the government and its citizens.

Many countries have constitutional provisions that protect fundamental rights and freedoms, such as the right to privacy, freedom of speech, and freedom of expression. These constitutional guarantees apply to the digital realm as well, and cyber laws are designed to ensure that these rights are respected and protected in the context of cyberspace. The constitution grants legislative bodies the authority to enact laws, including cyber laws, to regulate activities in the digital sphere. These laws are created within the framework established by the constitution, ensuring that they do not infringe upon constitutional principles or violate fundamental rights. Cyber laws aim to strike a balance between protecting individual rights and maintaining the security and integrity of digital systems. Constitutional principles guide the formulation of cyber laws, ensuring that they do not disproportionately restrict rights or violate the principles of due process and fairness.

The constitution often provides for judicial review, allowing courts to examine the constitutionality of laws, including cyber laws. If a cyber law is challenged on constitutional grounds, the courts can assess whether it conforms to constitutional provisions and principles. This process ensures that cyber laws adhere to the constitutional framework and do not unduly infringe upon individual rights. Constitutions may include specific provisions or safeguards related to cybersecurity, data protection, and privacy. For example, some countries have constitutional provisions that require the government to protect citizens' personal information and ensure the confidentiality and integrity of digital communications.

Over time, as technology and the digital landscape evolve, constitutions may be amended to address emerging challenges and provide a legal foundation for governing cyberspace. These amendments can provide the basis for developing and updating cyber laws to reflect the changing needs and realities of the digital world. The relationship between

cyber law and the constitution can vary between countries, as it depends on the specific constitutional provisions and legal systems in place. The constitution serves as a guiding framework for cyber law, ensuring that digital activities are governed within the parameters of fundamental rights and constitutional principles.

CONSTITUTIONAL REMEDIES IN BANKING FRAUDS:

Constitutional remedies in banking frauds primarily revolve around protecting the fundamental rights of individuals affected by such frauds. While the specific remedies may vary depending on the country and its constitutional framework, here are some general constitutional remedies that can be sought in the context of banking frauds:

Right to Equality: The right to equality, guaranteed by most constitutions, ensures that all individuals are treated equally under the law. If a banking fraud has occurred due to discriminatory practices or unequal treatment, affected individuals can seek remedies to address the violation of their right to equality.

Right to Property: The right to property, protected by many constitutions, safeguards individuals' ownership and possession of their assets. In banking frauds where property or funds are wrongfully acquired or seized, individuals can seek remedies to recover their assets or seek compensation for the loss incurred.

Right to Privacy: The right to privacy, recognized by many constitutions, protects individuals' personal information and prevents unauthorized intrusion into their private affairs. If a banking fraud involves a breach of privacy, such as unauthorized access to personal or financial data, affected individuals can seek remedies to protect their privacy rights and seek appropriate legal action against the perpetrators.

Right to Fair Trial: The right to a fair trial, enshrined in most constitutions, guarantees individuals the right to a fair and impartial legal process. If a banking fraud leads to legal proceedings, individuals have the right to a fair trial, including access to legal representation, the opportunity to present evidence, and a fair and unbiased adjudication of their case.

Right to Constitutional Remedies: Many constitutions provide for specific remedies to enforce fundamental rights. For example, the writs of habeas corpus, mandamus, certiorari, prohibition, and quo warranto may be available to challenge unlawful detentions, seek accountability, or challenge actions that violate constitutional rights.

These remedies can be sought in cases where banking frauds involve violations of fundamental rights protected by the constitution.

Constitutional remedies often involve approaching the appropriate courts or tribunals to assert and protect constitutional rights in the context of banking frauds.

ECONOMICS CRIME IN INDIA:

At first talking about the general definition of E-Commerce, the electronic commerce, commonly known as e-commerce, is the buying and selling of products through electronic media such as the Internet and other electronic services. With the spread of the Internet, this type of transaction has grown rapidly. The need for electronic commerce stems from the need for more efficient use of computers in banks and businesses. As competition intensifies, companies are required to improve customer satisfaction and share information.

Electronic commerce (e-commerce) refers to businesses and individuals who buy and sell goods and services over the Internet. E-commerce takes place in different market segments and can be done through computers, tablets, smartphones and other smart devices. Almost every conceivable product or service is available through e-commerce, including books, music, airline tickets, and financial services such as stock investments and online banking. Therefore, it is considered a highly disruptive technology.

HISTORY OF E-COMMERCE:

Most of us have purchased something online at some point, which means we have participated in e-commerce. It goes wrong without saying that e-commerce is everywhere. However, few people may know that the history of e-commerce dates back to before the dawn of the Internet.

E-commerce actually goes back to the 1960s when companies used an electronic system called the Electronic Data Interchange to facilitate the transfer of documents. It wasn't until 1994 that the very first transaction. took place. This involved the sale of a CD between friends through an online retail website called NetMarket.

The industry has gone through so many changes since then, resulting in a great deal of evolution. Traditional brick-and-mortar retailers were forced to embrace new technology in order to stay afloat as companies like Alibaba, Amazon, eBay, and Etsy became

household names. These companies created a virtual marketplace for goods and services that consumers can easily access.

New technologies continue to make it easier for people to shop online. People can use their smartphones and other devices to connect with businesses, download apps, and make purchases. The introduction of free shipping, which reduces costs for consumers, has also helped increase the popularity of the e-commerce industry.

Further the E-commerce, which refers to the buying and selling of goods and services over the internet, has witnessed significant growth and transformation in India over the years. Here's an overview of the history of e-commerce in India:

I. Late 1990s: Emergence of Online Marketplaces The concept of e-commerce started to gain momentum in the late 1990s with the emergence of online marketplaces. Companies like IndiaMART and Tradeindia.com were among the pioneers, providing platforms for businesses to showcase their products and connect with buyers.

II. Early 2000s: The Dotcom Boom The early 2000s saw the rise of various e-commerce players, often referred to as the "dotcom boom." Companies like Rediff.com, Indiaplaza, and Fabmart (later rebranded as Indiaplaza) began offering online shopping platforms for consumers.

III. Mid-2000s: Entry of E-commerce Giants In the mid-2000s, major players entered the Indian e-commerce market. Flipkart, founded in 2007, started as an online bookstore and expanded into a wide range of product categories. Other notable players that emerged during this time were Snapdeal (2010) and Paytm (2010).

IV. 2010-2014: Mobile Commerce and Group Buying The advent of smartphones and increased internet penetration led to the rise of mobile commerce. Companies like Myntra (founded in 2007) and Jabong (2012) gained popularity for their mobile shopping apps. Additionally, group buying websites like Groupon India (2011) offered discounted deals to consumers.

V. 2014-2016: Funding and Consolidation During this period, several e-commerce players attracted significant investments and witnessed rapid growth. Flipkart, Snapdeal, and Paytm raised substantial funding from both domestic and

international investors. However, there was also a wave of consolidation, with some players merging or shutting down due to intense competition.

VII. 2016-Present: Dominance of Flipkart and Amazon The e-commerce market in India witnessed intense competition between Flipkart and Amazon, both vying for market dominance. In 2018, Walmart acquired a majority stake in Flipkart, giving the company a significant boost. Amazon, on the other hand, invested heavily in expanding its operations in India.

Government Initiatives and Digital Payments The Indian government's "Digital India" campaign, launched in 2015, aimed to promote digital transactions and online services. Demonetization in 2016 further accelerated the adoption of digital payments and e-commerce platforms. Companies like Paytm, PhonePe, and Google Pay emerged as popular digital payment solutions.

Diversification and Expansion In recent years, e-commerce in India has witnessed diversification beyond traditional retail. Online food delivery platforms like Swiggy and Zomato gained prominence, as did online grocery delivery services such as BigBasket and Grofers. Additionally, sectors like fashion, electronics, and travel continued to see significant growth.

The history of e-commerce in India is marked by rapid growth, intense competition, and technological advancements. It has transformed the way people shop and conduct business, with e-commerce platforms becoming an integral part of the Indian economy.

SPECIAL CONSIDERATIONS:

E-commerce has changed the way people buy and consume products and services. More and more people are turning to computers and smart devices to order products that can be easily delivered to their homes. As a result, the retail landscape has changed. Amazon and Alibaba have gained considerable popularity, forcing traditional retailers to make changes to the way they do business.

But that's not all. Not to be outdone, individual sellers have increasingly engaged in e-commerce transactions via their own personal websites. And digital marketplaces such as eBay or Etsy serve as exchanges where multitudes of buyers and sellers come together to conduct business.

BASIC UNDERSTANDING OF ELECTRONIC COMMERCE:

As mentioned above, e-commerce is the process of buying and selling tangible products and services online. Completing a transaction requires the exchange of data or currency with multiple parties. It is part of the larger electronic commerce (e-business) industry that encompasses all processes involved in running a business online. E-commerce enables businesses (particularly short-reach businesses such as small and medium-sized enterprises) to access a wider market and reach a larger market by providing a cheap and efficient distribution channel for their products and services. It helped establish a presence. Target (TGT) has complemented its brick-and-mortar presence with his online store, where customers can buy everything from the comfort of their homes to clothing and coffee makers to toothpaste and action figures.[7]

Offering a product or service is not as easy as it sounds. Extensive research is required about the product or service you want to sell, the market, target audience, competitors, expected business costs, etc.[8]

Once that is decided, you need to come up with a name and form a legal entity such as a corporation. Next, set up an e-commerce site with a payment gateway. For example, a small business owner who owns a clothing store may set up a website to promote clothing and other related products online, allowing customers to pay via credit card or payment processing service. Example such as PayPal etc.

ADVANTAGES AND DISADVANTAGES OF ELECTRONIC COMMERCE:

E-commerce offers consumers the following advantages:

- **Convenience**: E-commerce can occur 24 hours a day, seven days a week. Although eCommerce may take a lot of work, it is still possible to generate sales as you sleep or earn revenue while you are away from your store.
- **Increased Selection**: Many stores offer a wider array of products online than they carry in their brick-and-mortar counterparts. And many stores that solely

[7] https://www.acfe.com/fraud-101.aspx
[8] https://www.lawctopus.com/symbiosis-law-school-hyderabad-digital-art-competition//

exist online may offer consumers exclusive inventory that is unavailable elsewhere.

- **Potentially Lower Start-up Cost:** E-commerce companies may require a warehouse or manufacturing site, but they usually don't need a physical storefront. The cost to operate digitally is often less expensive than needing to pay rent, insurance, building maintenance, and property taxes.
- **International Sales:** As long as an e-commerce store can ship to the customer, an e-commerce company can sell to anyone in the world and isn't limited by physical geography.
- **Easier to Retarget Customers:** As customers browse a digital storefront, it is easier to entice their attention towards placed advertisements, directed marketing campaigns, or pop-ups specifically aimed at a purpose.

DISADVANTAGES:

There are certain drawbacks that come with e-commerce sites, too. The disadvantages include:

- **Limited Customer Service**: If you shop online for a computer, you cannot simply ask an employee to demonstrate a particular model's features in person. And although some websites let you chat online with a staff member, this is not a typical practice.
- **Lack of Instant Gratification**: When you buy an item online, you must wait for it to be shipped to your home or office. However, e tailers like Amazon make the waiting game a little bit less painful by offering same-day delivery as a premium option for select products.
- **Inability to Touch Products**: Online images do not necessarily convey the whole story about an item, and so e-commerce purchases can be unsatisfying when the products received do not match consumer expectations. Case in point: an item of clothing may be made from shoddier fabric than its online image indicates.
- **Reliance on Technology:** If your website crashes, garners an overwhelming amount of traffic, or must be temporarily taken down for any reason, your business is effectively closed until the e-commerce storefront is back.

- **Higher Competition:** Although the low barrier to entry regarding low cost is an advantage, this means other competitors can easily enter the market. E-commerce companies must have mindful marketing strategies and remain diligent on SEO optimization to ensure they maintain a digital presence.

PERFECT EXAMPLE OF E-COMMERCE:

Amazon is a giant in the e-commerce field. In fact, the company is the world's largest online retailer and is still growing. As such, this represents a major disruption in the retail industry, forcing some major retailers to rethink their strategies and shift their focus. The company started its business using an e-commerce based model for online sales and product delivery. Founded in 1994 by Jeff Bezos as an online bookstore, it has since expanded to carry everything from clothing to household items, power tools, food, beverages and electronics.

On the other hand white collar crime in India is not a new phenomenon. Economic criminals have exploited the deficit in various sectors to swindle hundreds of millions of euros. They are constantly researching how to exploit vulnerabilities and holes, while also looking for new areas to subvert systems. White-collar crime has been on the rise in many areas since the early 1990s, turning millions of investors and many organizations (banks, insurance companies, etc.) against it.[9]

Trendingly, the term e-commerce plays a very important role in bank fraud, which is very difficult to track and is often associated with internet usage. But it would be a mistake to think that this is a new phenomenon. Before the Internet was developed and commercially widely used, private electronic networks and other technologies based on closed electronic networks were already in place to provide all kinds of electronic communication between commercial establishments and business entities. It was used and was used to access binding contracts or for commercial purposes to the contract.

E-commerce and trading over the Internet is a reality and will continue for a long time to come. All transactions involving the transmission of electronic signals can be classified as electronic commerce. Businesses both large and small are rapidly moving online due to the Internet's unique ability to reach a company's marketing message worldwide and

[9] https://www.iimb.ac.in/sites/default/files/2018-07/WP_No._505.pdf.

target consumers who are more likely to actually purchase a product. [10] The World Trade organization[11] (WTO) Ministerial Declaration on E- Commerce defines E- Commerce as 'the production, distribution, marketing, sales or delivery of goods and delivery of goods by electronic means'. According to European Commission[12], e-commerce encompasses more than the purchase of goods online. It includes a desperate set of loosely defined behaviours, such as shopping, browsing the internet for goods and services, gathering information about items to purchase and completing transactions. This includes delivery and order status inquiries for these goods and services. This includes conducting consumer satisfaction surveys, collecting information about consumers, and maintaining consumer databases for promotional and other related activities, as well as other sustainable corporate activities. The Gartner Group[13] defines e-commerce as an evolving set of:

A. The homegrown or packaged software application that connects multiple businesses or individual consumers to a business for the purpose of conducting business.

B. The business strategy that optimizes relationships between companies through the use of information technology.

C. The business processes such as procurement and sales, order status and payment confirmation are by definition cross-border.

D. The technologies and tools that enable the implementation and realization of these applications, strategies, and processes.

In other words, electronic commerce is any commercial transaction that takes place over or over an electronic network, whether between individuals or for-profit entities. All that matters is that the advertising is done through electronic media. [14] Transactions can be made via telephone, fax, ATM, electronic payment systems such as prepaid calling cards, electronic data interchange, television and the Internet.

Simply put, it is a great business opportunity for everyone in the world. Initially, the Internet was seen as a kind of medium. Then everyone realized the internet's amazing

[10] Sharma Vakul; E-Commerce: A New business paradigm, in legal dimensions of Cyberspace; Indian Law Institute, New Delhi, 2004.
[11] See, www.wto.org.
[12] See, http://europa.eu.int.
[13] See, www.gartner.com
[14] Davies, LJ; "A model for internet regulation" (1998).

ability to interact, opening up arguably endless new possibilities. Even well-connected users use the Internet as a typical online shopping mall to gather information and purchase goods. The amazing thing is that e-commerce is facilitating global trade. [15] This means that every future-oriented company should have at least a temporary internet connection. Moreover, e-commerce will fundamentally change the concept of the market. In India too, infrastructure bottlenecks are gradually becoming a thing of the past, thanks to rapid advances in satellite technology and huge investments by global consortia in laying high-quality fiber optic cables that can improve connectivity many times over. is becoming This sets the conditions for us to enter the world of e-commerce. However, in reality, the legal framework for e-commerce is still in its infancy. The so-called cyber law has just come into force and is still in its early stages. It should also be mentioned that laws should not be rigid, as such laws can destroy entrepreneurship on the Internet. Surprisingly, India has taken deliberate steps to bring legal support to e-commerce. With the passage of the Information Technology Act, India joins a select group of countries to enact cyberspace-related laws.

