INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 4 AND ISSUE 4 OF 2024

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

# CRITICAL EVALUATION OF LEGAL MECHANISM GOVERNING BANKING FRAUDS WITH SPECIAL REFERENCE TO ONLINE FRAUDS

**AUTHORS –** RADHIKA* & DR. RAJIV BHALLA**, LL.M. (MASTER OF LAWS) SCHOLAR* & PROFESSOR**, UNIVERSITY INSTITUTE OF LEGAL STUDIES, CHANDIGARH UNIVERSITY, MOHALI, PUNJAB, INDIA

**BEST CITATION** - RADHIKA & DR. RAJIV BHALLA, CRITICAL EVALUATION OF LEGAL MECHANISM GOVERNING BANKING FRAUDS WITH SPECIAL REFERENCE TO ONLINE FRAUDS, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 4 (4) OF 2024, PG. 330-342, APIS – 3920 – 0001 & ISSN - 2583-2344.

**ABSTRACT**

The advancements in an easily integrated method of automated banking have helped improve the customer experience while also becoming a threat to online banking fraud. This paper explores the Indian legal provisions to curb banking fraud, especially in the online platform, and the current developments, deficits, and recommendations. The legal framework comprises critical legislation, laws such as the Information Technology Act, 2000, and Bharatiya Nyaya Sanhita, 2023, along with the guidelines from the Reserve Bank of India (RBI). Nevertheless, some small steps have been made to fill in the gaps, though many of the advanced online fraud schemes are still unmet by legislative changes and tightening regulations. A comparative analysis of what applies in the US and the UK highlights gaps showing the lack of sufficient laws to address digital financial crimes together with roles for the regulatory authorities that are more proactive. Some of the factors that exert immense pressure on enforcement include jurisdictional problems, prosecutor problems, and the dynamic nature of fraud. To strengthen the procedure with measures against fraud, the paper provides recommendations: improving current legislation, developing international cooperation, and including such innovations as artificial intelligence, biometric identification, and blockchain. Equally important is training law enforcement agencies on the nature of cybercrime and awareness creation. Synergizing the legal and regulatory perspective with technological solutions for combating online banking fraud would go a long way toward the realization of a secure and more resilient financial system in India.

**Keywords:** Online banking fraud, Cybersecurity regulations, Artificial intelligence, fraud prevention

## INTRODUCTION

Technological enhancement has transformation the process of banking making it easier and faster but at the same time increasing risk such as online fraud. In India and across the world, people are falling prey to online banking frauds raising the issue of the effectiveness of present law to deal with such cases. Despite strict measures adopted by banks in India including the use of chip-based cards and bio metrics the instances of on-line banking frauds include fraudulent and unauthorized use of the personal or financial data legally procured by the fraudster culminating into erosion of customer confidence and reputation loss of banks besides national security being under threat from criminals who have access to such data. [480]

In India anti-fraud structures involve elements of the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, RBI regulation and judicial precedents. But these are commonly out-of-date in terms of approaching such hi-tech fraud modalities as phishing and identity theft. There is a need for legislative improvements in minutes with reference not only to the issue of fraud but also justice and

[480] Arvind Kumar Gupta, *Serious Fraud Investigation Office (Law & Practice)* 100 (Bharat Law House, New Delhi, 1st edn., 2021).

indemnified recovery for the victims concerned. This paper assesses the efficacy of current laws and compares them to global standards, then proposes adjustments to enhance Indian laws against cyber fraud. [481]

Research questions include: an analysis of the RBI's regulatory involvement and other financial authorities in addressing fraud, discussion of enforcement issues, the role of digital forensic and worldwide collaboration on the fight against international frauds. Key questions include: the implementation of present-day legal instruments, judges' impact, and the function of reference models in the development of an efficient anti-fraud system. To that end, the paper will make policy recommendations at the end of this analysis that will enhance the security of the digital banking systems in India.

## UNDERSTANDING BANKING FRAUD: CONCEPT AND TYPES

Fraud particularly affects the banking sector, and its cases are frequent and, on the increase, due to the growing trend in banking. Internet banking, mobile banking applications, and other digital payment services are popular and efficient means of enhancing financial transactions, and at the same time, they have become additional risks for different types of fraud to customers and financial institutions. Banking fraud is defined as deceitful actions that lead to personal and/or organizational losses or both, performed by an individual or a group of people. One of the challenges of banking fraud is breaking down as the criminals learn new methods of operation while looking for new ways to engage in unlawful business. Therefore, the following data on the concept of banking frauds and their classification will be of great importance when writing this paper since it analyses different dimensions of banking frauds to establish effective legal measures that can effectively combat these vices.

