GROWTH OF 'AI' IN FINANCIAL FRAUDS: ANALYSING CUSTOMERS, BANKS AND PLATFORMS' LIABILITY & EFFECTIVENESS OF CURRENT LEGISLATIONS

Khushi, BA.LL.B. (Hons.), Quantum University, Roorkee

ABSTRACT

Artificial Intelligence (AI) has triggered a paradigm shift in the digital financial ecosystem, revolutionizing financial services while simultaneously creating unprecedented opportunities for fraud. This paper looks at the development of AI-driven financial fraud, from traditional cyber-enabled scams to more advanced tactics like deepfake impersonation, voice cloning, intelligent phishing, and synthetic identity fraud. It examines how AI has increased the scale, credibility, and complexity of fraudulent activities, creating significant challenges for financial security and consumer protection.

A key focus of this study is the changing responsibility among customers, banks, and digital platforms. It evaluates bank responsibility for unauthorized transactions, the rising expectation for customer vigilance, and the new roles of intermediaries that manage digital payments. The paper highlights the legal ambiguities surrounding liability distribution and their effects on consumer rights and dispute resolution.

Further, the research assesses the adequacy of existing legal and regulatory frameworks in addressing AI-enabled financial frauds. It highlights important gaps in laws meant for traditional misconduct. The paper calls for a new liability framework and specific legal changes to tackle the unique challenges posed by autonomous and AI-assisted fraud, ensuring accountability, financial strength, and better consumer protection in the digital era.

Keywords: Artificial Intelligence, Financial Frauds, Liability, Cybersecurity, Deepfakes.

I. INTRODUCTION

A. BACKGROUND

In February 2024, a finance worker at a multinational firm's Hong Kong office transferred USD 25 million to fraudsters after attending what happened to be a routine video conference call with the company's Chief Financial Officer and several colleagues. The catch? Every person on that call, except the victim, was an AI-generated deepfake. It is reportedly one of the largest deepfake financial fraud cases recorded to date and it signals a fundamental shift in the landscape of financial crimes.[1]

As India is rapidly digitizing its economy and positions itself as a global technology hub, over the time, AI has emerged as both a transformative tool and a sophisticated weapon in the hands of financial criminals. From voice cloning scams to tricking corporate entities into authorizing fraudulent transfers to AI-generated fake identities that slip even highly sophisticated verification systems to tackle such instances, leading to growing use of artificial intelligence in financial fraud is creating new and serious challenges at both domestic and global level of business along with regulators and law enforcement agencies.[2]

Traditionally, banking financial fraud was restricted to manual acts such as cheque forgery, document exploitation and internal malpractices. With the emergence of digital banking, fraud has gradually shifted towards online platforms, turning into phishing, deepfake impersonation, identity thefts and voice cloning. According to the Reserve Bank of India (RBI), digital payment frauds account for the highest number of fraud cases in the banking sector, particularly in internet-based transactions.[3] The evolution of Artificial Intelligence (AI) has further transformed this landscape. On one side, AI has facilitated banks to strengthen fraud detection systems through machine learning (ML), behavioural monitoring and real-time analytics. At the same time, advancements in AI technologies, such as voice cloning, deepfakes and automated phishing systems, have enabled fraudsters to carry out more advanced and large-scale attacks, thus increasing the risk exposure for banks and their customers.

[1] Sarandeep Singh, *When Algorithms Steal: How AI is Rewriting the Rules of Financial Fraud in India*, RGNUL Student Research Review, February 6, 2026, available at https://www.rsrr.in/post/when-algorithms-steal-how-ai-is-rewriting-the-rules-of-financial-fraud-in-india (Last visited on 1 May, 2026).
[2] Id., para. 2.
[3] Reserve Bank of India, *Annual Report 2022–23*, 152.

The change has clouded the traditional boundaries of liability. In the Digital landscape, frauds often involve various relevant actors, including banks, customers and third-party platforms, making it tough to allocate clear responsibility. Notwithstanding the regulatory frameworks such as guidelines issued by Reserve Bank of India (RBI) and provisions under the Information Technology Act, 2000 as well as Bharatiya Nyaya Sanhita, 2023 aim to address these issues, their impact in dealing with AI-driven frauds remains ambiguous. Thereby, it becomes important to analyse the emerging role of AI in banking frauds, the allocation of liability among various stakeholders, and the effectiveness of existing legal and regulatory frameworks.

B. OBJECTIVES OF THE STUDY

The main objective of this paper is to comprehensively analyse the emergence of Artificial Intelligence in banking frauds. It also aims to examine the issues of liability and the adequacy of existing legal mechanisms. The specific objectives guiding this study are as follows:

1. To examine the growth of AI in financial frauds and interpret how it has reformed the nature and methods of financial crimes along with its impact on the financial system.

2. To categorize the kinds of AI-driven financial frauds in the digital banking ecosystem.

3. To investigate the distribution of liability among multiple stakeholders including banks, customers and digital platforms in financial frauds.

4. To study the outlook and evolving threats related to AI-driven financial frauds. Moreover, to evaluate potential technological advancements in this sector.

5. To assess the adequacy of current legal and regulatory mechanisms along with the guidelines issued by the RBI and to recommend measures for refining fraud prevention and strengthening accountability mechanisms in the digital banking landscape.

C. RESEARCH QUESTIONS

To analyse the problems related to AI-driven financial frauds & liability, the present study is directed by the following research questions:

1. How has the growth of AI changed the nature and intricacy of financial frauds?

2. What is the adequate allotment of liability among customers, banks and digital platforms in matters of banking frauds driven by Artificial Intelligence?