Banking and e-commerce are two important aspects of modern financial transactions. Let's examine each one in more detail.

INDIAN POSITION AND PERSPECTIVES TO HANDLE BANK FRAUD CASES:

In India, bank fraud cases are handled through a combination of legal, regulatory, and investigative measures. The Indian government, regulatory bodies, and law enforcement agencies have implemented various initiatives and mechanisms to address and mitigate bank frauds. Here are some key perspectives and measures taken in India to handle bank fraud cases:

Legislative Framework: India has a comprehensive legislative framework in place to address bank frauds. The Indian Penal Code (IPC), the Prevention of Corruption Act, the Companies Act, and various other laws govern different aspects of banking frauds. These laws provide the legal basis for investigating and prosecuting fraudsters.

Regulatory Bodies: The Reserve Bank of India (RBI) is the central regulatory authority for banking and financial institutions in India. It plays a crucial role in ensuring the

[15] Patrick E Cole et al; "Business – The internet economy".

stability and integrity of the banking system. The RBI issues guidelines, directions, and regulations to prevent and detect frauds, and it collaborates with banks to establish robust risk management and internal control mechanisms.

Fraud Detection and Reporting: Banks in India are required to have systems and procedures in place to detect and report frauds promptly. The RBI mandates the reporting of all significant fraud cases to the Central Fraud Monitoring Cell (CFMC) and other concerned agencies. Banks also have dedicated departments, such as the Centralized Fraud Monitoring Units (CFMUs), to monitor, investigate, and report fraud cases.

Investigative Agencies: Several investigative agencies in India are responsible for handling bank fraud cases. The Central Bureau of Investigation (CBI) and the Serious Fraud Investigation Office (SFIO) are among the key agencies involved in investigating complex and high-value fraud cases. The Economic Offences Wing (EOW) of state police departments also investigates and registers cases related to banking frauds.

Cyber Crime Units: With the rise in digital banking and online transactions, cybercrime has become a significant concern. State police departments have specialized cybercrime units or cells that investigate and handle cyber-enabled banking frauds. These units collaborate with other investigative agencies and financial institutions to trace and apprehend cyber fraudsters.

Recovery and Asset Seizure: Authorities in India strive to recover the proceeds of bank frauds and seize the assets acquired through fraudulent means. The Enforcement Directorate (ED)[16] and other agencies focus on identifying and attaching the assets of fraudsters to prevent their misuse and facilitate recovery for the affected banks or victims.

International Cooperation: Banking frauds often have international dimensions, involving offshore transactions or coordination between individuals in different countries. Indian authorities actively collaborate with international agencies, such as Interpol and other countries' law enforcement agencies, to exchange information, seek assistance in investigations, and extradite offenders involved in cross-border frauds.

Public Awareness and Education: Public awareness and education campaigns play a crucial role in preventing bank frauds. The RBI, banks, and other agencies regularly

[16] https://economictimes.indiatimes.com/tech/technology/ed-investigating-several-cases-related-to-crypto/digital-currency-frauds-mos-finance/articleshow/99217545.cms

conduct awareness programs, disseminate guidelines, and promote safe banking practices to educate the public about common fraud schemes, phishing attacks, and preventive measures.

Combating bank frauds is an ongoing challenge, and authorities in India continue to strengthen their mechanisms and initiatives to address evolving fraud risks. The perspectives and measures outlined above reflect the general approach taken in India to handle bank fraud cases, but specific cases may involve variations in investigation, prosecution, and recovery processes based on the nature and complexity of the frauds.

E-COMMERCE: A CHANCE TO EXECUTE FRAUD

While e-commerce offers numerous benefits and convenience, it is true that it also presents opportunities for fraudulent activities. The nature of online transactions and the potential anonymity associated with them can attract individuals seeking to exploit vulnerabilities in the system. Here are some reasons why e-commerce can be a platform for executing fraud:

Firstly Limited Face-to-Face Interaction wherein the traditional brick-and-mortar transactions, face-to-face interactions provide a certain level of verification and trust. In e-commerce, however, there is often a lack of direct personal contact, making it easier for fraudsters to conceal their true identity and deceive unsuspecting individuals. Secondly The Global Reach and Cross-Border Transactions in which the E-commerce allows businesses and customers to engage in transactions across borders and with parties from different jurisdictions. This can make it more challenging to enforce regulations and investigate fraudulent activities, as legal frameworks and enforcement mechanisms may vary across countries. Thirdly The Payment Card Vulnerabilities which states that E-commerce relies heavily on payment cards for transactions. Card details can be stolen through various means, such as data breaches, phishing attacks, or malware. Fraudsters can then use this information to make unauthorized purchases, leading to financial losses for individuals and businesses. Fourthly the fake online stores and sellers in which fraudsters can create counterfeit websites or establish fake online seller accounts to lure customers into making purchases. They may offer enticing deals or advertise popular products at significantly lower prices, only to disappear after receiving payment or delivering substandard or counterfeit goods. Last but not the lease the Identity Theft and Account Takeover in which E-commerce platforms often store customers' personal

information, such as names, addresses, and payment details. If hackers gain unauthorized access to this data through data breaches or phishing attacks, they can use it to commit identity theft or take over user accounts, making fraudulent transactions on behalf of the account holders. Lastly difficulty in verifying product authenticity wherein the e-commerce can be challenging to verify the authenticity and quality of products before making a purchase. This creates an opportunity for fraudsters to sell counterfeit or substandard goods, misrepresent product information, or engage in deceptive advertising practices.

It is relevant and important to understand that to mitigate the risk of fraud in e-commerce, various preventive measures can be employed. These include implementing secure payment gateways, using encryption technologies, enhancing user authentication methods, conducting thorough background checks on sellers or marketplaces, employing fraud detection systems, and educating users about safe online practices. It is important for individuals to be vigilant, exercise caution when making online purchases, and report any suspicious activities or fraud incidents to the relevant authorities. E-commerce platforms also play a crucial role in implementing robust security measures, verifying sellers, and promptly addressing customer concerns or disputes to foster trust and confidence in the online marketplace.[17]

BANKING: -

Banking is understood to mean the activities carried out by financial institutions such as banks to facilitate various financial services. These services include depositing and withdrawing money, lending and borrowing, investment management, and other financial transactions. Banking has evolved over time and the advent of technology has increased the popularity of online banking.

Online banking, also known as internet banking or e-banking, allows customers to make financial transactions and access banking services through secure websites and mobile he applications. It provides convenience and allows customers to complete tasks such as checking balances, transferring money, paying bills, applying for loans and investing from the comfort of their home or on the go.

[17] https://www.ca-cib.com/sites/default/files/2021-10/Basel-III-Disclosures_0921.pdf

Security is a major concern in the banking industry and institutions take various measures to ensure the safety of online transactions. These measures include encryption, two-factor authentication, biometrics, and monitoring systems to detect and prevent fraud.

There are different types of e-commerce models, including:

Business to Consumer (B2C):[18]

In this model, companies sell their products or services directly to consumers through an online platform or website. Examples include online retailers such as Amazon and Walmart.

Business to Business (B2B):

In this model, companies conduct electronic transactions with other companies. This includes online supply chain management, wholesale trading and online collaboration platforms.

Consumer to Consumer (C2C):

C2C e-commerce allows an individual to sell products and services directly to others through his platform online. Common examples include platforms such as eBay and Craigslist.

Consumer to Business (C2B):

In this model, consumers sell their products and services to businesses. Examples include freelancers who offer their services on various platforms. Ecommerce platforms typically offer features such as product catalogs, shopping carts, secure payment gateways, and order management systems that facilitate transactions. E-commerce payment methods include credit/debit cards, digital wallets, and other online payment systems.

Both banking and e-commerce have experienced significant growth and transformation due to technological advances. They play an important role in the digital economy, providing convenience and accessibility for both individuals and businesses.

RISK AT BANKING: -

[18]https://www.investopedia.com/terms/r/retailbanking.asp#:~:text=Retail%20banking%2C%20also%20known%20as,money%20in%20a%20secure%20manner.

Banking, like any other industry, involves a certain amount of risk. Common risks associated with banking transactions include:

Credit risk:

This is the risk that borrowers will not be able to meet their loans or loan obligations, resulting in financial loss for the bank. Banks evaluate a borrower's creditworthiness before making a loan. However, economic conditions and unforeseen circumstances may affect a borrower's ability to repay.

Market risk:

Market risk is the potential loss that may result from changes in market conditions such as interest rates, exchange rates, stock prices and commodity prices. Banks with significant trading activities and investments in financial instruments are exposed to market risk.

Liquidity risk:

Liquidity risk is the risk of being unable to meet short-term financial obligations. This happens when banks are unable to convert assets into cash quickly or when sufficient funds are not available to cover their liabilities. Sudden deposit withdrawals or an inability to sell assets at fair value can lead to a bank liquidity shortage.

Operational risk:

Operational risk is the potential for loss caused by deficiencies or failures in internal processes, people or systems, or external events. These include risks related to technology failure, fraud, human error, legal and regulatory compliance, and business disruption.

Cyber security risk:

Cyber security risks have become a major concern for banks as their reliance on digital systems and online transactions increases. Cyber threats such as data breaches, hacking attempts, and malware attacks can lead to financial loss, reputational damage, and exposure of customer information.

Compliance and regulatory risk:

Banks follow different regulatory frameworks and therefore have to comply with different laws and regulations. Failure to comply may result in fines, legal liability, and reputational damage. Regulatory changes and unanticipated interpretations can also pose compliance and regulatory risks.

Reputation risk:

Reputational risk is the risk that a bank's reputation may be harmed as a result of actions or events. Negative public perception, customer dissatisfaction or publicized misconduct can undermine trust and affect a bank's operations and customer relationships. Banks use risk management practices and frameworks to identify, assess, monitor and mitigate these risks. Additionally, to ensure the stability and integrity of the banking system, regulators have set guidelines for risk management.

MODES OF PAYMENT IN BANKING SYSTEM AND ITS RISKS:

Just as in the real world different commercial activities use different payment methods for goods and services, so too are different payment mechanisms available and used in e-commerce, the online version of commerce can be called an online payment system. An online payment mechanism means “payment” and “receipt” of virtual currency. Such online payment systems require not only parties conducting business on the Internet, but also a "payment gateway" to facilitate such transactions. First and foremost, you should use credit cards and other online payment methods with advanced technical tools. Some of the popular modes of payment in cyberspace are:

Credit Cards:

The majority of online transactions are currently affected by credit or debit card payments.[19] Consumers enter their credit card information into online forms and submit them to websites that offer goods and services over the Internet. Many websites use Secure Socket Layer (SSL). SSL is built into most new browsers and automatically encrypts information in transit for added security. However, due to widespread consumer mistrust of security, most websites also allow consumers to provide credit card information over the phone. A major advantage for online merchants is that credit/debit cards are a payment method that is familiar to most consumers and does not require

[19] Hammond Suddards, Credit Cards 68 (1999).

consumers to install any special plug-ins or devices, making the process even easier for online transactions and to shop while surfing the net. [20]

Master Card recently launched Site Data Protection Services (SDP), a comprehensive suite of global e-business security services that proactively protect online merchants from hacker attacks. It's a satellite network. Credit card companies have also introduced Magneprint, a technology that proactively helps prevent card skimming by using the "unique noise" characteristic of each card's unique magnetic stripe to distinguish between original and clone cards. Just as a fingerprint can uniquely identify an individual, Magneprint can uniquely identify a magnetic stripe card.

Secure Electronic Transaction (SET):

Secure Electronic Transaction (SET) is a protocol that was developed in the late 1990s as a joint effort between Visa, Mastercard, and other organizations. Its purpose was to provide a secure method for conducting electronic transactions over open networks, such as the internet. Although SET is not widely used today, it laid the foundation for many of the security features and practices seen in modern e-commerce.

The key objectives of SET are:

Confidentiality:

SET aimed to ensure that sensitive information, such as credit card numbers and personal details, remained confidential during transmission over the network. This was achieved through the use of encryption techniques.

Integrity:

SET aimed to protect against data tampering or modification during the transaction. It employed digital signatures to verify the authenticity and integrity of messages exchanged between the parties involved.

Authentication:

SET focused on verifying the identities of participants in a transaction. It utilized digital certificates to authenticate the identity of the buyer, seller, and the payment gateway involved in the transaction.

[20] Prabhakar Kiron; Payment Mechanism in cyberspace; Legal Dimensions of Cyber Space; Indian Law Institute.

Non-Repudiation:

SET aimed to prevent either the buyer or the seller from denying their participation in a transaction. Digital signatures played a crucial role in providing non-repudiation by providing evidence of the transaction and the parties involved.

While SET was designed with strong security principles, it faced challenges in terms of complexity, implementation costs, and the need for widespread adoption among merchants and consumers. As a result, it did not gain widespread popularity, and alternative approaches, such as Secure Sockets Layer (SSL) and Transport Layer Security (TLS), became more prevalent for securing online transactions.

Today, SSL/TLS encryption, secure payment gateways, and other security measures are commonly used in e-commerce to ensure the secure transmission of sensitive information and protect against unauthorized access or fraud. These technologies, along with other security practices, have evolved to meet the changing landscape of e-commerce and address emerging threats.

Secure electronic transactions are used to overcome the security issues associated with using credit cards. This method enables cardholder identity verification and reduces the risk of credit card fraud through disclosure of card details through open systems. It also provides authentication that cardholders are legitimate users of branded payment card accounts. It also provides certification that online merchants can accept branded payment card transactions through their relationship with the acquiring financial institution. [21] This method uses two separate keys, a public key and a private key, to encrypt and decrypt messages. The public key used uses a complex formula to encrypt the message. The message is then sent over the Internet in this encrypted form. Public keys are published in a directory so they can be accessed by third parties. However, even if an unauthorized third party had the encrypted message and public key, they would not be able to read the message. It can only be read using a private key known only to the provided recipient. The identity of the sender of a message is determined using digital means.

In addition to all perspectives, there are many other issues such as:

[21] http://www.davidreilly.com.

- E-Government has limitations related to people's technological resources, preferences and the wide range of problems they pose to government. For example, few people have Internet access in urban areas, but almost no one has Internet access in rural areas. For the majority of citizens who are not online, they can contact their government by phone, personal visit, or by writing a letter.
- In addition, many people choose not to use the Internet or email to contact their government. Interestingly, most people still prefer to use their phones to contact the government, even those with internet access. And when it comes to urgent or complex issues, people tend to prefer "real-time" interactions with government officials via phone calls or in-person visits. Therefore, although e-government is one of several ways to contact government, it is not the only or the most important of them. When contacting the government, people use the following methods. There are various methods such as telephone calls, personal visits, e-mails and letters.
- One of the main reasons for the failure of many e-government projects in various countries is poor communication and inadequate exchange of information between stakeholders. Various studies show that multi-stakeholder partnerships improve the success rate of e-governance and ICT development efforts. The success of partnerships often depends on the level of personal interaction between practitioners rather than the organizational structure.
- The development and implementation of e-government should consider impacts including but not limited to environmental, social, cultural, educational and consumer issues. Governments need to be mindful of the "digital divide" – the impact of non-use, inaccessibility, or inaccessibility of e-government and other digital resources on social structures and potential income and economic implications.
- There are also administrative issues related to service integration, local e-government, Internet governance, and financial considerations. Cost of Implementation/Impact on Existing Budgets, Impact on Public Procurement and Funding. Legal implications include freedom of information and privacy issues.