### Defining Banking Fraud

Tracing from the legal and financial point of view, banking fraud means any action containing deceit, misrepresentation, or violation of regulation laws that will give financial gains or profit to the fraudster and loss to the victims, be it an individual, corporate body, or banking institution. As per "Section 318 of the Bharatiya Nyaya Sanhita, 2023" (BNS), banking fraud normally means doing anything dishonest to dishonestly induce any person under the will of the accused to deliver any property or money, knowing that he is using a stolen or false ID or skilled false documents to perform unlawful banking operations. [482] Banking fraud includes general forms of fraud such as credit card fraud, loan fraud, and money fraud, and the most recent forms of fraud include phishing, ransomware attacks, and identity fraud. This deceit is mostly to influence the banking systems or certain accounts with a view of altering the process to dismantle the funds illicitly, which raises high perils about monetary security and personal safety.

Conventional banking fraud is somehow a thing of the past whereby banking fraud was characterized by forgery of checks, embezzlement, etc. Nowadays, banking fraud is more inclined to higher technology systems. The availability of Internet connections and the diversity of the usage of electronic materials make the rate of cybercriminals rise, especially the cases of Internet banking fraud. These types of fraud challenge the credibility of the banking industry and impose severe economic costs, as evidenced by the fact that banking fraud worldwide costs billions of dollars every year. Thus, profiling banking fraud also necessitates recognition of the different types it, especially due to the interaction between the offline and online types with the growth of the software and technology industry.

[481] B. R. Sharma, *Bank Frauds: Prevention and Detection* 250 (Lexis Nexis, Gurgaon, 4th edn., 2016).

[482] C. K. Takwani, *Indian Penal Code (IPC)* 376 (Eastern Book Company, Lucknow, 2nd edn., 2022).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 4 AND ISSUE 4 OF 2024
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

**Classification of Banking Fraud**

Banking fraud can be broadly classified into two categories: offline fraud and online fraud. Both types pose different difficulties for police and banks because they use different approaches and are based on different shortcomings of the banking security system. Whereas conventional fraud forgeries may involve the use of hardcopy documents, checks, or cash flow statements, online fraud harnesses technology to conduct its stock-in-trade business frauds through computers and the internet and could cross international boundaries. Type C: The classification is useful in formulating specific legal and regulatory solutions to tackling each of them because there may be differences in online and offline prevention and detection mechanisms. [483]

***Offline Fraud: Traditional Methods***

The other type of fraud is offline fraud, whereby the fraudster indulges in the vice and does not use any form of technology in the traditional banking systems. Examples of offenses that WWW fraud is similar to include check fraud, in which fake or modified checks are used to withdraw cash, which is similar to loan fraud, in which false representation of financial data is used to secure an illegitimate loan, and embezzlement, whereby employees who are entrusted with the responsibility of handling funds misappropriate them. Offline frauds can normally be forced and prosecuted more effectively compared with their online counterparts because of the availability of tangible evidence as well as the less possibility of jurisdictional confusion. However, they still present considerable problems, especially in the regions where digital banking facilities are not so popular and the traditional features of banking services are widely used. Legal tools concerning offline fraud regulations mostly rely on the provisions of the 'Bharatiya Nyaya Sanhita, 2023' under the headings of cheating, forgery, and betrayal of trust.

***Online Fraud: Emerging Risks in Digital Banking***

The major threat of the current banking environment is online fraud since there is an emphasis on online banking as well as the improvement in the methods used by hackers. While traditional fraud is characterized by individuals having physical access to the banking systems either to steal or to forge other individuals, online fraud is mainly committed through the use of technological gadgets to subjugate the banking systems. They include attempting to acquire sensitive information through emails or messages usually faked or fake, getting access to banking systems or accounts, impersonation to perform transactions using the stolen identity, and the use of viruses or other malignant codes to capture confidential data or authority of the banking systems. An interesting disassembling factor of law when dealing with cases related to online fraud includes the fact that the offenders normally reside in different regions, thus posing a huge challenge when it comes to the sharing of duties and responsibilities when apprehending offenders.

In India, specific laws that help in tackling the problem of online banking fraud include the "Information Technology Act, of 2000," because it contains provisions on cyber security, digital signatures, and data protection. 'Section 66C" of the IT Act has opted for identity theft, while "Section 66D" has addressed the punishment for cheating by impersonation by using computer resources. Also, specific authorities like the Reserve Bank of India have provided some rules to follow for cybersecurity in banks, relationships with the customer, awareness camps, and reporting of fraud. However, cases of online banking fraud are on the increase, and this indicates that the legal framework for combating such frauds needs to be updated frequently because, with advancing technology and techniques used by fraudsters, laws also

[483] Kant Mani, *Electronic Banking Frauds [ATM, Mobile Banking and Internet Banking]* 150 (Lawmann, Mumbai, 1st edn., 2022).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 4 AND ISSUE 4 OF 2024
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

need to be dynamic. [484]