3. Are current legal and regulatory frameworks in India enough to address the issues raised by AI-driven financial frauds?

D. RESEARCH METHODOLOGY

The present research adopts a doctrinal research methodology, mainly based on secondary sources of data. The study relies on existing scholarly work, reports of the Reserve Bank of India, relevant statues, regulations and guidelines concerning with financial frauds have also been analyzed. Further, the research follows a qualitative approach, examining existing literature to understand the growth of AI in banking sector, the distribution of liability among multiple actors, and the adequacy of current laws and regulations.

II. SIGNIFICANCE OF ARTIFICIAL INTELLIGENCE (AI) IN BANKING

In recent years, Artificial Intelligence has appeared as a transformative force in the banking sector, significantly enhancing efficiency, personalising customer service, managing risk, detecting fraud, and offering financial advice.[4] With the rapid digitalization of banking services, banks are leveraging AI-based mechanisms, for instance, machine learning (ML), data analytics, and automation to enhance delivery of service and strengthen security mechanisms.

A. RISK ASSESSMENT AND MANAGEMENT

AI is rapidly replacing conventional human-led analysis in corporate operations, as manual operations are costly and time-consuming. Artificial Intelligence facilitates the automation of difficult tasks across various sectors, providing intelligent analytics, fostering clear thinking and assisting more informed decision-making. AI based systems are improving accuracy in calculations and data analytics, by constantly learning from data, therefore enhancing overall efficiency. In addition, AI-enabled chatbots have demonstrated to be highly efficient as customer service tools, minimizing operational costs while providing prompt and steady responses. Because of these advantages, AI is developing as a transformative technology with

[4] Shivam Swaroop Mathur, *The Legal Aspect and Evolution of AI in Global and Indian Banking*, IJLLR, (2024).

the capability to notably transform both commercial and non-commercial operations.[5]

Furthermore, Artificial Intelligence also plays a significant role in risk management by assisting banks to assess and mitigate different kinds of financial risks, such as credit risk, market risk and operational risk. Using predictive analytics, AI-powered systems examine customer's creditworthiness, detect possible defaults, and helps in informed decision making. In addition, AI assists in regulatory adherence by automating operations, including, data verification and reporting, thus decreasing human error and enhancing performance. This improves the overall steadiness and resilience of the banking sector.

B. FRAUD DETECTION

Artificial Intelligence (AI) is the best technology for fraud and security detection; it can assess a person's past spending patterns and behaviour towards transactions. From there, it can spot unusual behaviour, such as using a card from a different nation just hours after it has been used elsewhere or if there has been an extraordinary attempt to withdraw money from an account under investigation. Another stunning feature of AI fraud detection is its unwavering confidence in experience-based learning. When a person corrects a typical transaction that raises a red flag, artificial intelligence allows the system to learn from the experience and make informed conclusions about what constitutes fraud and what doesn't.[6]

C. CONVENIENT CUSTOMER SUPPORT AND CARE

In recent times, AI-based technology like voice systems, text chats, and chatbots have replaced the traditional customer care domain. By using these advanced technological systems, customer may now get high-level customer support and specialist guidance at a reasonable cost. AI-driven remedies have thereby taken the role of traditional customer service operations, saving time, cost and energy.[7]

D. FINANCIAL ADVICE

Artificial Intelligence is also progressively being used to deliver financial advices and tailored

[5] Hamir Nandaniya, *Why Can Chatbots Replace Mobile Apps Immediately*, Maruti Techlabs, available at https://marutitech.com/chatbots-replace-mobile-apps/ (Last visited on May 22, 2026).
[6] Id.
[7] Anil B. Malali & S. Gopalakrishnan, *Application of Artificial Intelligence and Its Powered Technologies in the Indian Banking and Financial Industry: An Overview*, 25(4) *IOSR J. Hum. & Soc. Sci.* 55 (2020).

banking services. With the help of algorithms and data analytics, AI-enabled systems examine customer spending behaviour, and income levels to offer personalized investment recommendations and budgeting knowledge. This not only improves customer experience but also enhances availability to banking services.

III. AI AS AN INSTRUMENT FOR FINANCIAL FRAUDULENT ACTIVITIES

A. THE WAY THE GROWTH OF AI HAS CHANGED THE NATURE AND INTRICACY OF FINANCIAL FRAUDS

In practice, swindlers often remain one step forward of those trying to obstruct them, as protectors must constantly catch up with emerging attack methods.[8] The COVID-19 pandemic and the causing shift to digital payments and teleworking of both banks and non-banking institutions have considerably expedited this process and provided swindlers with extra opportunities and advantages. Fraudsters, money launderers, identity thieves and hackers are concentrated on numerous channels and developing and using new kinds of attacks so that they cannot be easily caught by conventional fraud detection systems.[9]

Whereas number of present-day financial frauds integrate technical manipulation with social engineering, AI-driven banking frauds often shows unique functional patterns, specifically the use of synthetic media (e.g., deepfake audio/video), automated casual agents, and the ability to generate highly personalized and convincing fraudulent communications at scale. These capabilities enable fraudsters to mimic trusted individuals or institutions, evade traditional detection mechanisms, and exploit consumer trust with unprecedented speed and sophistication, thereby amplifying both the reach and impact of financial fraud.

Overall, AI has not just significantly escalated financial frauds but has intrinsically changed their essence, from simple, manual scams to extremely intelligent, versatile and technology-based threats. Frauds at present time are more personalized, fast-paced, and hard to detect, requiring equally sophisticated countermeasures.