- There are 80% of the rural population's needs are related to health, education and agriculture and these must be met primarily through other means. E-government is of little help here.
- That with so much confidential and sensitive information stored on the Internet, comprehensive planning against security threats and cybercrime is also urgently needed. Even the most progressive and forward-thinking organizations like NASA have fallen victim to hackers and cybercriminals.

FRAUDS:

"Fraud means:

(1) Deliberately misrepresenting the truth or concealing important facts in order to induce others to act unfavorably to you; Fraud is usually illegal, but in some cases (especially deliberate) it can be a criminal offence.

(2) Recklessly making false representations without believing the truth in order to induce others.

(3) Tort consisting of willful misrepresentation, omission of material facts, or reckless misrepresentation intended to induce harmful behavior in others;

(4) Malicious Transactions. especially. Colloquially, the terms "fraud" and "fraud" are used interchangeably to refer to any kind of financial misconduct. Legally, fraud usually refers to broader and more serious crimes, and fraud is also a type of fraud.

Fraud is generally fraudulent activity that involves money or some type of business transaction. Fraud comes in many forms. You may have been told you could win a prize if you gave your credit card information, or were asked to donate to a non-existent charity. Scams reach us in many ways, including phone calls, emails, and even in-person visits.

Fraud means deception. It is an offence under the ambit of breach of trust. Fraud is a serious criminal offense and a violation of civil law. The motives for fraud vary. This includes financial gain, discrediting adversaries. Not only is it financially profitable, but it also leads to prestige. Fraud as Defined In Section 17 of Indian Contract Act, 1872

"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 contract:

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

Actions considered fraud must be limited to actions by contracting parties with the intent to defraud other parties or their agents or induce them to enter into transactions or contact.

Any fraudulent act affecting the contract must relate to the conduct of the parties to the contract that contract. This definition emphasizes the need to prove the intent of the person who did it and committed fraud.

If the person deliberately commits fraud, he will be punished. An individual here refers to the principal or his/her agent. Anything that involves cheating is wrong Suggestions or omissions of facts, false promises, or deceptive deception.

An electronic payment system refers to an automated process Exchange of monetary value between business parties Communicating transactions and their value through information Communication technology (ICT) networks of Payment cards are one of the most popular electronic payment channels (debit or credit), online web portal, point of sale (POS) terminal, automated teller machine (ATM), mobile Telephone, Automated Clearing House (ACH), Direct Line Debit/Deposit and Real Time Total Settlement System (RTGS). Criminals are on the rise as the use of electronic payments grows found another way to increase their outrage How to take money from innocent victims. She Using methods such as forgery, identity theft, or card counterfeiting trapping, farming, cloning, malware attacks, BIN attacks, Skimming, Phishing, Card Fraud and Theft electronic payment users; These are not simple consumers Subject to Electronic Payment Crime Only, Subject to Others. These include distributors, retailers, banking institutions,

Organizations that use personal data for transactions companies and even governments. No possible targets that can get away with these criminals.

India remains the fastest growing mobile country in Africa and the third largest in the world, with over 60% of the population connected to the internet. India, therefore, has great potential for the introduction of mobile commerce in addition to e-commerce which is gradually gaining momentum. The main difference between electronic and mobile business transactions, prefixed with 'e' and 'm', is that electronic media provides 'anytime, anywhere access' to business processes, whereas mobile media provides 'anytime, anywhere access' to business processes. to provide access anywhere. However, payment success has a significant impact on m-payment when security and usability aspects are carefully considered. Credit and debit card payments require multiple entities to process the transaction from start to finish.

Consumers and their payment cards, Merchants and their point of sale (POS) payment devices, card brands (e.g. Visa, MasterCard etc.), issuing banks and card processors. With billions of transactions processed each year, large amounts of electronic data and digital currency pass through this payment ecosystem.

It is important to understand that with access with sensitive information enabling billions of transactions to be done each year. Infrastructure has become a top target for hackers. The e-commerce industry has never been more critical in the fight against cybercrime. The good guys fight the bad guys and the good guys decide to win. It's no secret that the payment ecosystem is fragile. Like the internet, payment infrastructure is designed for connectivity, not security. With so many serious threats and successful hacking attacks against system vulnerabilities, the industry is now caught up in protecting systems. Despite the importance of ICT in banking, the scale of fraud in India today has reached epidemic proportions.

NATURE OF ELECTRONIC FRAUD IN INDIA:

Computer fraud involves subverting programs or infiltrating systems through remote sensors by computer programmers or professionals. The manipulation of computing and other information and communication technology (ICT) to defraud banks gives a better insight into the potential strains of technological revolution.[22] When the computer was

[22] https://www2.deloitte.com/content/dam/Deloitte/in/Documents/finance/in-finance-annual-fraud-survey-noexp.pdf

invented, the inventor's intention was to speed up data processing comfortably. We do this efficiently by providing timely and accurate information. However, like any other mechanical and/or electrical or electronic device, it has been harnessed for heinous acts as well. What was supposed to support day-to-day data operations turned out to be deadly. Banks indulge in the euphoria of efficiency while at the same time dabbling in fraudulent operations. Computer responsibility to control tampering, fraud and counterfeiting continues to be a nightmare for the banking system. Any act of any kind that clearly involves the manipulation of computers or data and in which the victim involuntarily suffers or may suffer loss, injury or damage, or from which the perpetrator may benefit or receive The act is known as "computer crime". The introduction of ICT in banking is commonly referred to as electronic banking (e-banking), and banking service introduction strategy has become a fundamental importance and concern for all banks, and has indeed led to regional and global competition. It is a prerequisite for strength. This is because it directly affects the business decisions and plans of banks and the products and services they offer. The Internet and e-banking have continuously changed the way banks and their corporate relationships around the world are organized and many innovations in service delivery.

In the 2003 report of the technical committee on e-banking of the Central Bank of India (CBN) defines e-banking as “a means whereby banking business is transacted using automated processes and electronic devices such as personal computers, telephones, internet, card payments and electronic channels. It further states that some banks practise electronic banking for informational purpose, some for simple transactions such as checking account balance as well as transmission of information, while others facilitate funds transfer and other financial transactions. Many systems involve a combination of these capabilities.

TYPES OF ELECTRONIC FRAUDS VIZ A VIZ BANKING SECTOR:

Electronic fraud, also known as cyber fraud or online fraud, refers to fraudulent activity that takes place in the digital realm. These scams use electronic devices, the Internet, or computer networks to defraud individuals, steal confidential information, or illegally gain financial gain. Here are some of the common electronic scams:

Phishing:

Phishing is a deceptive technique in which scammers impersonate legitimate organizations or individuals to trick victims into divulging sensitive information such as login credentials, credit card details, and social security numbers. Phishing attacks often come through fraudulent emails, text messages, and fake his websites.

Identity theft:

Identity theft involves stealing personal information such as names, dates of birth, social security numbers, and financial account information to commit fraud. Cybercriminals can use this information to make fraudulent purchases, open fraudulent accounts, or engage in other criminal activities.

Online fraud:

Online scams come in many forms, including advance payment scams, lottery scams, romance scams, and home office scams. These scams typically trick victims into paying money or providing personal information under false pretenses.

Credit card fraud:

Credit her card fraud occurs when an unauthorized person obtains another person's credit her card information and uses it to make unauthorized purchases or withdrawals. This can be caused by physical card theft, card skimming devices, data breaches, or online transactions without proper security measures in place. Malware and Ransomware Attacks:

Malware is malicious software designed to gain unauthorized access to a computer system or network. Ransomware, a type of malware, encrypts the victim's data and demands a ransom to release it. These attacks can cause financial loss, data theft, or business disruption.

Account takeover:

Account takeover occurs when cybercriminals gain unauthorized access to her online accounts, such as email, social media, and financial accounts. This access can be abused to steal personal information, conduct fraudulent transactions, or carry out other malicious activities.

Investment and Trading Fraud:

Online investment and trading platforms are the target of fraudulent activities such as pyramid schemes, pump-and-dump schemes, and fake investment opportunities. These scams trick individuals into making investments that promise high returns, but ultimately result in financial losses.

Preventing and mitigating electronic fraud includes using strong passwords, enabling two-factor authentication, updating software and antivirus programs regularly, staying alert to suspicious emails and websites, and learning about common fraud techniques. This includes implementing strict security practices, such as education. In addition to this, organizations and law enforcement work together to investigate and prosecute cybercriminals to stop such fraudulent activity.

MODERN AREAS OF FRAUDS:

The 21st century has seen major changes in almost every area of life. Technology has promised humanity unprecedented progress, enabled computerization as a source of wisdom for a new age, and spawned new banking services that are fast and efficient. However, this feature also posed risks to various banking operations that required well-defined and timely precautions. Computer automation, which provides a myriad of services, has certain safety/precautionary measures against its built-in flaws, and the RBI, in describing its activities, has stated that in order to minimize such risks, Indicates precautionary measures to be taken.

The precautions taken to prevent or minimize the occurrence of computer-related fraud have a great impact on the attitudes of people working in the computer field. The various other ways are as follows:

A) Easy to get away and cannot get caught.

B) Stealing a little from big company would not hurt.

C) Everybody else is stealing, why not me.

D) Computer security is not a priority.

E) Computer will take care of everything-no checking is required.

F) Lack of input control - output verification.

G) Lack of evidence.

H) Lack of access control-audit trails.

I) Lack of dual checks in sensitive and high-value transactions.

J) Long serving trusted operators/supervisors/Managers.

K) Missing EDP audit.

CHAPTER 3

LAW RELATED TO BANKING FRAUDS IN INDIA:

In India, banking frauds are primarily governed by several laws and regulations that aim to prevent, detect, and prosecute fraudulent activities in the banking sector. Here are some key laws related to banking frauds in India:

Indian Penal Code (IPC):[23]

The IPC is a comprehensive criminal law that addresses various offenses, including those related to banking frauds. Several sections of the IPC, such as Section 420 (cheating and dishonestly inducing delivery of property), Section 406 (criminal breach of trust), and Section 409 (criminal breach of trust by a public servant or banker), are commonly invoked in cases of banking frauds.

Prevention of Corruption Act, 1988:[24]

This act deals with corruption-related offenses, including bribery and illegal gratification involving public servants. It is applicable to cases where banking frauds involve public servants or officials.

Negotiable Instruments Act, 1881:[25]

This act governs negotiable instruments like cheques, promissory notes, and bills of exchange. Offenses related to dishonoring cheques, commonly known as cheque bounce cases, are covered under this act.

Banking Regulation Act, 1949:[26]

The Banking Regulation Act empowers the Reserve Bank of India (RBI) to regulate and supervise banking activities in India. It provides provisions related to the licensing and functioning of banks, prevention of fraudulent practices, and penalties for non-compliance.

Prevention of Money Laundering Act, 2002 (PMLA):[27]

[23] K.D. Gaur; Indian Penal Code; Edition 2019
[24] Universal Bareact of Prevention of Corruption Act
[25] Universal Publication Bareact of Negotiable Instrument Act.
[26] Eastern Book Company Bareact of Banking Regulation Act.
[27] Universal Publication Bareact of Prevention of Money Laundering Act.

PMLA is aimed at preventing money laundering and the financing of illegal activities. It requires banks and other financial institutions to follow stringent customer due diligence processes, report suspicious transactions, and maintain records of financial transactions.

Information Technology Act, 2000 (IT Act):[28]

The IT Act deals with cybercrimes and provides legal frameworks for addressing offenses related to unauthorized access, hacking, data theft, and other cyber frauds. It plays a crucial role in prosecuting electronic banking frauds and other cyber-related offenses.

Reserve Bank of India (RBI) Guidelines and Circulars:[29]

The RBI issues guidelines and circulars from time to time to regulate banking operations and address emerging risks, including frauds. These guidelines lay down the framework for fraud prevention, detection, and reporting by banks.

Apart from these specific laws, other legislation such as the Companies Act, 2013, Securities and Exchange Board of India (SEBI) regulations, and Anti-Money Laundering (AML) regulations also have implications for banking frauds and financial crimes in India.

It's important to note that this is not an exhaustive list, and the legal landscape for banking frauds is constantly evolving with new laws, regulations, and judicial interpretations. If you encounter a banking fraud or suspect fraudulent activities, it is advisable to consult legal professionals and report the incident to the appropriate authorities or law enforcement agencies for further action.

DIRECTIVES BY THE RESERVE BANK OF INDIA REGARDING REPORTING OF BANKING FRAUDS:

There is a regulatory requirement to report every fraud within 21 days of its detection to the RBI. As per the RBI instructions, the information must be complied properly and disseminated to the Bank's head office, so that the same may be circulated to all its branch offices. The circular further reported that Zonal Heads shall continue to declare any account/incident as fraud whenever an element of fraud is discernible and report it to Head Office, Vigilance Department within 7 (seven) days from the date of detection of

[28] Universal Publication Bareact of Information Technology Act,2000.
[29] https://www.nachrcoi.co.in/our-services/banking-fraud-legal-guidance/

fraud in respect of any branch/office under their control or other branches/offices such a s MCU/FCC/Processing Centres within their operational area. Subsequently, Vigilance Department shall place a brief account of frauds by way of a 'Note to ED/CMD' for their information and direction and thereafter it would be reported to RBI and Board of Directors of the Bank.[30]

Moreover, the ABC Bank Policy on fraud, 2010[31] duly circulated by ABC Bank, emphasizes that the zonal heads have to ensure that the complaints are lodged in all cases of frauds promptly, without undue delay a s per the guidelines issued by the Vigilance departments from time to time a s per the directions of the RBI.

The ABC Bank's policy further depicts that in some of the fraud cases it ha s been observed that Complaints were not properly drafted which defeated the whole purpose of the exercise. In order to bring uniformity in this matter. Branches must send draft copy of the complaints in all cases of frauds to concerned Zonal Office along with relevant papers for vetting of the complaints. Zonal office ha s to vet all complaints above Rs. 10,000/- but below Rs. 100.00 lac without any exception before it grants permission to the branch for filling of Complaint with Police Authorities. Head Office, Vigilance Department will continue with the practice of vetting all complaints over Rs. 100.00 lac.

It is very important to appreciate the reason behind the filing of cases with CBI/Police Authorities immediately as under:

- It leads to arrest of the culprits in most of the cases;
- It helps bank in recovery of the defrauded amount.
- In this situation, fraudsters are unable to repeat similar frauds at other branches/banks.
- It sends a strong message to potential fraudsters (both internal and external) and this act as a deterrent.[32]

RBI states that NPAs from retail banking are just 2 percent, whereas NPAs from corporate banking are 36 percent. Given the size of transactions in corporate banking, it

[30] Derry v. Peek, (1889) 14 AC 337 : 5 TLR625.