## LEGAL FRAMEWORK FOR CONTROLLING BANKING FRAUD IN INDIA

The banking fraud regulatory regime of India is comprised of several statutes, regulatory directions, and cybersecurity measures that exist to ultimately thwart fraudulent activities, particularly in the realm of banking and digital transactions. The legal mechanisms are envisaged to contemplate different species of banking fraud, whether traditional, which includes forgery and embezzlement, or modern forms of fraud in the form of phishing, identity theft, as well as the use of malware, among others. In addition to setting out the criminal consequences for offenders, these frameworks also have civil law remedies to compensate banking fraud victims, alongside measures for industry supervision of risk control, thereby ensuring that fraudsters are deterred and financial institutions operate under accountable standards of risk management. To a significant extent, the efficiency of these mechanisms is due to the combination of legislative actions with regulatory standards and cyber security models that may work in the constantly changing environment of digital banking. Due to the increasing cases of online banking fraud, there is a need for continuous improvement of these legal frameworks to effectively address emerging risks and challenges.[485]

### Key Legislation Addressing Banking Fraud

The act at the forefront of regulating banking fraud in India is the "Information Technology Act, of 2000," and the second is the "Bharatiya Nyaya Sanhita, 2023" (BNS). These laws serve to give a legal framework to different kinds of fraud, state the punishment for criminal activities, and define the roles and duties of different participants in providing security and reliability of financial operations. Measures provided in these laws are intended to prevent crime by enhancing penalties for fraud and prescribing methods for investigating and prosecuting fraudulent crimes. Moreover, there is acceptance of provisions under other laws like the 'Prevention of Money Laundering Act 2002' which also has a relationship with restricting banking fraudulence-related offenses related to money fraudulence.

#### *"Information Technology Act, 2000": Provisions Related to Online Fraud*

The core legislation in India is the Information Technology Act, of 2000, as amended by the Information Technology Amendment Act, of 2008, regarding cybercrime. The Act was passed mainly for the purpose of giving legal effect to electronic transactions and digital signatures, but it also encompasses legal measures against cybercrime. For identity theft, the IT Act has "Section 66 C," and Section 66 C covers the use of identification of others with intent to cause fraud. Similarly, "Section 66D" deals with the provision for punishment for cheating by impersonation using computer resources and hence occupies a very important status in combating online banking frauds. Sections relating to hacking, unauthorized access to computers and computer systems, and data theft as contained under the Act come with banking fraud-related cases. New provisions amended in the Act, particularly after the IT Amendment Act, of 2008, have empowered legal action against more cyber offenses, increasing the strength of legal actions against online fraudsters.

#### *Bharatiya Nyaya Sanhita, 2023 (BNS): Sections Dealing with Financial Fraud*

The Bharatiya Nyaya Sanhita, 2023, also works hand in hand with the provisions of the IT Act for covering financial fraud under cheating, forgery, criminal breach of trust, and many other related unfair acts. For example, now and again, "Section 318—Cheating and dishonestly inducing delivery of property; property includes money" of the BNS is used in banking fraud

[484] Shikher Deep Aggarwal and Kush Kalra, *Commentary on the Information Technology Act* 600 (Whitesmann, New Delhi, 2nd edn., 2024).
[485] Tauseef Ahmad, "Law and Policy Relating to Bank Fraud and its Prevention and Control", 2(3) *International Journal of Law Management & Humanities 1* (2020).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 4 AND ISSUE 4 OF 2024
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

cases. This section gives room for imprisonment and fines for any person convicted of fraudulent dealings with individuals and institutions. Likewise, "Section 316" deals with the aspect of forgery for cheating, and this would apply to fraudulent loan applications, forged documents, or fake bank accounts. Moreover, "Section 316" is the criminal breach of trust by a public servant or banker; common in situations when employees or officers take advantage of their positions to cheat. The elements provided by BNS provide traditional legal structures that, when applied coupled with the IT Act, play an integral part in the prosecution of banking fraud in India. [486]

**Regulatory Guidelines and Mechanisms**

Besides the mere statutes and regulations, there are also special regulatory organizations, including the Reserve Bank of India (RBI), which sets up some of the bureaucratic measures for controlling the occurrences and prevention of banking fraud. These guidelines are meant to implement a preventive strategy in dealing with the risk aspects around the financial sector; particularly for the banks, there are directions for instigating adequate security measures as a way of detecting fraud. Regulations also contain provisions for the customers to seek remedy should they have been abused by the fraudsters.