[8] Vitaliy Shpachuk, Olena Markova & Bogdan Adamyk, *AI-Driven Financial Fraud: Key Risks and Legal Protections for Financial Institutions*, 27(1) *J. Banking Regulation* 6 (2026).
[9] S. N. John, C. Anele, O. Kennedy, F. Olajide & C. Kennedy, *Realtime Fraud Detection in the Banking Sector Using Data Mining Techniques/Algorithm* (2017).

B. HOW FRAUDSTERS USE AI?

Fraudsters or swindlers are using various tools like automated phishing messages, deepfake technology and AI-enabled voice cloning to extract large amount of money from the public that can convincingly impersonate trusted individuals like, bank officials. These methods have increased the chance of success, making scams difficult to trace. The methods or ways are as follows:

1. Deepfake Technology: Deepfake is the ability to distort reality by creating and audio and video of real people, saying and doing things they never said or did.[10] At present, Swindlers are exploiting this technology in increasingly advanced financial frauds. This technology has characteristics that enable rapid and widespread diffusion, putting it into the hands of both sophisticated and unsophisticated actors.[11] Fraudsters collect public available data such as, photos, videos, or voice samples, often from social media. Using this data, they train AI models to create highly realistic replicas of a person's identity. These replicas are then used by fraudsters in financial scams such as fake video calls, where the victim get highly convinced that they are interacting with a trusted authority like a bank officer, close relatives etc. In various cases, swindlers create a sense of urgency like an emergency of confidential business deal to pressurize victims to transfer money quickly. Deepfake technology can closely imitate facial expressions, voice, tone and speech patterns which help fraudsters to easily bypass any chance of doubt and distrust, making verification harder. Consequently, deepfake-enabled fraud has become an advanced tool in financial frauds, transforming scam from generic deception to highly tailored and technologically advanced manipulation.

2. AI-Driven Phishing: Phishing is a method in which fraudsters exploit social engineering tactics, often masquerading as trustworthy entities, to deceive individuals into divulging sensitive information, such as login credentials and financial details.[12] Nowadays, fraudsters are using AI-driven phishing instead of traditional phishing to bypass the security and verification measures. Scammers use artificial intelligence (AI) to generate extremely tailored and convincing emails, messages or chat interactions that seem to come from trusted and legitimate sources such as government agencies, banks or trusted corporations. In contrast to

[10] Robert Chesney & Danielle Keats Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 *Calif. L. Rev.* 1753 (2019).
[11] Id.
[12] Shivam Swaroop, supra note 4.

traditional phishing, AI enabled tools can examine huge amount of data from online activity and social media to customize messages according to the victim's interest, behaviour pattern and communication style. For example, fraudsters may send emails or messages that closely replicate official bank communication, with exact formatting, AI-powered logos and even particular context related details, making them harder to recognize as fraudulent. AI-powered chatbots are also used by scammers to involve victims in real-time conversations, mentoring them step-by-step to provide personal and sensitive information like, passwords or login credentials, OTPs, or to click malicious links. These kinds of attacks often create urgency like, account suspension warnings, KYC requirement or security alerts to drive victims into acting speedily without any verification. Consequently, AI-driven phishing substantially escalates the success rate of banking frauds by making them highly realistic, more targeted and difficult to trace.

3. AI-Powered Identity Theft: Fraudsters use artificial intelligence to manipulate personal data to create fake identities or improve stolen ones. They create "synthetic identities" by blending real and fabricated information including, names, phone numbers, Aadhar details, PAN card details that seem legitimate to financial institutions. AI-powered tools help fraudsters bypass security and verification measures like KYC (Know Your Customer) by generating highly realistic documents, facial images, or biometric data. These synthetic identities are then used to open bank accounts, obtain credit cards and apply for loans. Once they get access, scammers withdraw funds or make default on loans, leaving banks and other financial institutions to bear the loss and since these fake identities often do not belong to a single individual, identifying and tracing the scam becomes extremely difficult, making it a rapidly evolving challenge in AI-powered financial ecosystem.

4. AI-driven investment and trading fraud: AI-driven financial frauds are not just limited to deepfake and identity theft. Scammers are using AI to create highly persuasive fake investment platforms, websites, advertisements, or advisory services that assure hight returns with zero or small risk. AI-powered tools help produce credible and professional-looking websites, realistic market data, and even deepfake endorsements and feedback of celebrities or popular personality to build trust.

Fraudsters also use AI chatbots that engage with victims, directing them to invest more money while showing fake and fabricated profits on dashboards. Once a huge and targeted amount of

money is deposited, the scammers block withdrawals and disappear completely, leaving no trace behind.

5. AI-Based Voice Impersonation Fraud: This involves the use of AI to clone a person's voice and use it to commit financial frauds. Scammers usually collect voice samples through blank or silent calls, social media videos and then train AI to imitate tone, speaking style, accent with exact and extreme accuracy. This is used to make phone calls or send voice notes that sounds and appear similar to the real person.

In these frauds, scammers often pretend to be close family members to build confidence and urgency. For example, a targeted person may receive a call that sounds exactly like his or her close family member or relative asking for urgent money. Since they sound authentic, familiar and identical to the real person, victims get easily trapped. The use of artificial intelligence in voice impersonation to commit banking frauds, directly exploits human trust and confidence, making it extremely dangerous.