[31] https://economictimes.indiatimes.com/wealth/save/10-types-of-banking-frauds-in-india-customers-should-know-about/articleshow/90438911.cms

[32] The RBI Master Circular on 'Frauds-Classification and Reporting', dated July 02, 2012

is important that banks implement a robust monitoring mechanism post sanction and disbursement of facilities, and be vigilant to early signs of stress in the borrower accounts.[33]

DETAILED STUDY AND COVERING OF LAWS RELATED TO BANKING FRAUDS IN INDIA:

INDIAN PENAL CODE:

The Indian Penal Code (IPC) contains several provisions that are relevant to banking frauds in India. Here are some key sections of the IPC that can be invoked in cases of banking frauds:

Section 420:[34] Section 420 of the IPC deals with the offense of cheating and dishonestly inducing delivery of property. It is commonly applied in cases of banking frauds where individuals deceive others by making false promises, misrepresentations, or by adopting fraudulent means to obtain property or funds. This section can be used to prosecute individuals involved in various types of banking frauds, such as loan frauds, investment scams, or fraudulent transactions.

Section 406:[35] Section 406 of the IPC pertains to the offense of criminal breach of trust. It applies when a person entrusted with property or funds, such as a bank employee or a financial institution, dishonestly misappropriates or converts that property for their own benefit or for the benefit of others. This section can be used to address cases of embezzlement, diversion of funds, or misappropriation of customer deposits in the context of banking frauds.

Section 409:[36] Section 409 of the IPC deals with criminal breach of trust by a public servant or a banker. It applies when a public servant or a banker, entrusted with property or funds, intentionally breaches that trust and misappropriates or misuses the property for personal gain or for the benefit of others. This section specifically addresses situations where the breach of trust involves a public servant or a banker.

[33] It is not necessary that NPAs are frauds. However, it is clear that all frauds become NPAs.
[34] Ibid No.9, Pg36
[35] Id
[36] Id

Section 415:[37] Section 415 of the IPC relates to the offense of cheating. It encompasses situations where a person deceives another by intentionally delivering false information, misleading statements, or by any other fraudulent means, with the intent to induce the victim to deliver property or to commit some act that results in financial loss. This section can be invoked in cases where individuals are deceived through fraudulent banking schemes or false representations.

These sections of the IPC, among others, provide a legal framework to address various forms of banking frauds in India. Law enforcement agencies and the judiciary rely on these provisions to investigate, prosecute, and punish individuals involved in fraudulent activities within the banking sector.

It's important to consult legal professionals or refer to the official IPC text for precise and comprehensive information regarding the specific elements and implications of each section mentioned.

PREVENTION OF CORRUPTION ACT 1988:

The Prevention of Corruption Act, 1988 (PCA) in India primarily focuses on combating corruption-related offenses, including those that may be connected to banking frauds. Although the PCA primarily addresses corruption within the public sector, certain provisions can be relevant to banking frauds involving public servants. Here's how the PCA relates to banking frauds in India:

Bribery Offenses: The PCA criminalizes the act of giving or receiving bribes, both by public servants and private individuals. In the context of banking frauds, if a public servant or a private individual involved in the banking sector is found to have accepted or given bribes to facilitate fraudulent activities, it can be prosecuted under the bribery provisions of the PCA.

Illegal Gratification: The PCA prohibits the acceptance of illegal gratification by public servants. If a public servant involved in the banking sector accepts illegal gratification as a reward for carrying out or omitting to carry out any official duties, it can be considered an offense under the PCA.

Abuse of Official Position: The PCA addresses cases where public servants abuse their official position to obtain pecuniary advantages for themselves or others. If a public

[37] Ibid, Page 39

servant in the banking sector misuses their position, authority, or resources for personal gain or to facilitate banking frauds, it may be treated as an offense under the PCA.

Criminal Misconduct: The PCA covers instances of criminal misconduct by public servants, which include misuse of power, illegal enrichment, obtaining valuable things or pecuniary advantages, or misappropriation of public funds. If a public servant involved in banking engages in criminal misconduct that leads to fraudulent activities, it can be considered an offense under the PCA.

It's important to note that the PCA primarily focuses on corruption offenses, and its application to banking frauds depends on the involvement of public servants. For banking frauds primarily involving private individuals or institutions, other relevant laws like the Indian Penal Code (IPC) and the Prevention of Money Laundering Act (PMLA) may be more applicable.

For comprehensive and up-to-date information regarding the specific provisions and implications of the PCA, it is advisable to consult legal professionals or refer to the official text of the act.

NEGOTIABLE INSTRUMENTS ACT, 1881:

The Negotiable Instruments Act, 1881 is the primary legislation in India that governs negotiable instruments, including cheques, promissory notes, and bills of exchange. While the Act does not specifically address banking frauds, it provides certain provisions that are relevant to dealing with fraudulent activities involving negotiable instruments. These provisions help establish liability and provide remedies for victims of fraud. Here are some key points:

Section 138: This section deals with the dishonor of cheques due to insufficient funds in the account or other reasons. If a cheque is dishonored and the payee gives notice to the drawer within 30 days of receiving the dishonored cheque, the drawer can be held criminally liable. The drawer can be punished with imprisonment for a term that may extend to two years, or with a fine, or both.

Section 139: This section creates a legal presumption that the holder of a cheque received it for the discharge of any debt or liability. It means that if a cheque is issued by a person and it is dishonored, it is presumed that the person is liable unless proved otherwise.

Section 140: This section allows the court to presume that the holder of a cheque received it in good faith for consideration, even if the consideration is not specified on the cheque.

Section 141: This section holds the directors, managers, or other officers of a company responsible for any offense committed by the company under Section 138, unless they can prove that the offense was committed without their knowledge or that they exercised due diligence to prevent the commission of such an offense.

Section 143: This section provides for jurisdiction regarding offenses under Section 138. The offense can be tried by a court within whose local jurisdiction the cheque was dishonored by the bank.

It's important to note that while the Negotiable Instruments Act addresses the dishonor of cheques, banking frauds can involve various other activities beyond the scope of this Act. Additional legislation, such as the Indian Penal Code, the Companies Act, and the Prevention of Money Laundering Act, among others, may apply to banking frauds in India, depending on the nature of the offense.

It is advisable to consult with legal professionals or refer to the latest legislation and amendments to obtain accurate and up-to-date information regarding banking frauds and related laws in India.

BANKING REGULATION ACT, 1949:

The Banking Regulation Act, 1949 is a significant legislation in India that regulates and governs the functioning of banks and financial institutions. While the Act does not specifically address banking frauds, it provides certain provisions that are relevant to dealing with fraudulent activities in the banking sector. These provisions help establish regulatory frameworks, reporting requirements, and penalties for fraudulent practices. Here are some key points:

Section 5(b): This section defines banking business and specifies that accepting deposits of money from the public is a primary activity of banking. It sets the foundation for regulating banks and protecting the interests of depositors.

Section 10: This section outlines the licensing requirements for banks. It empowers the Reserve Bank of India (RBI) to grant, refuse, or cancel banking licenses based on various

criteria, including the bank's financial soundness, management, and integrity. The RBI plays a crucial role in preventing fraudulent entities from operating as banks.

Section 35A: This section empowers the RBI to inspect and investigate the affairs of any banking company. It enables the RBI to examine banks' books, records, and accounts to detect any irregularities or fraudulent activities. The RBI has the authority to take appropriate actions based on its findings.

Section 46: This section establishes provisions for the punishment of certain offenses committed by banks and their officers. It specifies that individuals found guilty of offenses, such as misappropriation, forgery, fraud, or willful omission to disclose information, can be punished with imprisonment or fines.

Section 46A: This section allows the RBI to impose penalties on banks for contraventions of the Act, rules, regulations, or directions issued by the RBI. The penalties can be monetary fines or other punitive measures, which act as deterrents against fraudulent practices.

It's important to note that while the Banking Regulation Act provides a regulatory framework for banks, specific laws, rules, and regulations related to fraud prevention, detection, and investigation may exist outside the Act. Other laws, such as the Indian Penal Code, the Prevention of Money Laundering Act, and the Companies Act, may also apply to banking frauds in India.

To understand the comprehensive legal landscape regarding banking frauds, it is advisable to consult with legal professionals, refer to the latest legislation and amendments, and stay updated on the guidelines and circulars issued by the RBI and other regulatory authorities.

PREVENTION OF MONEY LAUNDERING ACT 2002:

"India's Prevention of Money Laundering Act 2002 (PMLA) plays a key role in combating money laundering and related crimes, including those related to bank fraud. How PMLA Views Bank Fraud in India:

Money laundering crime: The PMLA defines money laundering as the process of converting illegally obtained criminal proceeds into legitimate assets. When bank fraud involves criminal proceeds, such as ill-gotten funds, and then attempts to conceal or disguise those funds, these are money laundering crimes within the meaning of the

PMLA.

Reporting and recordkeeping requirements: PMLA requires banks and other financial institutions to implement rigorous customer due diligence procedures, maintain records of financial transactions, and report suspicious transactions to India's Financial Intelligence Unit (FIU). These requirements help detect and prevent bank fraud that may be associated with money laundering activities. Seizure and confiscation of income:

The PMLA authorizes authorities to seize and seize assets involved in or derived from money laundering crimes. In cases of bank fraud where funds were obtained illegally, the PMLA permits the seizure of such funds and assets related to the fraud.

Penalties: PMLA provides severe penalties for crimes related to money laundering, including bank fraud. It provides for imprisonment, fines and confiscation of criminal proceeds. The law also establishes special courts to ensure speedy trials and effective prosecution of money laundering cases, including bank fraud. Coordination with International Authorities:

PMLA promotes international cooperation in fighting money laundering and related crimes. This enables information exchange, mutual legal assistance and coordination with foreign jurisdictions in investigations and prosecutions. This helps combat cross-border bank fraud and money laundering networks.

It is important to note that the PMLA applies to a wide range of financial crimes, including bank fraud with money laundering elements within its jurisdiction. Indian banks and financial institutions are required by law to comply with the PMLA's provisions, such as maintaining adequate records to report suspicious transactions and assist in investigations of bank fraud related to money laundering. I'm here. For complete and up-to-date information on the specific requirements and obligations of the law, we encourage you to consult a legal professional or refer to our official PMLA guidelines.

INFORMATION TECHNOLOGY ACT, 2000 (IT ACT):

The Information Technology Act, 2000 (IT Act) is a significant legislation in India that deals with electronic transactions, data protection, and cybersecurity. While the IT Act does not specifically focus on banking laws, it has provisions that are relevant to the banking sector regarding electronic banking, digital signatures, and electronic frauds. Here are some key points:

Electronic Documents and Digital Signatures: The IT Act recognizes electronic records and digital signatures as legally valid and equivalent to their paper-based counterparts. This recognition enables banks to carry out various electronic transactions and communicate with customers using electronic means.

Secure Electronic Records and Secure Digital Signatures: The IT Act provides a framework for ensuring the security and integrity of electronic records and digital signatures. Banks are required to implement appropriate security measures to protect customer data and prevent unauthorized access or tampering.

Electronic Funds Transfer: The IT Act enables electronic funds transfer and facilitates online banking services. It allows banks to offer electronic payment systems, such as internet banking, mobile banking, and electronic funds transfer mechanisms.

Cyber Frauds and Offenses: The IT Act addresses cybercrimes and offenses related to electronic transactions, including banking frauds. It criminalizes activities such as unauthorized access to computer systems, identity theft, phishing, data theft, and other fraudulent practices conducted through electronic means.

Cybersecurity and Data Protection: The IT Act imposes obligations on banks and financial institutions to implement reasonable security practices and procedures to protect customer data and prevent data breaches. It also establishes the office of the Indian Computer Emergency Response Team (CERT-In) to handle cybersecurity incidents and promote best practices.

It's important to note that while the IT Act provides a legal framework for electronic transactions and cybersecurity, there may be additional guidelines, circulars, and regulations issued by regulatory authorities like the Reserve Bank of India (RBI) that specifically address banking-related aspects of information technology and cybersecurity.

To obtain comprehensive and up-to-date information regarding the intersection of the IT Act and banking laws in India, it is advisable to consult legal professionals, refer to the latest legislation and amendments, and stay updated on guidelines and circulars issued by the RBI and other regulatory authorities.

DETERRENT EFFECT OF BANKING LAWS ON SOCIETY:

Banking laws play a crucial role in maintaining the stability and integrity of the financial system and have a deterrent effect on society in several ways:

I. Preventing Unlawful Activities: Banking laws define the legal framework within which financial institutions operate. They establish guidelines and regulations that prohibit illegal activities, including money laundering, terrorist financing, and other financial crimes. The existence of these laws acts as a deterrent to individuals and organizations considering engaging in such activities, as they are aware of the potential legal consequences.

II. Establishing Accountability and Liability: Banking laws establish clear rules and standards of conduct for financial institutions and individuals working within the banking sector. These laws outline the responsibilities and liabilities of banks, their directors, officers, and employees. By holding individuals and institutions accountable for their actions, banking laws deter fraudulent activities, unethical behavior, and the misuse of funds.

III. Enforcement and Penalties: Banking laws are enforced by regulatory bodies and government agencies responsible for overseeing the financial sector. These entities have the authority to investigate, audit, and take legal action against those found in violation of banking laws. The existence of enforcement mechanisms, including penalties, fines, and imprisonment, creates a deterrent effect by discouraging individuals from engaging in illegal activities.

IV. Transparency and Disclosure: Banking laws often require financial institutions to provide accurate and timely information to regulators, shareholders, and the public. This promotes transparency and ensures that financial institutions are accountable for their operations. By increasing transparency, banking laws discourage fraudulent practices and unethical behavior as individuals and institutions know they are subject to scrutiny.

V. Investor and Consumer Protection: Banking laws aim to protect the interests of investors and consumers by setting standards for financial products and services. These laws require full disclosure of terms and conditions, prohibit unfair practices, and establish mechanisms for dispute resolution. The existence of these protective measures instills confidence in the financial system, encouraging participation and deterring fraudulent activities that could harm investors and consumers.

Systemic Stability: Banking laws also focus on maintaining the stability of the financial system as a whole. By implementing regulations that ensure adequate capitalization, risk management, and prudential standards, these laws help prevent systemic risks and protect the economy from financial crises. The knowledge that banks are subject to these regulations and must maintain stability acts as a deterrent against reckless behaviour that could destabilize the financial system.

Briefly stating, the Banking laws have a deterrent effect on society by establishing legal boundaries, enforcing accountability, imposing penalties for violations, promoting transparency, protecting investors and consumers, and ensuring systemic stability. These measures create an environment where individuals and institutions are discouraged from engaging in fraudulent activities and unethical behaviour, thereby contributing to the overall integrity and trust in the banking system.

CASE LAWS:

Here are some notable case laws related to banking frauds in India:

a.) Asif Azim Case[38]: This is the first example of cyber fraud. The most notable development was India's first successful cybercrime conviction in February. On 5 February 1998, 24-year-old Asif Azim was convicted by Delhi Municipal Judge Gulshan Kumar of defrauding Sony India of a 29-inch color TV and wireless headphones worth Rs.500. 27,570. As a first-time offender, he was given a one-year suspended sentence and a personal bail of 20,000 rupees. Mr. Azim, who worked at his I-Energizer, a call center in Noida, stumbled upon the details of his credit card for one of his customers, Mr. Barbara Kampa. Then he decided to shop for free. He created his email address on behalf of Kampa and used it to order on his website of Sony India India using his credit card information for Barbara on May 8 last year. Did. Sony India's credit card company Citibank ruled the transaction legitimate and the product was delivered to Azim's home as early as next week. An email was sent to Campa with a photo of Azim receiving the product.