***Reserve Bank of India (RBI) Guidelines on Fraud Risk Management***

The RBI has time and again come out with such circulars and guidelines to address the factors concerning the risk management of frauds, the improved mechanism and reporting of these frauds, and the liabilities of the banks involved in such frauds. They stress that a firm's operations must have sound internal control procedures, audit outstanding, and employee education on ways of identifying fraud risks. For example, 'Master Directions on Frauds: Classification and Reporting by Commercial Banks and Select FIs', specified the format for identification and reporting of frauds and the schedule for reporting to the RBI. Other guidelines contained in this piece include fraud monitoring committees, oversight roles of audit committees, and preventive measures, including the use of real-time fraud detection software. When it comes to cyber fraud, the RBI expects the banks to implement several protective measures comprising encryption, authentication, and keeping track of strange activities of customers for a higher level of security for the customers. [487]

***Banking Ombudsman Scheme: Addressing Customer Grievances***

The banking ombudsman scheme, framed under the "Banking Regulation Act, of 1949," is a process according to which customers of any bank having a grievance against the bank about any banking service, which includes fraud and unauthorized transactions, can approach the Ombudsman. It enlightens customers on how to complain about issues like delays in refunding unauthorized debits, non-compliance with the laid-down regulatory code of conduct in reversing wrongful transactions, and other cases of cheating the customers. The Ombudsman has some powers to pass an award or order the bank to compensate the complainant where the bank is at fault. This scheme can be taken advantage of by customers as an easy and swift means to seek justice when they feel that the bank has wronged them in some way and as a mechanism that forces banks to exercise accountability.

**Cybersecurity Regulations and Online Fraud Prevention Measures**

This report concluded that cybersecurity regulation is a critical component of the legal regimes for containing banking fraud, especially

[486] Kalpna, "Banking Frauds in India", *available at:* https://iledu.in/banking-frauds-in-india/ (last visited on October 15, 2024).

[487] Vaneeta Patnaik, SocioEconomic Offences: Nature and Dimensions - Bank Fraud: Types and Prevention, *available at:* https://epgp.inflibnet.ac.in/epgpdata/uploads/epgp_content/S001608/P001741/M022095/ET/1504180707BankfraudFormat.pdf (last visited on October 15, 2024).

given the rising trends in cybercrimes in the banking sector. The Indian policy called the "National Cyber Security Policy" outlines measures necessary for the protection of the digital environment, including financial systems. It has formed this policy on the strength of a strong cybersecurity architecture in managing the risks of online banking fraud. It helps financial institutions enforce strong cybersecurity measures for people, assess risks at least twice a year, and get threat intelligence from governmental organizations.

The Indian Computer Emergency Response Team," better known as "CERT-In," which falls under the "Ministry of Electronics and Information Technology," is the nodal body for the purpose. ACFO actively participates in the early identification of prospective threats and communicates alerts to financial organizations regarding potential cyber hazards. CERT-In also deals with international agencies for protection against cross-border security threats, which plays a very vital role in controlling and preventing banking fraud happening globally. In ways that include issuing guidelines on reporting of incidents and conducting mock cyber security incidents, CERT-In plays its part in enhancing the defense of banking systems against fraud and hence a secure financial system.

## COMPARATIVE ANALYSIS: INTERNATIONAL LEGAL FRAMEWORKS FOR CONTROLLING BANKING FRAUD

This report concluded that cybersecurity regulation is a critical component of the legal regimes for containing banking fraud, especially given the rising trends in cybercrimes in the banking sector. The Indian policy called the "National Cyber Security Policy" outlines measures necessary for the protection of the digital environment, including financial systems. It has formed this policy on the strength of a strong cybersecurity architecture in managing the risks of online banking fraud. It helps financial institutions enforce strong cybersecurity measures for people, assess risks at least twice a year, and get threat intelligence from governmental organizations. [488]

The Indian Computer Emergency Response Team," better known as "CERT-In," which falls under the "Ministry of Electronics and Information Technology," is the nodal body for the purpose. ACFO actively participates in the early identification of prospective threats and communicates alerts to financial organizations regarding potential cyber hazards. CERT-In also deals with international agencies for protection against cross-border security threats, which plays a very vital role in controlling and preventing banking fraud happening globally. In ways that include issuing guidelines on reporting of incidents and conducting mock cyber security incidents, CERT-In plays its part in enhancing the defense of banking systems against fraud and hence a secure financial system.

### Legal Framework in the USA

Due to the sovereign system of the United States, the legal regulation of banking fraud uses both federal and state legislation as an interdependent system. The country has put in place very strong legal measures that give protection to not only conventional banking scams but also subsequent risks resulting from electronic transactions. This strong legal framework is backed up by the participation of various financial authorities, including the Federal Reserve, the OCC, and the FTC, who frequently oversee compliance and share the set standards across the financial industry. As with most crimes, the USA also has a pretty vigorous law enforcement-financial institution partnership, with the latter empowering the former to be more proactive when it comes to banking fraud threats that are on the radar.