6. Document forgery and manipulation: Document forgery and manipulation have emerged as significant forms of AI-driven financial fraud. With the advancement of generative artificial intelligence, fraudsters can create or alter financial documents such as bank statements, invoices, salary slips, tax records, and identity proofs with remarkable accuracy. Unlike traditional editing methods, AI tools can generate realistic layouts, signatures, logos, and numerical data, making forged documents difficult to identify through manual inspection. These manipulated documents are often used to obtain loans, bypass Know Your Customer (KYC) procedures, submit false insurance claims, or support fraudulent financial transactions. The increasing sophistication of AI-generated documents poses serious challenges for financial institutions, as conventional verification systems may fail to detect subtle alterations.

IV. ADDRESSING THE QUESTION OF LIABILITY

The use of AI in finance also raises important questions about liability and accountability.[13] Since, banking frauds generally involves multiple actors such as customers, banks and digital or AI-powered platforms, the ascertainment of liability can't be imposed on an individual entity alone. Rather, liability falls upon according to the position, responsibility, duty of care and

[13] Shahmar Mirishli, *Regulating AI in Financial Services: Legal Frameworks and Compliance Challenges*, arXiv (2025).

level of negligence of each concerned party involved. Hence, liability for AI-driven banking frauds may extensively be divided as follows: bank liability, customer liability, and platform liability.

A. BANKS LIABILITY

Banks play the major and primary role in preventing AI-driven banking frauds because they regulate the banking infrastructure, authentication mechanism, transaction monitoring mechanisms and security & safety measures. According to the guidelines issued by Reserve Bank of India, the systems and procedures in banks must be designed to make customers feel safe about carrying out electronic banking transactions. To achieve this, banks must put in place:

1. appropriate systems and procedures to ensure safety and security of electronic banking transactions carried out by customers;

2. robust and dynamic fraud detection and prevention mechanism;

3. mechanism to assess the risks (for example, gaps in the bank's existing systems) resulting from unauthorised transactions and measure the liabilities arising out of such events;

4. appropriate measures to mitigate the risks and protect themselves against the liabilities arising therefrom; and

5. a system of continually and repeatedly advising customers on how to protect themselves from electronic banking and payments related fraud.[14]

Moreover, the Reserve Bank of India (RBI) in its circular, "Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions" has cleared that banks have full liability in cases where the banking fraud happens because of contributory fraud/ negligence/ deficiency on the part of the bank (irrespective of whether or not the transaction is reported by the customer).[15]

[14] Reserve Bank of India, *Customer Protection – Limiting Liability of Customers of Co-operative Banks in Unauthorised Electronic Banking Transactions*, RBI/2017-2018/109, DCBR.BPD. (PCB/RCB). Cir.No.06/12.05.001/ 2017-18 (Dec. 14, 2017).
[15] Reserve Bank of India, *Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions, RBI/2017-18/15, DBR.No. Leg.BC.78/09.07.005/2017-18 (July 6, 2017).*

Banks perhaps face liability for; inadequate AI oversight, improper safety and security measures, unsuccessfulness to prevent data of customers against AI-driven frauds.[16] The courts and consumer forums may hold the banks liable if they fail to carry out adequate AI-driven financial fraud detection system or ignores warning signs of unauthorised and suspicious transactions. If AI usage leads to harm, negligence, or breach of these existing duties, legal accountability may arise regardless of the presence of AI-specific laws.[17]

B. CUSTOMERS LIABILITY

Customers safety is of the foremost priority in financial frauds; however, they also bear certain duties in sustaining the security of their confidential banking credentials. While financial institutions have major responsibilities in deterring AI-driven financial frauds, customer awareness and cautious digital attitude is highly expectable to prevent frauds. Customer's liability usually originates where unauthorized transactions occur due to the customer's own negligence, delay in reporting scams, or revelation of confidential information including UPI PINs, OTPs, password and other important bank credentials.

Full and partial liability: According to the Reserve Bank of India (RBI), customers shall be liable for the loss where it occurs due to negligence by a customer, such as where he has shared the payment credentials, the customer will bear the entire loss until he reports the unauthorised transaction to the bank. If the delay in reporting is beyond seven working days, the customer liability shall be determined as per the bank's Board approved policy.[18]

In ***Punjab National Bank v. Sachin Kumar & Another***, the Uttarakhand State Consumer Commission held that since the transactions had been initiated from the customer's own mobile phone using authenticated bank credentials, neither aforesaid bank nor Google Pay was liable for the financial fraud. The Commission stated that safeguarding confidential credentials is the responsibility of customers and they will be liable for the loss where it occurs due to their own negligence. This case examined that customer negligence remains a significant factor in determining liability and reaffirmed the liability criteria set by RBI.[19]

[16] Mirishli, supra note 13.
[17] Kate Scott, *AI and Risk for Financial Institutions*, Int'l Fin. L. Rev. (Feb. 25, 2019).
[18] RBI Circular, supra note 15.
[19] *Punjab National Bank v. Sachin Kumar & Anr.*, SC/5/A/212/2022 (Uttarakhand State Consumer Disputes Redressal Comm'n Feb. 3, 2026).

Zero liability: A customer's entitlement to zero liability shall arise where the unauthorised transaction occurs in the following events:

1. Contributory fraud/negligence/deficiency on the part of the bank (irrespective of whether or not the transaction is reported by the customer).