At the end of June, when Mr. Kampa realized he had been charged for an item he didn't buy and called his bank, the situation turned into panic. After consulting with her, Citibank reported that the transaction was fraudulent and void. In other

[38] Sood, V. (2001)"Cyber Law simplified"

words, Sony had to pay for the transaction. The matter was then reported to her CBI. The CBI team determined that the Internet Protocol her address from which the message originated was in Noida, not the United States. They then identified the source computer he was using. When the CBI confronted him, Azim confessed everything. He said he did it just to get something for free. Azim was convicted under Sections 418, 419 and 420 of the Indian Penal Code. The CBI arrested Arif Azim on online fraud charges and registered the case under IPC Article 420. The conviction boosted public confidence in law enforcement's ability to detect cybercrime and the resilience of India's justice system to meet the new challenges of the cyber age.

b.) Harshad Mehta Scam (1992): Harshad Mehta, a stockbroker, orchestrated a massive securities scam in the early 1990s. The case involved fraudulent practices in the banking sector, such as manipulating stock prices, issuing fake bank receipts, and exploiting loopholes in the banking system. The scam led to significant losses for banks and investors. Harshad Mehta was convicted and sentenced to imprisonment.

c.) Satyam Scandal (2009): The Satyam Computer Services scandal was a corporate fraud case that exposed fraudulent financial reporting by the company's management. The scam involved inflating profits, creating fictitious assets, and manipulating financial statements. Satyam's chairman, Ramalinga Raju, admitted to the fraud, and several executives were charged. The case highlighted the need for improved corporate governance and auditing standards.

d.) Vijay Mallya and Kingfisher Airlines (2012 onwards): Vijay Mallya, the former chairman of Kingfisher Airlines, was involved in a high-profile case of loan default and financial irregularities. Kingfisher Airlines amassed substantial debt and failed to repay loans taken from various banks. Mallya was accused of diverting funds, misusing loans, and non-disclosure of assets. He was declared a wilful defaulter, and legal proceedings are ongoing.

e.) Punjab National Bank (PNB) Fraud (2018): One of the largest banking frauds in India, the PNB fraud involved jeweler Nirav Modi and his companies. Nirav Modi and his associates fraudulently obtained Letters of Undertaking (LoUs) from PNB, which were used to secure credit from other banks abroad. The scam amounted to billions of dollars, and Nirav Modi fled the country. Several bank officials were implicated, and the case highlighted the need for stricter oversight and risk management in the banking sector.

IL&FS Financial Crisis (2018): Infrastructure Leasing & Financial Services (IL&FS) faced a severe financial crisis due to mismanagement and fraudulent practices. The company had significant debt obligations and defaulted on several repayments, leading to concerns about its financial stability. The case exposed governance and regulatory failures in the infrastructure financing sector.

These are just a few examples of prominent banking fraud cases in India. The Indian legal system has taken steps to address such frauds and strengthen regulations to prevent future incidents. However, banking frauds remain a significant challenge, and ongoing efforts are focused on enhancing transparency, risk management, and accountability in the banking sector.

PERSONAL DATA AND LAW JUDGMENT IN BANKING FRAUDS

Personal data protection and privacy are significant considerations in banking fraud cases. While investigating and prosecuting banking frauds, law enforcement agencies and judicial bodies must adhere to legal frameworks that safeguard individuals' personal data. Here's how personal data and law judgment intersect in banking fraud cases:

Data Protection Laws wherein in many countries have data protection laws in place that govern the collection, processing, and sharing of personal data. These laws impose obligations on banks and other entities handling personal data to ensure its confidentiality and security. In banking fraud cases, law enforcement agencies must comply with these data protection laws when accessing and processing personal data as part of their investigations. Law enforcement agencies require a legal basis to access personal data during the investigation of banking fraud cases. This may include obtaining search warrants, court orders, or other legal authorizations to access and retrieve relevant personal data from banks, financial institutions, or other sources. The legal system

ensures that the access to personal data is lawful, proportionate, and respects individuals' privacy rights.

Banks and financial institutions are often required to retain customer transaction data and other relevant records for a specified period. This serves as crucial evidence in banking fraud investigations. Judicial bodies may issue preservation orders to ensure the data is not tampered with or deleted during the investigation and trial process. In some cases, personal data obtained during a banking fraud investigation may need to be anonymized or redacted to protect individuals' privacy. Sensitive information that is not directly relevant to the investigation or trial may be masked or removed to prevent unnecessary disclosure of personal details. In certain instances, court proceedings related to banking fraud cases may be conducted in-camera, meaning they are held privately without public access. This is done to protect the privacy of individuals involved in the case, including victims, witnesses, and those whose personal data may be discussed during the proceedings.

Confidentiality Orders: Courts can issue confidentiality orders to restrict the disclosure of certain personal data or sensitive information related to banking fraud cases. These orders are designed to prevent the unauthorized dissemination of personal information and maintain the privacy of individuals involved in the case. During the judgment phase, courts consider privacy rights and the potential impact of disclosing personal data. Courts aim to strike a balance between the public interest in accessing information and the need to protect individuals' privacy rights. Redactions or anonymization may be applied to the judgment to limit the disclosure of personal data.

It's important for law enforcement agencies and judicial bodies to handle personal data in accordance with the applicable laws and regulations. Data protection laws and privacy considerations ensure that personal data is treated with care and individuals' privacy rights are respected throughout the investigation and judgment processes in banking fraud cases.

COMPARISON OF INDIA BANKING LAWS WITH FOREIGN BANKING LAWS:

Comparing banking laws between countries can be complex and would require a comprehensive analysis.

Regulatory Framework: Each country has its own regulatory framework for the banking sector. In India, the Reserve Bank of India (RBI) is the primary regulatory authority responsible for overseeing banks and financial institutions. Foreign countries have their respective regulatory bodies such as the Federal Reserve in the United States, the Financial Conduct Authority (FCA) in the United Kingdom, or the European Central Bank (ECB) in the Eurozone.

Ownership and Structure: Banking laws may vary regarding ownership and structure. In India, there are different types of banks, including public sector banks, private sector banks, foreign banks, and cooperative banks. Public sector banks are owned by the government, while private sector banks are owned by private entities. Foreign banks operate in India under specific regulations. In some foreign countries, there may be different types of banks, such as commercial banks, savings banks, and credit unions, with varying ownership structures.

Capital Requirements: Banking laws generally prescribe minimum capital requirements for banks to ensure their financial stability. The specific capital adequacy ratios and requirements may differ between countries. For example, the Basel III framework sets international standards for capital adequacy, liquidity, and risk management. However, countries may adopt their own variations and timelines for implementation.

Lending and Credit Policies: Banking laws in different countries may have varying regulations regarding lending and credit policies. This includes rules on interest rates, loan classifications, collateral requirements, and prudential limits on exposure to certain sectors. These regulations aim to maintain financial stability and protect consumers.

Consumer Protection: Consumer protection laws and regulations may differ between countries. In India, the RBI has issued guidelines on fair practices in banking and consumer protection measures. It covers areas such as transparency in disclosures, grievance redressal mechanisms, and the prohibition of unfair practices. Foreign countries may have their own legislation and regulatory bodies to safeguard consumer interests.

Cross-Border Transactions and Anti-Money Laundering (AML): Banking laws also address cross-border transactions, international remittances, and anti-money laundering measures. Regulations on foreign exchange controls, reporting obligations, and KYC (Know Your Customer) requirements can vary between countries. International

cooperation and adherence to international standards like the Financial Action Task Force (FATF) recommendations play a crucial role in combating money laundering and terrorism financing.

It's important to note that the specifics of banking laws can vary significantly between countries, and the above points are meant to provide a general perspective.

INDIAN BANKING LAWS AND ITS IMPLEMENTATION:

Indian banking laws are formulated and implemented by the Reserve Bank of India (RBI), which is the central banking institution in the country. The RBI is responsible for regulating and supervising the banking sector to ensure stability, transparency, and customer protection. Here are some key aspects of Indian banking laws and their implementation:

Banking Regulation Act, 1949: The Banking Regulation Act serves as the primary legislation governing banks in India. It provides the legal framework for the establishment, functioning, and regulation of banks. The act grants the RBI extensive powers to supervise and regulate banks, including licensing, inspection, governance, and resolution of banking institutions.

Prudential Norms: The RBI has implemented prudential norms and guidelines to ensure the financial soundness of banks. These norms cover aspects such as capital adequacy, asset classification and provisioning, exposure limits, liquidity management, risk management, and corporate governance. Banks are required to comply with these norms to maintain financial stability and protect depositors' interests.

Banking Ombudsman Scheme: To address customer grievances and ensure fair banking practices, the RBI has implemented the Banking Ombudsman Scheme. Under this scheme, customers can approach the Banking Ombudsman appointed by the RBI to seek resolution for complaints related to deficiencies in banking services. The scheme aims to provide an accessible and efficient mechanism for resolving customer disputes.

Know Your Customer (KYC) and Anti-Money Laundering (AML) Measures: Indian banking laws require banks to implement stringent KYC and AML measures. Banks are required to verify the identity of customers, maintain records of transactions, and report suspicious activities to the authorities. These measures are aimed at preventing money laundering, terrorist financing, and other financial crimes.

Priority Sector Lending: Indian banking laws mandate that banks allocate a certain percentage of their lending to priority sectors, such as agriculture, small-scale industries, micro, small, and medium enterprises (MSMEs), education, housing, and social sectors. This requirement ensures that banks contribute to the development of these sectors and promote inclusive growth.

Technology and Cybersecurity: The RBI has been proactive in issuing guidelines and regulations to enhance the use of technology in banking while ensuring cybersecurity. These guidelines cover areas such as internet banking, mobile banking, payment systems, data protection, and cybersecurity frameworks. The objective is to promote secure and efficient digital banking services.

Enforcement and Supervision: The RBI has a robust system for enforcement and supervision of banking laws. It conducts regular inspections, audits, and off-site surveillance of banks to assess their compliance with regulatory requirements. The RBI also has the authority to take actions against banks for non-compliance, such as imposing penalties, restrictions, or even revoking licenses if necessary.

It's important to note that the implementation of banking laws in India involves collaboration between the RBI, banks, and other stakeholders. The RBI issues circulars, guidelines, and notifications to banks to communicate regulatory changes and expectations. Banks are responsible for implementing and adhering to these regulations while ensuring proper internal controls, risk management systems, and compliance frameworks.

TRADITIONAL AND MODERN AREAS OF FRAUDS:

Banking frauds encompass a wide range of illegal activities that target financial institutions, their customers, or the overall banking system. These frauds can be categorized into traditional and modern areas based on the techniques and methods employed. Here's an overview of both:

Traditional Areas of Banking Frauds:

Forgery and Counterfeiting: This involves creating fake documents, signatures, or counterfeit currency to deceive banks and customers.

Cheque Fraud: This includes altering or forging cheques, unauthorized cheque issuance, or depositing fraudulent cheques.

Identity Theft: Fraudsters steal personal information, such as social security numbers or banking details, to impersonate individuals and carry out fraudulent activities.

Credit/Debit Card Fraud: Criminals obtain credit/debit card information and make unauthorized transactions or create counterfeit cards.

Insider Fraud: Fraudulent activities carried out by individuals within the bank, such as embezzlement, misappropriation of funds, or manipulating records.

Modern Areas of Banking Frauds:

Phishing and Email Scams: Criminals send deceptive emails or messages posing as legitimate institutions to trick individuals into revealing sensitive information like login credentials or personal details.

ATM Skimming: Criminals install devices on ATMs to capture card information and PINs, allowing them to create cloned cards.

Online Banking Fraud: This includes unauthorized fund transfers, account takeovers, or manipulating online banking systems through various hacking techniques.

Mobile Banking Fraud: Criminals exploit vulnerabilities in mobile banking applications or use fake apps to steal user credentials or conduct fraudulent transactions.

Cryptocurrency Fraud: With the rise of cryptocurrencies, fraudsters have devised schemes such as fake initial coin offerings (ICOs), Ponzi schemes, or hacking exchanges to steal digital assets.

Further the methods and techniques used in banking frauds constantly evolve as technology advances and criminals find new ways to exploit vulnerabilities. Banks and financial institutions implement various security measures, such as advanced authentication systems and transaction monitoring, to combat these fraudulent activities.

LEGAL REMEDIES AND RIGHTS AVAILABLE TO THE VICTIMS OF SUCH CASE.[39]

Victims of banking frauds have various legal remedies and rights available to them to seek justice, compensation, and redress. The specific remedies and rights may vary

[39] https://rbidocs.rbi.org.in/rdocs/content/pdfs/BEAWARE07032022.pdf

depending on the jurisdiction and legal system in place. Some common legal remedies and rights available to victims of banking frauds:

I. Criminal Prosecution: In cases where the banking fraud involves criminal offenses, victims have the right to report the crime to the appropriate law enforcement agency. The authorities will investigate the matter and, if there is sufficient evidence, prosecute the perpetrators. Victims may participate as witnesses in the criminal trial, provide testimony, and seek justice through the criminal justice system.

II. Civil Lawsuits: Victims of banking frauds can file civil lawsuits against the perpetrators to seek compensation for the losses suffered. They can initiate legal proceedings in civil courts and present evidence to establish the liability of the fraudsters. If successful, victims may be awarded monetary damages to cover their financial losses, including the amount of the fraud and any additional damages caused.

III. Consumer Protection Laws: Many countries have consumer protection laws in place that safeguard the interests of consumers in banking transactions. Victims of banking frauds may have rights under these laws, such as the right to refunds, the right to dispute fraudulent transactions, or the right to compensation from the bank or financial institution involved.

IV. Regulatory Complaints: Victims can file complaints with the regulatory bodies overseeing the banking sector. These bodies, such as the central bank or financial regulatory authority, may investigate the matter and take appropriate action against the banks or financial institutions responsible for the fraud. This can include imposing penalties, issuing warnings, or implementing remedial measures.

V. Insurance Claims: If victims have insurance coverage that includes protection against banking frauds, they can file insurance claims to recover their losses. Insurance policies may provide coverage for fraudulent transactions or unauthorized access to bank accounts, subject to the terms and conditions of the policy.

VI. Right to Information: Victims have the right to access information related to their banking transactions and accounts. They can request relevant documents, records,

or statements from the bank or financial institution to understand the details of the fraud and gather evidence for legal proceedings.

VII. Victim Support Services: Some jurisdictions provide victim support services to assist victims of crimes, including banking frauds. These services may offer counseling, legal guidance, and support throughout the process of reporting the fraud, participating in investigations, and seeking legal remedies.

VIII. Privacy Rights: Victims have the right to privacy, especially when personal information has been compromised or misused during the banking fraud. They have the right to request the protection and confidentiality of their personal data during legal proceedings and investigations.

The victims of banking frauds to consult with legal professionals or seek advice from relevant organizations specializing in victim support to understand their specific rights and available legal remedies based on the jurisdiction and laws applicable to their case.

PREVENTIVE AND CURATIVE MEASURES VIS-À-VIS:

Preventive and curative measures are essential to combat banking frauds effectively. Let's explore some preventive and curative measures commonly employed by banks and financial institutions:[40]

Preventive Measures:[41]

Risk Assessment and Management: Banks conduct thorough risk assessments to identify potential vulnerabilities and implement risk management strategies to mitigate fraud risks.

We need to more understand the preventive measures so as to safe us and the society from all sorts of economic offences related to banks and E-Commerce.