#### *Federal Laws: "Computer Fraud and Abuse Act"*

The CFAA passed in 1986 is a central piece of

[488] Zubair Ahmed Khan, "Fraudulent Practices in Banking Institutions: Legal Issues and Challenges", 3 *Amity International Journal of Juridical Sciences* 15 (2017).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 4 AND ISSUE 4 OF 2024
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

federal legislation regulating computer crime, another form of cybercrime, including internet banking fraud. The Act makes hacking, identity theft, and other fraudulent activities targeting computers and/or computer networks operating in financial institutions a criminal offense. According to the CFAA, anyone convicted or engaging in the Computer Fraud and Abuse Act, including but not limited to accessing a computer without authorization or appropriate access, intentionally accessing another person's computer, financial data using falsified pretences, or resulting in computer files transferring viruses, is liable to legal consequences involving imprisonment or fines. The Act covers both domestic and international offenders, meaning the U.S. government has the mandate to sue anyone who conducts banking fraud from another country. The CFAA has been modified to accommodate emerging cyber threats with time and, as such, has flexible laws in response to increasing advancements in technology. [489]

***Role of Regulatory Bodies Like the Federal Reserve***

The Federal Reserve has major responsibilities for both supervising and monitoring the banking system of the USA, with special attention paid to the establishment of proper risk management measures to fight fraud. Banks use it to identify fraud risks and protect their systems from aggressors, and it offers acceptable standards on cybersecurity, transaction monitoring, and customer due diligence. The Federal Reserve also makes examinations of banks' internal control and anti-fraud precautions concerning federal rules frequently. In addition, federal banks also work hand in hand with other government agencies, including the Financial Crimes Enforcement Network (FinCEN), through which the Federal Reserve can exchange information on suspicious activity and contribute to the fight against cases of banking fraud. Due to a stringent regulatory structure that is sustained by the Federal Reserve, financial institutions end up in a better position to shield their clients and themselves from potential cyber fraud.

**Legal Mechanisms in the UK**

The mechanisms for regulating banking fraud in the United Kingdom are based on statutory instruments, regulatory standards, and the current trends that prevent banking fraud in Britain altogether. Due to the growing use of online transactions, the legal structure in the UK has changed over the recent past, and specific laws have been enacted to fight this vice. Concerning the prevention of financial fraud, the following are the laws of the United Kingdom: The Fraud Act of 2006 states offenses connected with fraudulent deeds and penalties for those who commit these offenses. The sound legal environment is backed up by the involvement of the Financial Conduct Authority, which controls the actions of financial companies as well as promotes adherence to the norms regarding fraud prevention. As with the rest of the globalized world, the UK also coordinates its efforts with other countries in combating banking fraud. [490]

***"Fraud Act, 2006"***

The "Fraud Act 2006" is another important legal instrument in the system of legal regulation of the fight against financial fraud in the United Kingdom, including Internet banking fraud. Fraud, according to the Act, covers crimes that are expressed through misrepresentation, non-disclosure, and abuse of position. It gives the legal ground to prosecute persons who use falsity to benefit or to put another person in a position of financial disadvantage. These legislations include the provisions of the Act averting phishing scams, identity theft, and unauthorized access to banking systems, among others; hence, the Act provides a plethora of legal provisions to counter online

[489] Banking Fraud - Its Detection, Prevention, and Reporting, *available at:* https://www.icsi.edu/media/webmodules/02122021_BANKING_FRAUD_ITS_DETECTION,_PREVENTION_AND_REPORTING.pdf (last visited on October 15, 2024).

[490] Charan Singh, Frauds in the Indian Banking Industry (Working Paper No. 505), *available at:* https://www.iimb. ac.in/sites/default/files/2018-07/WP_No._505.pdf (last visited on October 15, 2024).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 4 AND ISSUE 4 OF 2024
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

frauds. Sanctions under the Fraud Act are imprisonment for a maximum term of 10 years, a fine, or both according to the nature of the offense. Through outlawing various forms of fraudulent conduct, the Act can be said to act as a reformation to the likely offenders and also a method of checking those who engage in the act.

### *Role of the Financial Conduct Authority (FCA) in Combating Online Fraud*

FCA is a conduct authority that focuses on the retail financial markets in the United Kingdom to deliver for consumers and market integrity outcomes. The FCA plays a role in implementing measures to fight fraud by providing firms with guidelines on how to effectively prevent it, supervising firms to ensure compliance with AML regulations, and... conducting investigations for suspected incidents of fraud within the financial market. Another point the FCA also focuses on is that of customer awareness, urging citizens to buckle down and protect themselves from online fraud and phishing. The FCA has tried to enhance its approach to tackling cyber fraud in recent years through data analysis and technology to identify tastes in financial practices. Such cooperation with the law enforcement departments, as well as the international counterparts, strengthens the performance of the regulatory body in consideration of cross-border fraud cases, given the integration of the global financial systems.