2. Third party breach where the deficiency lies neither with the bank nor with the customer but lies elsewhere in the system, and the customer notifies the bank within three working days of receiving the communication from the bank regarding the unauthorised transaction.[20]

In ***PNP Polytex Pvt. Ltd. v. Reserve Bank of India,*** The Bombay High Court firmly rejected Bank of Baroda's argument that the use of valid OTPs implied negligence on the part of the company. The Court found that the victim fell prey to a third-party cybercrime. The court relied upon the RBI Master Circular on Customer Protection (updated from the July 6, 2017 guidelines). The framework limits customer liability to zero if the unauthorized transaction occurs due to a third-party breach (where the deficiency is neither with the bank nor the customer) and is reported to the bank within 3 working days.[21]

Thus, liability of customers even in AI-enabled financial frauds usually depends upon whether they revealed confidential information, the level of due care exercised, the swiftness with which fraud was reported etc. Meanwhile, judicial trends progressively recognize that AI-enabled financial frauds can exploit even vigilant customers. Hence, courts over time are moving away from directly blaming customers and rather analysing the overall facts and circumstances.

C. PLATFORMS LIABILITY

The fast integration of Artificial Intelligence into digital finance has significantly extended the role of online platforms, fintech intermediaries, social media companies, payment gateways, and AI service providers in the financial ecosystem. These technologies have also made it possible to carry out sophisticated financial fraud, including deepfake investment ads, AI-generated phishing, voice-cloning scams, synthetic identity fraud, fake loan applications and impersonation-based financial deception. As such, modern legal discussion is increasingly acknowledging that digital finance enabler platforms cannot be passive intermediaries, and

[20] RBI Circular, supra note 15.
[21] *PNP Polytex Pvt. Ltd. v. Reserve Bank of India*, 2026: BHC-OS:11082-DB, Writ Petition (L) No. 2791 of 2023 (Bom. H.C. Apr. 28, 2026).

may be liable in the event of fraudulent activities due to a lack of safeguards, negligent moderation, insufficient verification systems or a failure to with statutory due diligence standards.

Under Indian law, intermediary and platform liability is mainly governed by the Information technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.[22] Section 79 of the Information Technology Act grants intermediaries conditional "safe harbour" protection for third party content but such immunity is available only where the intermediary performs due diligence and doesn't knowingly facilitate illegal activity. Under the 2021 Intermediary Rules, platforms are also mandated to set up grievance redressal mechanisms, promptly remove unlawful content, support law enforcement agencies and prevent misuse of their digital systems.[23]

Recent academic literature has argued that AI has altered the scale and sophistication of digital fraud and thus increased the duty of care expected from online platforms. A research paper titled *"Deepfakes in Onboarding, KYC, and Financial Fraud: Authenticity Standards and Liability Framework for Digital Banks and FinTech"* explains that AI-generated synthetic identities and deepfake technology have advanced to the point of being able to bypass biometric verification systems and remote onboarding safeguards used by fintech companies and digital banks. The study highlights that platforms which rely on automated KYC and AI-assisted verification mechanisms may attract liability if they fail to implement proper detection tools or authentication security measures against synthetic fraud.[24]

Indian judicial trends also show increasing scrutiny of platform responsibility in AI-enabled fraud cases. In ***Ankur Warikoo v. John Doe*** (Delhi High Court, 2025), the Court recognized the dangers posed by AI-generated deepfake investment scams and directed intermediaries to remove fraudulent content promoting fake financial schemes. The case illustrates a growing judicial expectation that platforms must take preventive measures to combat financial fraud

[22] India, Ministry of Electronics & Information Technology, *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*, G.S.R. 139(E), Gazette of India, Extraordinary, Pt. II, Sec. 3(i) (Feb. 25, 2021).
[23] Sakkcham Singh Parmaar, *India's Deepfake Dilemma: Navigating the New Frontier of AI Content Regulation* (Jan. 26, 2026)., available at https://ssrn.com/abstract=6480499.
[24] Juan Emmanuel Delva Benavides, Jorge Antonio Leos Navarro & Alejandro Paul García Hernández, *Deepfakes in Onboarding, KYC, and Financial Fraud: Authenticity Standards and Liability Framework for Digital Banks and FinTech*, *Journal of Law & Technology* (2026).

and impersonation caused by AI.[25]

V. ANALYSING THE CURRENT LEGAL FRAMEWORKS GOVERNING AI-DRIVEN FINANCIAL FRAUDS IN INDIA

Although India has several laws dealing with cyber offences, financial frauds, synthetic media misuse, data protection, there is currently no single contemporary comprehensive legislation specifically regulating AI-driven financial frauds. Thus, the main laws and regulations currently governing AI-driven financial frauds in India include:

A. INFORMATION TECHNOLOGY ACT, 2000

1. Section 66, Computer-Related Offences and their Application: Section 66 of the IT Act establishes a wide framework for computer-related offences, criminalising the dishonest or fraudulent use of computer resources.[26] This rule may be applicable to scenarios in which synthetic media is created or distributed using computer system for fraudulent reasons.[27] However, it broadly criminalizes cyber offences without specifically recognizing AI-generated deception techniques.

2. Section 66C, Identity Theft: This section criminalizes the fraudulent use of someone's else identity and can be useful in cases AI-generated identity theft, synthetic identities, biometric spoofing or voice cloning but the provisions were drafted before generative AI technologies and doesn't explicitly cover deepfake impersonation.

3. Section 66D, Cheating by Personation using Digital Means: Section 66D explicitly targets cheating by personation in digital situations making it illegal to utilise communication devices or computer resources to impersonate another person.[28] This section can be used where fraudsters use AI tools to commit financial frauds based on personation such as deepfake investment frauds, phishing schemes, AI-driven impersonation scams. However, there is a loophole because this section focuses on traditional personation and lacks clarity regarding liability for AI-generated or automated impersonation.