1. Multi-factor authentication

The best approach is to start with a multi-factor authentication/multi-layered security structure. Romeo thinks this way from an institution that successfully prevents fraud. “Remember that there is no silver bullet that can solve this problem, so if you put all your hopes in one solution, you are in danger and an intruder has it all.

[40] https://rbi.org.in/scripts/notificationuser.aspx?id=10477/
[41] https://www.bankinfosecurity.com/5-tips-to-reduce-banking-fraud-a-2534

This multi-layered approach from a software perspective combined with the old fashioned out-of-band phone calls to customers to confirm suspicious transactions can reduce headaches for financial institutions and fraud losses for businesses.

In the old days, according to Romeo, calendars were set up for all scheduled transactions on all accounts, whether large or small. “Even if we had a weekly payslip, it would only come out once a week. Then all of a sudden we saw that every day there was some kind of fraudulent activities taking place.

2. Bank monitoring transactions

When Romeo was a banker, the bank says he set a daily limit for each user. “We used to store these limits for mainframe processors along with file limits and batch limits, so we could quickly see if something was added or if something was out of the ordinary. ” Another thing to note is the sheer volume of activities at just under $9,000. "The scammers know that anything under $10,000 won't arouse suspicion from banks."

3. Adjust the company's accounts daily

Romeo recommends companies reconcile bank accounts and transactions daily at the end of the day, or at least the beginning of the day. "This helps you track down transactions you didn't make. The sooner you let your bank know about this, the more likely you are to have them recall or cancel the transaction and get your money back." The longer you wait, the more likely you'll get your money back, the less likely you'll get your money back."

4. Use double and triple checks

Enterprise-side duplicate checking is at least a table issue. Romeo even suggests he makes three checks: one person creates the transaction, the second approves it, and then the third actually submits the transaction. “If you don’t have the people to do it, set up an ACH transaction with the agency, an out-of-band confirmation if it’s a phone call to confirm you sent it, confirmation that the correct information was received.” or through an automated voice response system, usually only one person has the password and ID to call the bank and is completely independent of that person's computer. I have.”

5. Scam Awareness

Finally, according to Romeo, continuous training of enterprise customers is important. This issue of corporate account takeover is also attracting a lot of attention at the national level. But until we understand the real risks facing financial institutions and their corporate customers and can implement simple solutions to mitigate those risks, there will be no real solutions.

Robust Internal Controls: Establishing strong internal control systems, including segregation of duties, dual authorization requirements, and regular audits, helps deter and detect fraudulent activities.

Employee Training and Awareness: Regular training programs educate employees about fraud risks, warning signs, and preventive measures. Awareness campaigns foster a culture of vigilance within the organization.

Customer Education: Banks educate their customers about common fraud schemes, cautioning them against sharing sensitive information and encouraging safe online practices.

Secure Technology Infrastructure: Banks invest in secure technology systems, including firewalls, encryption, and intrusion detection systems, to safeguard customer data and protect against cyberattacks.

Fraud Monitoring and Analytics: Utilizing advanced fraud detection tools and analytics, banks monitor transactions for suspicious patterns or anomalies, enabling timely detection and prevention of fraudulent activities.

Curative Measures:

Incident Response and Investigation: Banks have protocols in place for promptly responding to reported incidents of fraud. They conduct thorough investigations to identify the root cause, gather evidence, and take appropriate legal action.

Collaboration with Law Enforcement: Banks collaborate with law enforcement agencies to report incidents of fraud, provide necessary evidence, and support legal proceedings against fraudsters.

Enhanced Customer Support: Banks offer dedicated support channels for customers to report fraudulent activities, freeze accounts if necessary, and facilitate the recovery of lost funds.

Fraud Insurance and Compensation: Some banks provide fraud insurance or compensation schemes to protect customers from financial losses resulting from fraudulent activities. Continuous Improvement and Adaptation: Banks regularly review and enhance their fraud prevention measures, staying updated with evolving fraud techniques and incorporating new technologies to mitigate risks. No preventive or curative measure can guarantee complete eradication of banking frauds. However, implementing a multi-layered approach combining preventive and curative measures can significantly reduce the risk and impact of fraudulent activities.

BANKING FRAUDS AND CYBER CELL:

Banking frauds often involve the use of technology and the internet, making them fall within the jurisdiction of cybercrime. Cyber cells, also known as cybercrime units or cybercrime investigation cells, are specialized law enforcement units that focus on investigating and combating cybercrimes, including banking frauds. Here's how cyber cells play a role in addressing banking frauds:

Investigation and Forensics: Cyber cells have expertise in investigating cybercrimes, including banking frauds committed through online platforms. They employ digital forensic techniques to gather evidence, trace digital footprints, and identify the perpetrators involved in fraudulent activities.

Collaboration with Financial Institutions: Cyber cells work closely with banks and financial institutions to exchange information, gather evidence, and understand the modus operandi of banking frauds. This collaboration enables effective investigation and the identification of patterns or trends related to specific fraud schemes.

Reporting and Complaint Handling: Individuals or organizations affected by banking frauds can report incidents to the cyber cells. These specialized units handle the complaints, initiate investigations, and take necessary legal action against the perpetrators. They also provide guidance to victims on the steps to be taken and the available legal remedies.

Awareness and Prevention: Cyber cells play a vital role in creating awareness among the general public and financial institutions about the risks and preventive measures related to banking frauds. They conduct awareness campaigns, workshops, and training

programs to educate individuals and organizations on safe online practices, phishing awareness, and secure transaction methods.

Coordination with International Agencies: As banking frauds can often have international dimensions, cyber cells collaborate with international law enforcement agencies and Interpol to investigate cross-border fraud cases. This collaboration facilitates the sharing of intelligence, exchange of information, and extradition of offenders involved in transnational banking frauds.

Legislative Support and Policy Development: Cyber cells contribute to the development and implementation of laws and policies related to cybercrime and banking frauds. They provide insights and expertise to lawmakers and policymakers to create a robust legal framework that addresses emerging cyber threats and ensures effective deterrence against banking frauds.

The specific functions and responsibilities of cyber cells may vary between countries and jurisdictions. However, their overall aim is to investigate and combat cybercrimes, including banking frauds, and protect individuals and organizations from financial losses resulting from fraudulent activities.

LINE OF INVESTIGATION BY CYBER POLICE IN E COMMERCE AND BANKING FRAUDS:

When investigating e-commerce and banking frauds, cyber police follow a systematic line of investigation to gather evidence, identify perpetrators, and build a strong case. The general outline of the steps typically taken in the investigation process:

Complaint Registration: The investigation begins with the registration of a complaint from the victim or the affected financial institution. The complaint should include details of the fraudulent activity, such as unauthorized transactions, identity theft, or account takeover.

Evidence Collection: Cyber police collect relevant evidence to establish the occurrence of the fraud and identify the individuals involved. This may involve retrieving transaction records, communication logs, IP addresses, server logs, and any other digital evidence associated with the fraud.

Digital Forensics: Cyber police employ digital forensic techniques to analyze the seized digital evidence. They examine devices, including computers, mobile phones, and

storage media, to uncover traces of the fraudulent activities, identify the methods used, and establish the trail of the funds involved.

Tracing the Money Trail: In cases involving financial transactions, cyber police work to trace the movement of funds. This includes tracking bank accounts, electronic wallets, cryptocurrency transactions, and other financial instruments used by the fraudsters to launder or transfer the illicit proceeds.

Suspect Identification: Based on the collected evidence, cyber police attempt to identify the individuals or groups responsible for the fraud. This may involve tracing IP addresses, analyzing communication patterns, and collaborating with financial institutions and online platforms to gather additional information.

Collaboration with Financial Institutions: Cyber police work closely with banks and financial institutions to obtain transaction records, account details, and other relevant information. This collaboration helps in identifying any insider involvement, fraudulent accounts, or compromised systems within the financial institution itself.

International Cooperation: In cases where the fraud has cross-border elements, cyber police collaborate with international law enforcement agencies and Interpol. This enables the sharing of information, coordination of efforts, and potential extradition of suspects involved in transnational frauds.

Legal Action: Once the investigation is complete and sufficient evidence is gathered, cyber police initiate legal action against the perpetrators. This may involve filing charges, preparing a case for prosecution, and supporting the legal process to ensure that the offenders are held accountable for their actions.

Throughout the investigation, cyber police also focus on preserving the chain of custody for the collected evidence, adhering to legal and procedural requirements, and maintaining the confidentiality of sensitive information.

It's important to note that the specific steps and procedures may vary depending on the jurisdiction, legal frameworks, and available resources of the cyber police unit.

MEASURES IF CYBER POLICE FAILS TO REGISTER COMPLAINT IN BANKING FRAUDS:

If an encounter situation arises where the cyber police fail to register the complaint related to banking frauds, there are several steps that can be taken to escalate the matter and ensure that the complaint is appropriately addressed:

Approach Higher Authorities: If your complaint is not being registered or taken seriously by the local cyber police unit, you can escalate the matter to higher authorities within the law enforcement agency. Contact the supervising officer or the senior official in charge and explain the situation, providing all relevant details and evidence.

File a Written Complaint: Prepare a written complaint outlining the details of the banking fraud, including the nature of the fraud, the losses incurred, and any evidence you have. Submit the written complaint to the cyber police unit, ensuring that you keep a copy for your records. This helps create a formal record of your complaint and ensures that it cannot be easily dismissed.

Contact Banking Regulatory Authorities: If you are unable to get your complaint registered with the cyber police, you can reach out to the relevant banking regulatory authorities in your jurisdiction. These authorities, such as the central bank or financial regulatory agencies, often have dedicated departments or units to handle complaints related to banking frauds. They can guide you on the next steps to take and may have the authority to intervene on your behalf.

Seek Legal Assistance: Consider consulting with a lawyer who specializes in cybercrime or banking fraud cases. They can provide you with legal advice, assess the situation, and guide you on the available legal options. They may also be able to assist you in escalating the complaint or initiating legal action if necessary.

Report to Consumer Protection Agencies: In many jurisdictions, there are consumer protection agencies or ombudsman offices that handle complaints related to financial services. These agencies can investigate and mediate disputes between consumers and financial institutions. Contact the relevant agency in your jurisdiction and file a complaint with them, providing all the details and evidence of the banking fraud.

Report to Law Enforcement Watchdogs: Some countries have independent oversight bodies or watchdog organizations that monitor law enforcement agencies' performance and handle complaints related to their conduct. If you believe your complaint has been mishandled or ignored by the cyber police, you can report the issue to such organizations, providing them with the necessary information and evidence.

Remember to maintain a record of all communication, including dates, names, and positions of the individuals you interact with during the complaint registration process. This documentation can be valuable in case you need to escalate the matter further or seek legal recourse.

IF A BANKING FRAUD DONE IN INDIA, IS IT IMPOSSIBLE TO REACH THE CULPRIT?

While it can be challenging to reach the culprits of banking frauds in any jurisdiction, including India, it is not accurate to say that it is impossible. The investigation and prosecution of banking frauds involve multiple steps and cooperation from various entities. Here are some factors to consider when addressing banking frauds in India:

Reporting the Fraud is the first step and it is essential to report the fraud to the relevant authorities, such as the cyber police or the Economic Offences Wing (EOW). Provide them with all the necessary details and evidence to initiate an investigation. Believing on the investigation Process wherein once the complaint is registered, the cyber police or the EOW will conduct an investigation to gather evidence and identify the culprits. This may involve digital forensics, tracking financial transactions, and working with banks and other relevant entities to trace the funds and identify the individuals involved.

The Legal Framework where there are various laws and regulations in place to address banking frauds, such as the Indian Penal Code, the Information Technology Act, and the Prevention of Money Laundering Act. These laws provide a legal framework for investigating and prosecuting such offenses. On the other hand in cases where the fraud has international dimensions, authorities in India can collaborate with international law enforcement agencies, Interpol, or other relevant entities to seek assistance, share information, and potentially extradite suspects. The cooperation of the financial Institutions' play a crucial role in investigating banking frauds. They are required to cooperate with law enforcement agencies and provide information related to transactions, accounts, and other relevant data that can help in identifying the culprits.

Moreover, if the investigation yields sufficient evidence, legal proceedings can be initiated against the culprits. The case will be presented in the appropriate court, and if the accused is found guilty, they can be held accountable for their actions. While the process of reaching the culprits of banking frauds can be complex and time-consuming, it is not impossible. It requires a thorough investigation, cooperation from relevant

stakeholders, and adherence to legal procedures. It is important to have faith in the legal system and work closely with the authorities to ensure that the culprits are identified and brought to justice.

FOREIGN BANKING LAWS AND ITS IMPLEMENTATION IN FOREIGN COUNTRIES:

Foreign banking laws and their implementation vary across different countries based on their legal and regulatory frameworks. some general aspects of foreign banking laws and their implementation:

Regulatory Bodies: Each country has its regulatory body responsible for overseeing the banking sector. For example, in the United States, the Federal Reserve System (the Fed), the Office of the Comptroller of the Currency (OCC), and the Federal Deposit Insurance Corporation (FDIC) play key roles in regulating and supervising banks. In the United Kingdom, the Financial Conduct Authority (FCA) and the Prudential Regulation Authority (PRA) regulate and supervise banks. These regulatory bodies establish rules, issue guidelines, and enforce compliance with banking laws.

Licensing and Entry Requirements: Foreign banking laws typically outline the licensing and entry requirements for banks. These laws set criteria for obtaining a banking license, such as capital requirements, fit and proper criteria for bank directors and executives, and disclosure obligations. Banks must meet these requirements to operate legally within a foreign country.

Prudential Regulations: Foreign banking laws include prudential regulations aimed at ensuring the stability and soundness of banks. These regulations cover areas such as capital adequacy, liquidity management, risk management, asset quality, provisioning, and governance. Banks must comply with these regulations to maintain financial stability and protect customer interests.

Consumer Protection: Many countries have specific laws and regulations focused on consumer protection in banking. These laws aim to ensure fair practices, disclosure of terms and conditions, transparent pricing, and effective mechanisms for resolving customer complaints. Consumer protection agencies or ombudsman schemes may be established to address customer grievances and enforce compliance with consumer protection laws.

Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF): Foreign banking laws include measures to combat money laundering, terrorist financing, and other financial crimes. These measures often require banks to implement stringent Know Your Customer (KYC) procedures, report suspicious transactions, and maintain adequate AML/CTF controls. Regulatory authorities may conduct inspections and impose penalties for non-compliance with AML/CTF requirements.

Cross-Border Transactions and Foreign Exchange Controls: Foreign banking laws address cross-border transactions and foreign exchange controls. Regulations may cover foreign currency transactions, capital flows, repatriation of funds, restrictions on certain types of transactions, and reporting obligations for foreign currency transfers. These regulations ensure orderly conduct of cross-border banking activities and safeguard the stability of the foreign exchange market.

Supervision and Enforcement: Foreign banking laws establish supervisory mechanisms to monitor and enforce compliance with regulatory requirements. Regulatory bodies conduct regular inspections, audits, and off-site surveillance of banks. They have the power to take enforcement actions, including imposing penalties, restrictions, or revoking licenses in cases of non-compliance.

Foreign banking laws and their implementation can vary significantly between countries. Each country has its legal and regulatory frameworks tailored to its unique financial system, market structure, and priorities. Banks operating in foreign countries must understand and comply with the relevant laws and regulations to ensure legal and regulatory compliance.