## CHALLENGES IN THE LEGAL MECHANISMS FOR CONTROLLING ONLINE FRAUD

However, existing legal and regulatory frameworks for countering banking fraud seem to bear notable challenges in how to control online fraud. One realizes that due to the dynamic technological advancement, the laws have not been able to enforce necessary laws to fill those gaps. The current laws sometimes fail to capture the complexities of internet crimes because the criminals employ technicalities to commit the crimes and avoid getting arrested. Moreover, the contractual nature of many online fraud cases makes questions of jurisdictions and legal enforcement about the international aspects of cybercrime ambiguous. Fraudulent activities are hence a dominant that the legal mechanisms must be evolved and fine-tuned to face to ensure effective handling and prevention. This paper continues below to review the fundamental challenges in the present legal framework related to combating online banking fraud, which includes the absence of modern legal codes, multiple jurisdictions, issues in prosecuting the offense, and the influence of technology on fraud fighting. [491]

### Gaps in the Existing Legal Framework

The legal regulation of banking fraud in India is based on the following legal acts: the "Information Technology Act 2000" and the Bharatiya Nyaya Sanhita, 2023. However, these laws do allow significant loopholes and restrictions, which prevent them from being effectively utilized to fight the issue of online fraud. Even though the introduction of the IT Act was a move in the right direction, its provisions have still not been reviewed year after year to meet the challenges posed by cyber fraudsters. The BNS was developed a long time before the coming of the Internet; hence, it has some provisions that may lack the modern structure to deal with today's financial crimes. These gaps show that legal regulation of digital banking risks requires legislative improvements to provide the necessary coverage and timely response to new threats.

### *Outdated Provisions in Traditional Laws*

The Bharatiya Nyaya Sanhita, 2023 continues to be a main statute that deals with criminal offenses in India, such as fraud. Though its provisions are relatively generic and are more applicable to some of the traditional forms of fraud, such as forgery and embezzlement, these

[491] Fraud Prevention – Challenges, Strategies, Best Practices, and Technologies, *available at:* https://shuftipro.com/blog/fraud-prevention-challenges-strategies-best-practices-and-technologies/ (last visited on October 15, 2024).

do not exactly capture the peculiar modus operandi associated with online banking fraud. For example, "Section 318" of the BNS addresses cheating and dishonestly inducing delivery of property; however, it does not directly address the various forms of digital fraud such as phishing attacks, ransomware, or identity theft through the use of technologies. This explains why the language and scope of the BNS require an amendment to suit current realities in a bid to ensure that they can be applied to prosecute offenses related to online fraud. Besides, some of the penalties provided for under the BNS can be rather insignificant in the context of cybercrime, many of which involve monetary losses. [492]

***Inadequate Cybercrime Laws Specific to Online Fraud***

Although entering cyberspace is still relatively recent, while the Information Technology Act, of 2000, has some connection with cyberspace crimes such as cyber offenses, identity theft, and hacking, there are no sections that are exclusively related to different kinds of online banking frauds. The Act contains sections like "Section 66C" (identity theft) and "Section 66D" (cheating by impersonation using a computer resource), but these do not adequately provide for modern and complex digital frauding strategies such as social engineering, SIM swapping, or multi-levelled financial fraud. Moreover, the penalties provided under the IT Act may not be setting the correct tone as far as some of the large-scale online banking frauds happening where losses running into crores of rupees are involved. As techniques used by fraudsters in the cyber domain become sophisticated, it becomes necessary to enlarge specific legal measures relating to some of these specialized modalities of cyber fraud with better facilities for the recovery of the embezzled funds and indemnification of victims. [493]

**Jurisdictional Issues and Cross-Border Fraud**

Cybercrimes, especially those involving online banking, involve one or more jurisdictions, thus raising jurisdictional issues that complicate the law in handling such crimes. Most of the time, the culprits in online fraud orchestrate their activities from other countries; hence, it is very hard for police to apprehend or prosecute the criminals. Add to the fact that each country has its legal system, data protection laws, and cybercrime laws, which add to the problem. For instance, some states may lack sufficient legislation to deal with Internet banking fraud or may fail to apprehend offenders due to international cooperation, and therefore fraudsters can easily exploit these legal zones.

The factors associated with the difficulties of managing international online fraud cases are also related to the obtainment of digital evidence across borders, and often in another country, it is necessary to follow the international treaty and MLA. An accumulation of traces, like financial transactions, IP addresses, or messages, may be cumbersome and formal, and this delays the prosecution of offenders. Moreover, issues of data protection in civil and criminal proceedings, as well as legal requirements for admitting electronic evidence, become crucial factors that may hinder the possibility of effectively investigating and prosecuting cross-border fraud cases. India has to thus ramp up its international cooperation diplomacy, engage in bilateral treaties, and be part of global trends such as the Budapest Convention on Cybercrime to enhance its capabilities to tackle cyber fraud across borders.

**Difficulties in Prosecution and Conviction**

Another major real-life problem that we face while trying to curb online banking fraud involves the legal procedures that are required before one can be prosecuted and then

[492] Cybersecurity Laws and Regulations Report 2024 - India, *available at:* https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/india (last visited on October 15, 2024).