[25] Ankur Warikoo & Anr. v. John Doe & Ors., 2025 SCC Online Del 3727 (Del. H.C.).
[26] Information Technology Act, 2000, § 66.
[27] Sommya Kashyap, *The Digital Mirage: India's Evolving Legal Battle Against Deepfake Technology*, 22 *Scripted: A Journal of Law, Technology & Society* 162 (2025).
[28] Id.

4. Section 72, Penalty for Breach of Confidentiality and Privacy: Section 72 of IT Act, 2000 penalizes unauthorized disclosure of confidential electronic information by persons who obtain lawful access under the Act. However, the provision was drafted specifically human actors in mind and doesn't explicitly consider authorized autonomous AI systems such as banking chatbots or algorithmic customer-service tools. In result, where an AI-powered system mistakenly discloses confidential bank or customer information to scammers through deepfake impersonation or synthetic identity manipulation, the applicability of Section 72 becomes legally uncertain, exposing important gaps in India's current legal framework.

5. Section 79: This section provides conditional "safe harbour" protection to intermediaries; but its traditional "notice-and-takedown" approach appears increasingly improper for AI-driven financial frauds, where use of deepfake and AI Impersonation to commit financial scams can spread at massive scale before detection or removal.

B. RESERVE BANK OF INDIA (RBI) REGULATORY FRAMEWORK AND GUIDELINES

The Reserve Bank of India (RBI) has issued several circulars related to customer liability, cybersecurity standards, digital payment security and so on. The RBI's circular titled *"Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions"* provides the framework for determining liability between banks and customers in cases of digital fraud. The circular provides concept of zero liability where fraud occurs due to bank negligence; limited or partial liability in third-party breaches and conditional customer liability where negligence is on their part.[29]

RBI has also issued cybersecurity directions requiring banks to adopt real-time fraud monitoring systems, implement multi-factor authentication and verification and mandating to maintain robust cyber resilience mechanisms. Despite these measures, AI-enabled frauds are still exploiting vulnerabilities in banking systems through deepfake voice calls, biometric spoofing, SIM-swap frauds and synthetic identity attacks. Academic literature indicates that current RBI frameworks are primarily focused on traditional cyber frauds and do not explicitly address liability arising from AI-driven financial scams. This creates uncertainty regarding liability standards in AI-related financial fraud disputes.

[29] RBI circular, supra note 15.

C. INDIA'S SYNTHETIC MEDIA REGULATION: INDIA'S DRAFT AMENDMENT RULES FOR 2025[30]

In October 2025, India's Ministry of Electronics and Information Technology issued draft amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021[31] , marking the country's first substantive regulatory attempt to address synthetic media and related frauds.[32] These rules impose due diligence obligations requiring intermediaries, especially those with over five million registered users in India, to mandate user declarations, use automated verification tools, and establish grievance redressal systems.

However, critics argue that existing intermediary liability standards were designed for ordinary user-generated content, deepfake detection technologies remain imperfect, and excessive monitoring obligations may conflict with free speech protections recognized in *Shreya Singhal v. Union of India.[33]* Research further argues that India's intermediary liability framework still largely operates on a reactive "notice-and-takedown" model rather than anticipatory AI governance. This makes rapid control of AI-generated financial frauds extremely difficult.

D. BHARATIYA NYAYA SANHITA, 2023 (BNS)

The adoption of the BNS represented a significant change in India's criminal justice system, replacing the colonial-era Indian Penal Code, 1860.[34] This modernised criminal law handles various offences that are directly applicable to AI-enabled financial frauds, despite the fact that it predates the widespread use of synthetic media technologies.[35]

1. Section 319, Cheating by Personation: This section defines cheating by personation as when a person deceives other by pretending to be someone else wilfully replacing one person for another.[36] This law is particularly relevant for use of deepfake or AI-tools to extort money and to commit banking frauds. However, the provision's traditional structure may struggle to capture the subtle technological components of AI-generated impersonation, especially in cases when the deepfake creator doesn't directly communicate with victims but instead

[30] Sommya Kashyap, supra note 27.
[31] India, Ministry of Electronics & Information Technology, supra note 22.
[32] Sommya Kashyap, supra note 27.
[33] *Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1.
[34] Bharatiya Nyaya Sanhita, 2023, Preamble (India).
[35] Sommya Kashyap, supra note 27.
[36] Bharatiya Nyaya Sanhita, 2023, § 319.

disseminates synthetic content via digital platforms.[37]

The Bharatiya Nyaya Sanhita, 2023 also includes provisions related to forgery, cyber deception and electronic fraud. Although the BNS can be applied to AI-driven financial fraud cases, researches argue that statue still lacks clear rules and provisions for AI-generated harm.

E. DIGITAL DATA PROTECTION ACT, 2023 (DPDP ACT)

The Digital Personal Data Protection Act, 2023 is the first comprehensive data protection legislation in India and has important impact for AI-enabled financial frauds as such frauds often rely on stolen personal data, misuse of biometrics and unauthorised profiling. The DPDP Act imposes obligation upon "Data Fiduciaries" to process personal data lawfully, maintain reasonable security measures, and prevent breaches of data. Experts have said AI-powered deepfake frauds often depend on large scale harvesting of personal data, voice samples, photographs and biometric details from digital platforms. Thus, stronger data protection obligations may help reduce the risks of AI-enabled financial fraud indirectly.

However, scholars have criticized the DPDP Act for no specifically and directly regulating AI-driven financial and other frauds. Thus, while the DPDP Act strengthens data security and privacy protections it remains not fully effective against AI-driven banking frauds.