KEY REASONS OF FRAUDS IN INDIAN BANKING SYSTEM AND INTERNATIONAL BANKING SYSTEM:

INDIAN BANKING SYSTEM	INTERNATIONAL BANKING SYSTEM
Weak Internal Controls: Inadequate internal control mechanisms within banks can create opportunities for fraud. Weak control systems, including lax oversight, poor risk management, and insufficient monitoring of transactions,	**Complexity of Cross-Border Transactions:** International banking involves complex transactions across different jurisdictions, currencies, and regulatory frameworks. The complexity of cross-border transactions can

can allow fraudsters to exploit loopholes and carry out fraudulent activities. **Collusion and Insider Fraud:** Collusion between bank employees and external fraudsters is a significant factor in banking frauds. Insider fraud occurs when employees misuse their positions and access to manipulate transactions, fabricate documents, or facilitate fraudulent activities in collusion with external parties. **Lack of Awareness and Training:** Insufficient awareness and training among bank employees about fraud prevention and detection can contribute to the occurrence of frauds. Banks need to invest in training programs to educate employees about the latest fraud techniques, emerging risks, and best practices for fraud prevention. **Technological Vulnerabilities:** With the increasing use of technology in banking operations, cyber threats and technological vulnerabilities have become significant concerns. Hackers and cybercriminals exploit weaknesses in banks' IT systems, leading to data breaches, unauthorized access, identity theft, and financial fraud. **Loan-Related Frauds:** Loan-related frauds, including fraudulent lending practices and loan default cases, pose a	create opportunities for fraudsters to exploit gaps, inconsistencies, or weak controls in the international banking system. **Lack of Standardization:** There is a lack of global standardization in banking regulations, reporting requirements, and supervisory frameworks. Differences in regulatory regimes across countries can be exploited by fraudsters who take advantage of weak or inconsistent regulations to engage in fraudulent activities. **Money Laundering and Terrorist Financing:** International banking systems are vulnerable to money laundering and terrorist financing activities. Fraudsters may attempt to use international banking channels to disguise the illicit origin of funds, transfer money across borders, or finance illegal activities. **Insider Fraud and Collusion:** Insider fraud, where bank employees or insiders misuse their positions and access, is a significant factor in international banking frauds. Collusion between bank employees and external fraudsters can facilitate complex fraud schemes involving multiple jurisdictions. **Technological Vulnerabilities and Cybercrime:** The reliance on technology in international banking exposes vulnerabilities to cybercrime. Cybercriminals can exploit weaknesses in banks' systems, networks, and

significant risk to the banking system. These frauds can involve false documentation, inflated collateral valuations, diversion of funds, and non-disclosure of vital information. **Regulatory Gaps and Weak Enforcement:** Weak regulatory frameworks and gaps in oversight and enforcement can contribute to banking frauds. Inadequate supervision, delayed actions against fraudulent entities, and limited coordination between regulatory bodies can create an environment conducive to fraud. **Financial Inclusion Challenges:** India's efforts to promote financial inclusion have led to the expansion of banking services in remote and rural areas. However, the challenges associated with reaching unbanked populations can increase the risk of frauds, including identity theft, ghost accounts, and misuse of government welfare schemes. **Corruption and Money Laundering:** Corruption and money laundering activities in the banking sector can facilitate frauds. Bribery, nepotism, and unethical practices can undermine the integrity of the banking system and provide opportunities for fraudulent activities.	digital infrastructure to gain unauthorized access, steal sensitive information, and carry out fraudulent transactions. **Jurisdictional Challenges:** International banking frauds can be challenging to investigate and prosecute due to jurisdictional issues. Fraudsters often operate across multiple countries, taking advantage of differences in legal systems, extradition treaties, and international cooperation. **Lack of Information Sharing:** Inadequate information sharing and coordination between regulatory bodies and financial institutions across different countries can hamper the timely detection and prevention of international banking frauds. Enhanced international cooperation and information exchange are essential to combat cross-border fraud. **Cultural and Language Barriers:** Differences in cultures, languages, and business practices across countries can create challenges in understanding and detecting fraudulent activities. Fraudsters may exploit these differences to manipulate transactions or deceive banks and customers.

Addressing these challenges requires a multi-faceted approach, including strengthening internal controls, enhancing employee training and awareness, improving regulatory frameworks and enforcement, adopting robust technological safeguards, and promoting a culture of ethics and integrity within the banking sector whereas Addressing frauds in the international banking system requires international collaboration, regulatory harmonization, and the implementation of robust risk management frameworks. Strengthening cybersecurity measures, enhancing information sharing mechanisms, promoting international cooperation, and adopting advanced technologies for fraud detection and prevention are key strategies to mitigate fraud risks in the international banking system.

CROSS BORDER CASE LAWS ON BANKING LAWS:

International case laws on banking frauds vary from country to country, as legal systems and regulations differ worldwide. However, several landmark cases related to banking fraud have received international attention. Some notable examples include:

Enron Scandal (United States, 2001): Although not specifically a banking fraud case, the Enron scandal involved accounting fraud by the energy company Enron. It highlighted issues of corporate governance, financial reporting, and auditing practices, leading to significant changes in regulations and corporate oversight.

Société Générale Rogue Trader Case (France, 2008): In this case, a trader named Jérôme Kerviel caused significant losses to Société Générale through unauthorized trades. The case raised questions about risk management and internal control within financial institutions.

Bernie Madoff Ponzi Scheme (United States, 2008): Bernie Madoff orchestrated one of the largest Ponzi schemes in history, defrauding investors of billions of dollars. The case exposed weaknesses in regulatory oversight and investor protection mechanisms.

Nirav Modi Fraud Case (India, 2018): Indian jeweler Nirav Modi and his associates were accused of defrauding the Punjab National Bank (PNB) of billions of dollars through

fraudulent issuance of letters of undertaking. This case highlighted lapses in the banking system's internal controls and prompted reforms in India's banking sector.

1Malaysia Development Berhad (1MDB) Scandal (Malaysia, 2015-ongoing): The 1MDB scandal involved the misappropriation of funds from a Malaysian state investment fund. The case has led to investigations and legal proceedings in multiple jurisdictions, including the United States, Switzerland, and Singapore.

IMPORTANT PREVETIVE WAYS TO COMBAT BANKING FRAUDS AND SAFEGUARDS:

Defining what constitutes bank fraud is fundamental, as definitions have the role and power to determine the scope and impact of a crime. Also, when defining bank fraud, ensure that the definition is broad enough to cover both traditional and emerging bank fraud that is occurring now and may occur in the future. should be noted. Therefore, the task of defining "bank fraud" must be left to a panel of experts.

- Bank fraud is recognized as a separate crime, but care should be taken to define it clearly as a socio-economic crime so that the perpetrators of the crime do not benefit from a trial under Chapter 21 of the Code of Criminal Procedure 1973; have to pay about bank fraud.
- The evolution of banking over the years has revealed that banking institutions are rapidly entering other commercial activities such as insurance and securities trading. The same is true for other for-profit companies. The RBI's recent move to license new private banks, and the spate of applications for those licenses by various incumbents, demonstrate that the lines between banking and other economic activities are rapidly disappearing. While this could contribute to accelerating economic growth, at the same time, a cautious view of the problem of bank fraud suggests that this mingling of banking and other commercial activities could lead to any It could mean that financial fraud is considered bank fraud scam. The old adage that prevention is better than cure applies to the problem of bank fraud.
- An investigation establishes the basis for conviction of a crime. The same is true for bank fraud. Investigations and law enforcement agencies will therefore continue to play a very important role in creating a fraud-free banking environment.

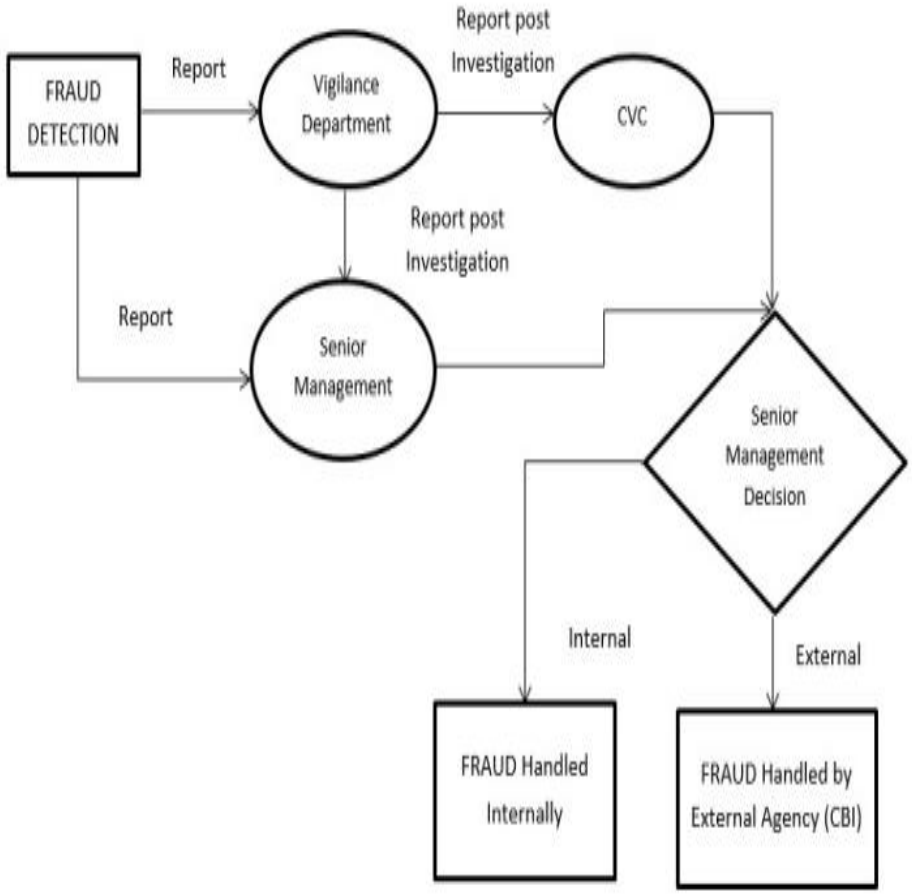
The judicial system creates the mechanisms for law enforcement. Structured according to the court system, there are many factors that determine the usefulness and effectiveness of substantive law in solving a particular problem. In the established court system that currently exists in India, some changes would go a long way in curbing the threat of bank fraud effectively.

From a procedural point of view, summary proceedings in lieu of normal court proceedings in bank fraud cases (up to certain limits) are time-saving and effective in ensuring prompt resolution of bank fraud cases. It is proved that there is. Money loss due to bank fraud leads to reduced time. Similarly, shifting the burden of proof in white-collar crimes to defendants may prove helpful in securing effective trials. It is also desirable to clarify the jurisdictional issues of the various national courts to avoid delays in hearings due to jurisdictional disputes.

- Further development of the consumer rights perspective on the issue of bank fraud is urgently needed, as economic losses from bank fraud ultimately affect customers who use banking services. Because even if the bank goes bankrupt due to financial fraud, customers risk losing their hard-earned money at the bank. Bank customers should therefore be considered not only as contracting parties to banking services, but also as consumers of banking services, as they are the central figure in all banking operations and the central figure in banking as a whole. . Banking systems exist.

The many challenges banks face in the 21st century have necessitated a reassessment of their legal strategies and processes in order to remain active in the Danish environment. The analytical review therefore clearly shows that the banking system is facing challenges due to social development and the revolution brought about by new scientific technologies. Nineteenth-century laws, modestly aided by a progressive 21st-century legislature, cannot withstand the constant onslaught of bank fraud.

Figure 5: Flow Chart depicting procedures post Fraud Detection and Reporting in PSBs



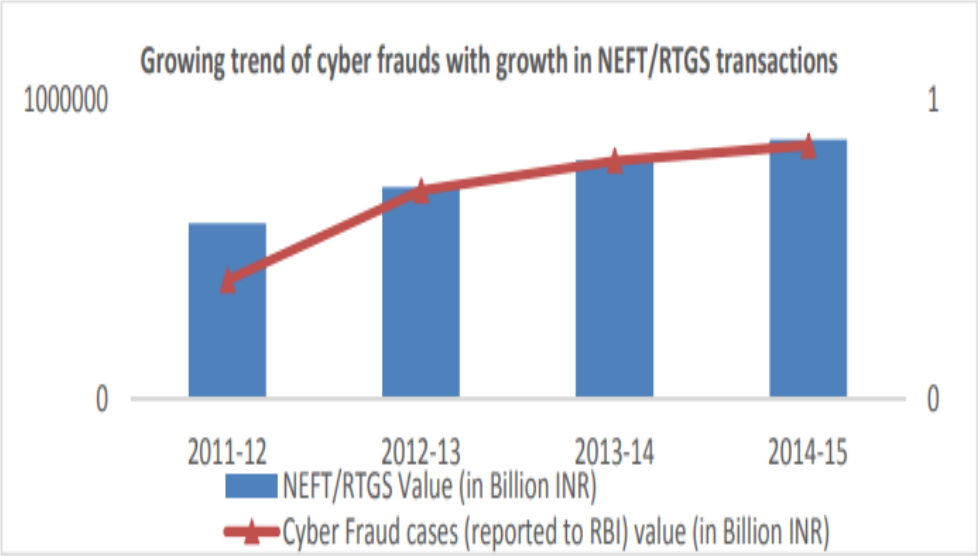
Source: Author's line-chart.

GRAPHICAL INDICATION OF BANKING FRAUD CASES:

India has witnessed a massive surge in cybercrime incidents in the last ten years - from just 23 in 2004 to 72,000 in 2014-15 (Figures 3 and 4). As per the government's cyber security arm, computer emergency response team-India (CERT-In), 62,189 cyber security incidents were reported in just the first five months of 2015-16.

CYBER FRAUDS:

Figure 3: Cyber Frauds



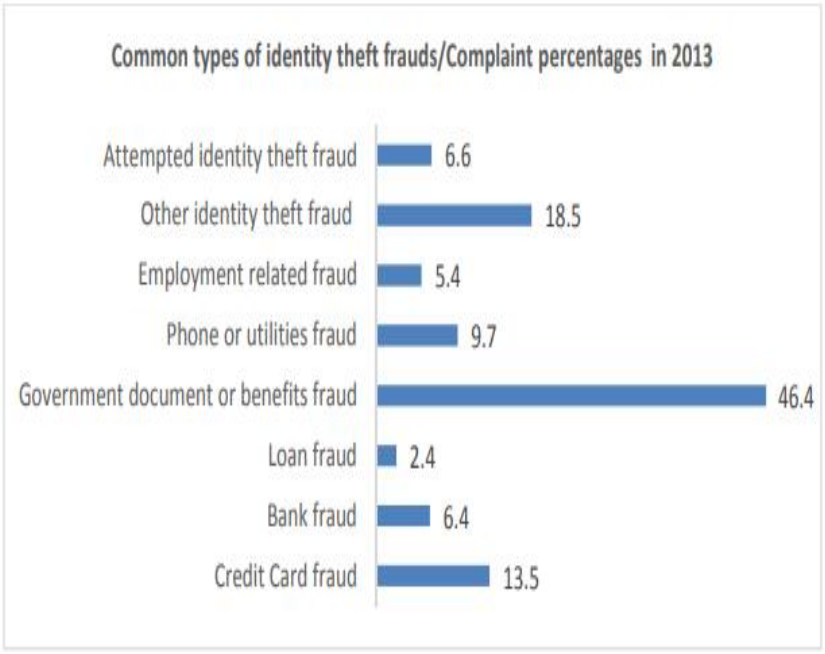
Source: PWC India and ASSOCHAM (2014).