[493] Amitabh Srivastava, Pradip R. Sagar, and Manisha Saroop, "Online fraud: A raging menace" *India Today,* January 4, 2024.

convicted, which is not easy since much of the evidence that is involved is in the digital format. Thus, in contrast to conventional crime, where tangible clues may be easily obtained, cyber fraud operates with electronic spores that can be easily camouflaged or erased by criminals. Due to the fleeting nature of digital evidence, together with the sophistication involved in capturing and analysing the information that is found in digital equipment, it proves very hard for law enforcement teams to pile up sufficient evidence in a bid to prosecute offenders. Meanwhile, the laws stipulating the relevancy of mobile data may also differ and may be attained with adherence to rigorous processes of data harvesting, storage, and identification.

For instance, in the case of *Shafhi Mohammad v. State of Himachal Pradesh*[494], the Supreme Court of India has recognized the difficulties that accompany electronic evidence and accentuated the question of developing new standards of judicial decision-making due to changes in information technologies. However, the legal system does not have much knowledge about digital forensics, and there is no standard procedure for dealing with cybercrime cases, which is why there are many delays and a lower number of successful cases. There is also the absence of cybercrime courts and trained judicial officers since it can be quite technical and challenging to unravel involving internet fraud cases involving technical, digital skills, and related financial laws. Consequently, there is a need to build the capacity of law enforcement and the judiciary to increase the rate of prosecuting fraud cases that are committed through the Internet.

### Impact of Technological Advancements on Fraud Prevention

The issue of technology is both a strength and a weakness in combating fraud in the online banking business. On one hand, the current advancements in cybersecurity include the use of multi-factor authentication, biometric verification, and artificial intelligence in detecting fraudulent transactions, which have enhanced the capacity of financial institutions to prevent fraudulent transactions. At the same time, fraudsters do not stay idle; they adapt to use new technologies to come up with better ways of dodging security measures, including using deep fake technology to steal identities or using artificial intelligence to enhance the automation of phishing. Technological advancement is done at such a fast rate that it becomes difficult to set adequate legislation and standards and also to arrest any emerging legal gap. Therefore, while there is profound help of technology in combating fraud, the phenomenon also becomes proof of the constant need to approach legal methods to innovate and stay effective.[495]

### TECHNOLOGICAL SOLUTIONS TO COMBAT ONLINE BANKING FRAUD

The fight against online banking fraud has become partially dependent on technology to identify, counter, and reduce fraudulent activities. While fraud is becoming increasingly technological as the offenders employ very tactical means of exploiting the weaknesses of online platforms, the legal approaches to addressing some of these emergent threats may be very limited. Therefore, technological applications are adopted to enhance the current legal framework and create a more effective barrier. AI, ML, biometric authentication, MFA, and blockchain have come in handy when it comes to preventing fraud in online banking. Besides proactive detection and prevention of fraud, these technologies play a great role in the collection of digital evidence to aid in legal actions against the perpetrators. The synergy of elements of the law and high technology provides a better basis for countering fraudulent activity in Internet banking and creating secure conditions for monetary

[494] (2018) 2 SCC 801.

[495] Arushi Mehta, "Impact of technological advancements on banking frauds: A case study of Indian banks", 7 *International Journal of Research in Finance and Management* 261 (2024).

operations. [496]

**Role of Artificial Intelligence and Machine Learning**

Both AI and ML enable organizations that offer online banking services to identify fraud by analysing big data for such signs and patterns. AI algorithms are also capable of tracking real-time financial transactions and alerting customers to any abnormal transaction, which may be due to spending habits, account activity, etc. They can use that predictive capability to identify future ventures that have a higher risk of fraud and prevent those frauds before they happen, thus reducing the risk probability of experiencing financial losses. For example, one of the ML algorithms can be applied to transaction history, specializing in identifying fraudulent transactions and enhancing this recognition based on new data. Such systems are also capable of evolving with new fraud strategies because the models can be modified to incorporate new trends, such as new fraud patterns and styles.

Additionally, fraud detection and prevention systems that use AI can use NLP to screen communications in an attempt to detect a phishing attempt or social engineering. For instance, those chatbots that are used in customer service can be designed with AI algorithms that can quickly identify any kind of ferocious activity, such as an attempt to attain fraudulent information. The adoption of both AI and ML has been supported in the legal field by referring to technological tools in the identification of cyber threats. In On this principle, the Supreme Court in *"Bennett Coleman & Co. Ltd. v. Union of India"*[497] recognized the dynamic concept of technology and the subject's relevance as a basis for determining reactive responses to contemporary risks like Internet mediatory fraud. Leaving aside AI and ML, the financial sector has the opportunity to advance its legal regulations by using novel technologies to effectively fight online fraud.

**Biometric Authentication and Multi-Factor Authentication**

The use of biometric authentication and multi-factor authentication (MFA) has become crucial features when it comes to protecting such transactions and preventing individuals from unauthorized access to their banking accounts. Usability A: Biometric methods like finger scans, face recognition, and iris scans are more secure than the use of passwords or pins because biometric facts are original and hard to imitate. Since biometrics is adopted in digital banking, customers are less likely to fall prey to fraudsters through identity theft and account takeover frauds. For example, incorporating an application of face recognition in mobile banking applications guarantees only the owner of the face shall access his or her account rather than an imposter.

Double-layer security is attained via multi-factor authentication; this calls for identity confirmation through something you know, something you have, and something you are. Need gleaning from diverse regulatory recommendations, wherein MFA has been underlined as a legal pass by RBI, which requires two-factor authentication for some online transactions to protect the consumers. The need for multiple-factor authentication also fits with international standards, as evidenced by the requirements like the Payment Services Directive (PSD2) of the European Union market that require strong customer authentication. In this case, legal requirements for the use of biometrics and multi-factor authentication can greatly improve the security of online banking since the incidence of online fraud can be easily minimized. [498]

[496] Aman Mishra, "Leveraging technological solutions to prevent financial fraud", *available at:* https://www.expresscomputer.in/guest-blogs/leveraging-technological-solutions-to-prevent-financial-fraud/114635/ (last visited on October 15, 2024).
[497] (1973) 2 SCC 788.
[498] Biometric Verification: How to Use It for Fraud Prevention, *available at:* https://www.unit21.ai/fraud-aml-dictionary/biometric-verification (last visited on October 15, 2024).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 4 AND ISSUE 4 OF 2024

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

**Blockchain Technology in Fraud Prevention**

The adoption of blockchain technology provides a unique solution for increasing transparency and minimizing the probability of fraud in the online banking system. Through decentralization and the integration of an unalterable database, blockchain minimizes the likelihood that anyone will attempt to misrepresent financial data fraudulently. In terms of its fundamental architecture, every block on a blockchain contains details of the transactions it has confirmed, including an encrypted version of the previous block, making it more or less impossible for scammers to hack or manufacture fake transaction records. Also, because blockchain is distributed in nature, it thus can be difficult for hackers to affect a wholesale cyber-attack on banking systems. GraphQL can enhance online banking applications by using legal frameworks to incorporate blockchain for transactions like cross-border payments, smart contracts, and an effective solution for identity management.[499]

**CONCLUSION**

The examination of the current legal factors employed in mitigating banking fraud, especially internet fraud, reveals the fact that there is a need to have an appropriate legal model to meet the ever-changing nature of internet fraud. While the change from offline to online banking has brought added convenience and enjoyment for cultural users, it has also brought added risk in the cybercrime sector. This paper regards the current legal framework for counteracting banking fraud in India as a combination of legal provisions, regulatory directives, and case law. Still, the current solutions leave many important areas unchecked where advanced methods of online scams are still prevalent. The present-day Indian laws have basic legislative instruments in the form of the "Information Technology Act, 2000" and the "Bharatiya Nyaya Sanhita, 2023" Still, there is a continuous need for revisions as per the changing knowledge and innovations, but rapid developments in technology and trends of fraud are rolling much faster than the speed of legal amendments.

By comparing the legal frameworks of the USA and the UK, this writer has understood that a far more essentialist approach should be employed with operational legal frameworks as well as active and sustained regulatory supervision. Cybercrime laws directly regarding digital financial frauds and activities of the regulatory authorities, such as the RBI, are other yet essential aspects of the stronger anti-fraud combat. Another factor is that there are obstacles to investigation that are jurisdictional or concerning difficulties of prosecution, which show that there is a need for strengthening cooperation and capacity building between the competent law enforcement authorities from different countries. Since fraudsters mainly conduct their activities on different continents, effective cooperation with countries through treaties and data-sharing initiatives, as well as conventions along with increased collaboration within international organizations, will be quite helpful for India in fighting cross-border online fraud.

AI, machine learning, biometric authentication, and blockchain offer important tools to support the systems already in place by offering supplementary security and means of monitoring fraud. The use of these technologies in synergy with legal requirements helps not only improve the fight against fraud but also enhance the collection of electronic evidence for use in prosecution cases. In the same manner, legal changes should encourage financial institutions to embrace good security measures endorsed by certified cybersecurity experts to protect their clients' transactions.

To overcome the current weaknesses, it is suggested to extend existing legislation to new fraud types, increase international cooperation,

[499] The Importance of Blockchain Technology in Fraud Prevention: How Does Blockchain Prevent Fraud?, *available at*: https://www.formica.ai/blog/the-importance-of-blockchain-technology-in-fraud-prevention-how-does-blockchain-prevent-fraud (last visited on October 15, 2024).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 4 AND ISSUE 4 OF 2024

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

and organize training for officers involved in combating fraud. The problem of combating banking fraud today requires the coordinated use of legal provisions, supervision, technical safeguards, and cooperation with foreign partners. India needs to extend its legal and regulatory measures so that there is a sound foundation for a safe and robust financial system that can put up with the threat coming from online banking fraud.