F. WHETHER THE CURRENT LAWS AND REGULATIONS ARE ADEQUATE OR NOT

Many scholars have argued that India's existing legal framework is only partially adequate to address AI-driven banking frauds. While laws such as the IT Act, BNS, RBI guidelines, intermediary liability principles, and the DPDP Act provide some protection, major gaps remain, including the absence of dedicated and specific AI legislation.[38] Therefore, scholars argue for a more comprehensive and dedicated AI laws, stronger cybersecurity standards for banks, specialized mechanisms for investigating AI-driven frauds. Overall, India's legal framework is evolving, but it remains highly ineffective to address the growing sophistication of generative AI-based banking frauds.

[37] Sommya Kashyap, supra note 27.
[38] Sarferaaz Khaan R., *Countering Deepfakes: A Strategic Blueprint for Modernizing Indian Criminal Law*, 2 *Int'l J. for Legal Res. & Analysis* 5 (2025).

VI. RECOMMENDATIONS AND REFORMS

To combat AI-driven banking frauds and overcome the existing legal and regulatory gaps, this paper suggests the following reforms:

A. ENACT A DEDICATED AI REGULATORY FRAMEWORK FOR THE FINANCIAL SECTOR

India presently doesn't have specified and dedicated law to regulate AI-driven financial frauds as these frauds are currently governed through fragmented laws such as the Information Technology Act, 2000, Bharatiya Nyaya Sanhita, 2023, RBI circulars, Digital Personal Data Protection Act, 2023 (DPDP Act), and other Government issued frameworks.

To address the current legal and regulatory gaps a sector-specific AI law for banking and finance is needed which should define "AI-enabled fraud," "synthetic identity fraud," and "deepfake impersonation"; classify high-risk AI systems used in banking; impose mandatory compliance obligations on financial institutions deploying AI tools; and establish statutory liability standards for AI-generated harm.

Moreover, India may draw inspiration from the European Union AI act which get passed in passed in 2024, and become the world's first comprehensive and legally binding AI-regulation.[39] It categorizes high-risk AI systems and imposes strict compliance obligations.

B. ESTABLISH CLEAR LIABILITY ALLOCATION FRAMEWORKS

One of the largest legal gaps in AI-driven financial fraud is uncertainty regarding liability. Existing legal doctrines are heavily "human-centric" and struggle to determine responsibility when fraud is facilitated by autonomous or semi-autonomous AI systems.[40]

For this a "shared liability model" would prevent victims from bearing losses caused by institutional technological failures. This aligns with modern scholarship advocating hybrid liability systems for AI-related harms. A reformed framework should clearly distribute liability

[39] Satarkar Nale, Ganesh, *Regulating Artificial Intelligence in India: Legal Frameworks, Governance Challenges, and the Path toward a Dedicated AI Law* (2026).
[40] Sahibpreet Singh & Manjit Singh, *Algorithmic Criminal Liability in Greenwashing: Comparing India, United States, and European Union* (2026).

among:

Actor	**Proposed Liability**
Banks and financial institutions	Primary liability for failure to maintain adequate AI governance, cybersecurity, or fraud monitoring systems
AI developers/vendors	Liability for defective algorithms, negligent design, biased systems, or inadequate security safeguards
Intermediaries/platforms	Liability where they knowingly facilitate fraudulent AI-generated content or fail to act after notice
Customers/users	Limited liability in cases involving negligence such as sharing OTPs, passwords, or knowingly ignoring security warnings, subject to RBI consumer protection guidelines
Fraudsters	Criminal liability under cybercrime and fraud laws
Regulators	Supervisory accountability for failure to enforce compliance standards

C. CREATE MANDATORY AI AUDIT AND CERTIFICATION MECHANISMS

Financial institutions increasingly deploy AI systems without uniform regulatory auditing standards. RBI's recent recommendations under the proposed FREE-AI framework emphasize governance, assurance, and audit structures for AI deployment. The Committee's mandate was to assess AI adoption in financial services, review global regulatory approaches, identify AI risks for regulated entities (REs) and recommend a practical governance, evaluation, mitigation and monitoring framework tailored to India's financial sector.[41] Such mechanisms would improve institutional accountability and reduce systemic financial risks.

D. DEVELOP SPECIALIZED AI-CYBERCRIME INVESTIGATION UNITS

Traditional cybercrime investigation units often lack expertise in detecting AI-driven frauds such as voice cloning, deepfake impersonation, synthetic identities, automated transaction

[41] Reserve Bank of India, *Framework for Responsible and Ethical Enablement of Artificial Intelligence (FREE-AI)* (Aug. 13, 2025).

laundering and AI phishing bots. Thus, this paper suggests to establish specialized and sector-specific AI forensic units for AI-enabled financial crimes. These units should be trained and expert in "Machine Learning" forensics, deepfake detection, blockchain tracing, AI evidence preservation and algorithmic audit analysis.

E. STRENGTHEN DATA PROTECTION AND IDENTITY VERIFICATION STANDARDS

AI-driven frauds usually exploit weak KYC systems, leaked personal data and identity theft. To combat these gaps, stronger data governance and verification systems are essential.

Key reforms should include:

1. multi-factor biometric verification;

2. continuous KYC monitoring;

3. encrypted identity authentication systems;

4. restrictions on excessive data collection;

5. mandatory breach disclosure obligations; and

6. stronger penalties for negligent data handling.

The DPDP Act should also be supplemented with AI-specific safeguards against automated identity manipulation and synthetic profile generation.

F. CUSTOMER AWARENESS AND DIGITAL LITERACY REFORM

A major reform required to combat AI-driven financial frauds is the strengthening of customer awareness and digital literacy mechanisms. Since many AI-enabled frauds such as deepfake calls, phishing messages, voice cloning, and fake banking interfaces exploit lack of public awareness, banks and regulators should legally conduct periodic cybersecurity awareness campaigns. RBI, banks, telecom operators, and digital platforms should also collaborate to educate customers about safe digital banking practices, identification of AI-generated scams, and secure handling of sensitive information such as OTPs and passwords. The research

highlights that despite advancements in banking security systems, customer awareness and cautious digital behaviour remain critical components of fraud prevention.[42]

VII. CONCLUSION

The increasing use of Artificial Intelligence in banking has undoubtedly made financial services faster, more efficient, and more accessible. At the same time, it has also created new opportunities for fraudsters to misuse technology in ways that existing laws were never designed to handle. Deepfake scams, AI-generated phishing attacks, synthetic identities, and automated fraud schemes show that financial crimes are becoming more sophisticated with technological advancement.

Although India has certain legal mechanisms, these frameworks still operate in a fragmented manner and are not fully equipped to deal with AI-driven financial frauds. Questions relating to liability, accountability, platform responsibility, and regulation of AI systems continue to remain uncertain.

The issue therefore is not whether AI should be used in banking, but how its use can be regulated responsibly. Stronger cybersecurity standards, clearer legal provisions, better coordination between regulators and digital platforms, and greater public awareness will play an important role in reducing future risks. As technology continues to evolve, the legal system must evolve with it so that innovation and consumer protection can progress together.

[42] Md. Waliullah et al., *Assessing the Influence of Cybersecurity Threats and Risks on the Adoption and Growth of Digital Banking: A Systematic Literature Review*, Am. J. Advanced Tech. & Eng'g Sols. (Mar. 23, 2025).

REFERENCES

JOURNAL ARTICLES

1. Benavides, Juan Emmanuel Delva, Jorge Antonio Leos Navarro & Alejandro Paul García Hernández, *Deepfakes in Onboarding, KYC, and Financial Fraud: Authenticity Standards and Liability Framework for Digital Banks and FinTech*, J. L. & Tech. (2026).

2. Chesney, Robert & Danielle Keats Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 Calif. L. Rev. 1753 (2019).

3. *Indian Banking and Financial Industry: An Overview*, 25(4) IOSR J. Hum. & Soc. Sci. 55 (2020).

4. Kashyap, Sommya, *The Digital Mirage: India's Evolving Legal Battle Against Deepfake Technology*, 22 Scripted: A J. L., Tech. & Soc'y 162 (2025).

5. Mathur, Shivam Swaroop, *The Legal Aspect and Evolution of AI in Global and Indian Banking*, IJLLR (2024).

6. Shpachuk, Vitaliy, Olena Markova & Bogdan Adamyk, *AI-Driven Financial Fraud: Key Risks and Legal Protections for Financial Institutions*, 27(1) J. Banking Regul. 6 (2026).

ONLINE ARTICLES & WEB SOURCES

1. Ganesh, Satarkar Nale, *Regulating Artificial Intelligence in India: Legal Frameworks, Governance Challenges, and the Path toward a Dedicated AI Law* (2026).

2. John, S. N., C. Anele, O. Kennedy, F. Olajide & C. Kennedy, *Realtime Fraud Detection in the Banking Sector Using Data Mining Techniques/Algorithm* (2017).

3. Mirishli, Shahmar, *Regulating AI in Financial Services: Legal Frameworks and Compliance Challenges*, arXiv (2025).

4. Nandaniya, Hamir, *Why Can Chatbots Replace Mobile Apps Immediately*, Maruti Techlabs.

5. Parmaar, Sakkcham Singh, *India's Deepfake Dilemma: Navigating the New Frontier of AI Content Regulation* (2026).

6. Scott, Kate, *AI and Risk for Financial Institutions*, Int'l Fin. L. Rev. (2019).

7. Singh, Sarandeep, *When Algorithms Steal: How AI is Rewriting the Rules of Financial*

Fraud in India, RGNUL Student Research Review (2026).

8. Singh, Sahibpreet & Manjit Singh, *Algorithmic Criminal Liability in Greenwashing: Comparing India, United States, and European Union* (2026).

9. Waliullah, Md. et al., *Assessing the Influence of Cybersecurity Threats and Risks on the Adoption and Growth of Digital Banking* (2025).

REPORTS & GOVERNMENT PUBLICATIONS

1. Reserve Bank of India, *Annual Report 2022–23* (2023).

2. Reserve Bank of India, *Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions* (2017).

3. Reserve Bank of India, *Customer Protection – Limiting Liability of Customers of Co-operative Banks in Unauthorised Electronic Banking Transactions* (2017).

4. Reserve Bank of India, *Framework for Responsible and Ethical Enablement of Artificial Intelligence (FREE-AI)* (2025).

CASES

1. *Ankur Warikoo v. John Doe*, 2025 SCC Online Del 3727.

2. *PNP Polytex Pvt. Ltd. v. Reserve Bank of India*, 2026 BHC-OS 11082-DB.

3. *Punjab National Bank v. Sachin Kumar*, SC/5/A/212/2022.

4. *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

STATUTES & REGULATIONS

1. Bharatiya Nyaya Sanhita, 2023 (India).

2. Information Technology Act, 2000, § 66 (India).

3. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.