Figure 1: Group wise summary of bank fraud cases

Note: Data pertains to the period from March 31, 2010 to March 31, 2013.
Source: Chakrabarty (2013).

Figure 2: Group wise summary of advance related fraud cases

Note: Data pertains to the period from March 31, 2010 to March 31, 2013.
Source: Chakrabarty (2013).



Source: PWC India and ASSOCHAM (2014).

CHAPTER 4

CONCLUSION

Since every coin has two faces, it is clear that advances in cyberspace have brought crime along with its many advantages. Needless to say, cybercriminals are following the progress in this field, and criminal incidents in cyberspace clearly demonstrate the seriousness of the situation. The Indian parliament has passed his two-pronged strategy to combat cybercrime. It has amended the Indian Penal Code, which specifically targets cybercrime, and introduced provisions in the IT Act to combat cybercrime. However, the law is very narrow in purpose and focused on e-commerce, so it is not comprehensive. Cybercrimes come under either criminal offences or civil wrongs. Some of them come under civil as well as criminal offences and can be called hybrid cybercrimes and they have both civil and criminal liability. Therefore, it is concluded that the need is not only to have appropriate legal provisions for cybercrime but also creating awareness among general public and the law enforcement agencies. The growth of technology in this field has been stupendous with a faster growth of cybercrimes. There have been efforts at international and national levels to control and regulate cybercrime but these efforts have not proven to be sufficient so far and the result is that crime is many steps ahead of any such attempts. In our opinion, a formally adopted universal legal framework around the world, backed by professional and well-resourced law enforcement mechanisms and sufficient public awareness, is the threat of white-collar crime. will be of great help in controlling and inducing The proposed hypotheses, if implemented in an effective and coordinated manner, could go a long way toward making this unprecedented scientific wonder sustainable not only for the present generation, but for many generations to come. [42]

RECOMMENDATIONS

We can see that public financial service providers outperform PVB in terms of the total number of bank fraud incidents. However, the total amount is much higher for public broadcasting than for private broadcasting. This is because public broadcasters offer large amounts of credit to their customers. Loan fraud has the highest impact of all bank fraud cases in India due to the high amounts involved and the cumbersome process of

[42] Dr. Amita Verma, Simi K Bajaj; Cyber Fraud: A digital Crime; IADIS International Conference Information Systems 2008

fraud detection by CVCs. Corruption may be primarily due to lack of proper oversight by top management and flawed employee incentive mechanisms. Collusion between employees, corporate borrowers with the third parties. Weak regulatory system. Lack of appropriate tools and technology to detect early signs of fraud. Lack of awareness between bankers and customers. and lack of coordination between different banks in India and abroad. Delays in the legal reporting process and various loopholes in the system are believed to be some of the major reasons for fraud and NPAs.

Despite their best efforts, banks have had limited success in convicting those responsible for financial crimes. One of the main causes of this problem is the lack of professional financial detectives with knowledge of the nuances of forensic accounting and a good legal understanding of fraud. Therefore, following recommendations are suggested for an early detection of frauds.

a) Independent expert executives:

The Government should appoint independent professional executives along all services of India who have the best financial and legal expertise to detect financial fraud and who can carry out effective and timely investigations of such fraud. You may consider executives. In the short term, the government may consider forming this cadre through side recruitment of private bankers, central banks and central bank officials.

b) Know your market:

In addition to knowing providers and customers, banks must also focus on knowing the market. All banks should have a dedicated department that assesses the macroeconomic environment of the companies they finance and the industries and markets in which their products are sold. This recommendation seems reasonable given the recent market crash in China. Several Indian manufacturing companies, which depended on importing machinery from China, were unable to start projects and generate cash flow, which affected the lending banks.

c) Internal Rating Agencies:

Banks must have strong internal rating agencies that rate large projects before approving loans. Rating agencies rate projects strictly based on business models and project plans, taking into account current macroeconomic conditions and the sector's exposure to the global economy, without being influenced by the brand name or creditworthiness of the

parent company. There is a need to. If internal and external agency assessments are not similar, an investigation should be performed to determine the cause of the differences. Moreover, when evaluating such projects, banks should use the services of at least two to three independent auditors to avoid possible collusion. d) Use of the latest technology:

Bank data collection mechanisms are very outdated and need a thorough overhaul. Banks should employ the best available IT systems and data analytics to ensure effective implementation of the RBI's proposed Red Flag Account (RFA) and Early Warning Signal (EWS) frameworks. This leads to better profiling of customer contributing patterns through analytics. This will allow banks to work and monitor in near real time. In addition, we encourage the Institute for Banking Technology Development Research (IDRBT) to consider encouraging the development of relevant software for commercial banks at affordable costs. This is essential to strengthen surveillance of suspicious and fraudulent transactions at bank branches.

e) Monitoring of vandalism at the local level:

The RBI may consider expanding the scope of its surveillance and should monitor the movement of trading outliers at the regional level in line with SEBI's circuit breakers, which will track signs of financial fraud as early as possible. can be effective in doing so.

f) Strong punitive measures against third parties:

Governments should investigate the role of third parties such as accountants, lawyers, auditors and rating agencies involved in bank fraud-related accounts and consider introducing harsh penalties to deter future prosecutions. . There are also arguments to question the authentication/credentials of third parties, such as auditors, to assess their ability to assess accounts that may contain fraudulent entries.

g) Strict Laws to Prevent Fraudulent Financial Reporting:

There are a number of areas where current legislation could be strengthened to improve accountability for auditors' work.

I. One of them could be a stronger KYC code. A benchmark in this case could be the guidelines issued by the OECD regulating Trust and Corporate Service Providers (TCSPs), which have helped extend liability for misconduct in these institutions to lawyers and accountants. rice field. In India, NBFCs are required to take a similar approach and report

suspicious trading activity. However, this has not been done effectively as these laws are very weak in their current form.

II. Another law that could be strengthened is willful inaction, which should be classified as a criminal offence. It is now a civil offense under Indian law but a criminal offense in other countries.

h) Means of Ground Reconnaissance:

Banks need to have an intelligence repository that can be used to track borrower activity to ensure real-time compliance and early detection of fraud. A dedicated fraud monitoring unit with highly qualified and trained staff should be established within the bank. It also requires professional research institutes with the expertise of institutions such as CBI, RBI, SEBI and commercial banks.

i) Dedicated departments dealing with fraud cases:

All corporate branches of public authorities should have a dedicated legal department that acts as a one-stop shop for law enforcement agencies and provides easy access to relevant documents.

j) Financial Education:

Employees often do not know the exact definition of fraud, so they need to be informed about this aspect. Therefore, employees should be provided with regular employee learning sessions and global best practices for early detection and prevention of fraud. E-modules with E-certification and updates will be made available periodically.

k) Transparent Recruitment and Appropriate Compensation:

Banks need to ensure corporate governance at the highest level. Top management must establish guidelines and guidelines for ethical practices and standard procedures to be followed at all times and set an example of zero tolerance for negligence or wrongdoing. Considering the roles and responsibilities of top management, emphasis should be placed on proper recruitment processes at the top management level, with a minimum term of three years and preferably accountability clauses. Incentive mechanisms also need to be changed to balance short-term and long-term goals.

l) Interagency coordination:

Sharing sensitive information about the personal wealth of project proponents requires clandestine coordination between banks and authorities such as the Central Board of Direct Taxes (CBDT). In the event of information of concern, CVC and RBI should work together to investigate misconduct by event organizers.

Lastly we can say that many Laws have been made to control all this irrelevant things but still there are no such proper departments allotted which can handle all this abrupt activities due to which the Criminals take more and more advantage and it gives them immense courage to indulge more into it as there is no tight securities as such. Therefore, the legal system awakens and required to make certain legislations to protect the interest of the entire society. Therefore, this new branch of law is emerged, because the conventional procedure to prevent the crime is useless for offences committed through the computer or internet. The rules and regulation, which deals with the cyber space internet and its regulation, are subject matter of the cyber laws.

BOOKS:

Taxmann, Cyber Crimes and Cyber

Jain MP Indian Constitutional Law; LexisNexis Butterworths Wadhwa, Volume 1; 6th Edition, 2010.

Dr. JN Pandey, Constitution of India; Central Law Agency, 52nd Edition.

VN SHUKLA; The Constitution of India; Eastern Book Company; 2017.

K.D. Gaur; Indian Penal Code; Edition 2019

Universal Bareact of Prevention of Corruption Act

Universal Publication Bareact of Negotiable Instrument Act.

Eastern Book Company Bareact of Banking Regulation Act.

Universal Publication Bareact of Prevention of Money Laundering Act.

Universal Publication Bareact of Information Technology Act,2000.

Sood, V. (2001); Cyber Law simplified

REFERENCES:

https://www.sciencedirect.com/journal/electronic-commerce-research-and-applications

https://www.ijser.org/researchpaper/Cybercrimes-in-E-commerce.pdf

https://www.techtarget.com/searchsecurity/definition/cybercrime

http://puneresearch.com/media/data/issues/5c0aba271062d.pdf

Laws on Cyber Crime: P .K. Singh, (2007) Book Enclave, Jaipur, Page 48.

https://www.business-standard.com/article/finance/sbi-ex-chief-pratip chaudhuriarrested-sent-to-14-day-judicial-custody-121110200055_1.html

https://www.verywellmind.com/what-is-cyberstalking-5181466

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2741013

Chapter III; The Law Relating to Cyber Crime in India.

Laws on Cyber Crime: P .K. Singh, (2007) Book Enclave, Jaipur, Page 58.

https://www.acfe.com/fraud-101.aspx

https://www.lawctopus.com/symbiosis-law-school-hyderabad-digital-art-competition//

Sharma Vakul; E-Commerce: A New business paradigm, in legal dimensions of Cyberspace; Indian Law Institute, New Delhi, 2004.

See, www.wto.org.

See, http://europa.eu.int.

See, www.gartner.com

Davies, LJ; "A model for internet regulation" (1998).

https://www.iimb.ac.in/sites/default/files/2018-07/WP_No._505.pdf.

https://www.ca-cib.com/sites/default/files/2021-10/Basel-III-Disclosures_0921.pdf

https://www.investopedia.com/terms/r/retailbanking.asp#:~:text=Retail%20banking%2C%20also%20known%20as,money%20in%20a%20secure%20manner

Patrick E Cole et al; "Business – The internet economy".

Hammond Suddards, Credit Cards 68 (1999).

Prabhakar Kiron; Payment Mechanism in cyberspace; Legal Dimensions of Cyber Space; Indian Law Institute.

http://www.davidreilly.com.

https://www2.deloitte.com/content/dam/Deloitte/in/Documents/finance/in-finance-annual-fraud-survey-noexp.pdf

https://www.nachrcoi.co.in/our-services/banking-fraud-legal-guidance/

Derry v. Peek, (1889) 14 AC 337 : 5 TLR625.

https://economictimes.indiatimes.com/wealth/save/10-types-of-banking-frauds-in-india-customers-should-know-about/articleshow/90438911.cms

The RBI Master Circular on 'Frauds-Classification and Reporting', dated July 02, 2012.

https://rbi.org.in/scripts/notificationuser.aspx?id=10477/

https://www.bankinfosecurity.com/5-tips-to-reduce-banking-fraud-a-2534

Dr. Amita Verma, Simi K Bajaj; Cyber Fraud: A digital Crime; IADIS International Conference Information Systems 2008

BIBLIOGRAPHY

1. Taxmann, Cyber Crimes and Cyber
2. Jain MP Indian Constitutional Law; LexisNexis Butterworths Wadhwa, Volume 1; 6th Edition, 2010.
4. Dr. JN Pandey, Constitution of India; Central Law Agency, 52nd Edition.
5. VN SHUKLA; The Constitution of India; Eastern Book Company; 2017.
6. K.D. Gaur; Indian Penal Code; Edition 2019
7. Universal Bareact of Prevention of Corruption Act
8. Universal Publication Bareact of Negotiable Instrument Act.
9. Eastern Book Company Bareact of Banking Regulation Act.
10. Universal Publication Bareact of Prevention of Money Laundering Act.
11. Universal Publication Bareact of Information Technology Act,2000.
12. Sood, V. (2001); Cyber Law simplified

WEBSITES

13. https://www.sciencedirect.com/journal/electronic-commerce-research-and-applications
14. https://www.ijser.org/researchpaper/Cybercrimes-in-E-commerce.pdf
15. https://www.techtarget.com/searchsecurity/definition/cybercrime
16. http://puneresearch.com/media/data/issues/5c0aba271062d.pdf
17. Laws on Cyber Crime: P .K. Singh, (2007) Book Enclave, Jaipur, Page 48.
18. https://www.business-standard.com/article/finance/sbi-ex-chief-pratip chaudhuriarrested-sent-to-14-day-judicial-custody-121110200055_1.html
19. https://www.verywellmind.com/what-is-cyberstalking-5181466
20. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2741013
21. Chapter III; The Law Relating to Cyber Crime in India.

22. Laws on Cyber Crime: P .K. Singh, (2007) Book Enclave, Jaipur, Page 58.

23. https://www.acfe.com/fraud-101.aspx

24. https://www.lawctopus.com/symbiosis-law-school-hyderabad-digital-art-competition//

25. Sharma Vakul; E-Commerce: A New business paradigm, in legal dimensions of Cyberspace; Indian Law Institute, New Delhi, 2004.

26. See, www.wto.org.

27. See, http://europa.eu.int.

28. See, www.gartner.com

29. Davies, LJ; "A model for internet regulation" (1998).

30. https://www.iimb.ac.in/sites/default/files/2018-07/WP_No._505.pdf.

31. https://www.ca-cib.com/sites/default/files/2021-10/Basel-III-Disclosures_0921.pdf

32.https://www.investopedia.com/terms/r/retailbanking.asp#:~:text=Retail%20banking%2C%20also%20known%20as,money%20in%20a%20secure%20manner

33. Patrick E Cole et al; "Business – The internet economy".

34. Hammond Suddards, Credit Cards 68 (1999).

35. Prabhakar Kiron; Payment Mechanism in cyberspace; Legal Dimensions of Cyber Space; Indian Law Institute.

36. http://www.davidreilly.com.

37. https://www2.deloitte.com/content/dam/Deloitte/in/Documents/finance/in-finance-annual-fraud-survey-noexp.pdf

38. https://www.nachrcoi.co.in/our-services/banking-fraud-legal-guidance/

39. Derry v. Peek, (1889) 14 AC 337 : 5 TLR625.

40. https://economictimes.indiatimes.com/wealth/save/10-types-of-banking-frauds-in-india-customers-should-know-about/articleshow/90438911.cms

41. The RBI Master Circular on 'Frauds-Classification and Reporting', dated July 02, 2012.

42. https://rbi.org.in/scripts/notificationuser.aspx?id=10477/

43. https://www.bankinfosecurity.com/5-tips-to-reduce-banking-fraud-a-2534

44. Dr. Amita Verma, Simi K Bajaj; Cyber Fraud: A digital Crime; IADIS International Conference Information Systems 2008

CERTIFICATE OF PLAGIARISM CHECK

Certificate of Plagiarism Check
Title of Work: E-COMMERCE: GENERAL CHALLENGES AND STRIVE IN COMBATING E-FRAUDS"
Author(s) of Work: SUMBUL NAQVI
Date of Check:
Result of Check:
Plagiarism Checking Tool Used:
Statement of Originality:
Name of Person Conducting Check:
Signature:
Date: