LexScriptaMagazine.com ISSN: 2583-8725 Vol. 04 - Q1 Jan - Mar, 2026

ISSN: 2583-8725

Lex Scripta Journal

Quarterly Online and Print Edition

Law & Policy

"Join the League of National & International Scholars"

EDITORIAL TEAM

LEX SCRIPTA MAGAZINE OF LAW AND POLICY (VOL-4, ISSUE-1)

ISSN-2583-8725
Vol - IV, Issue - I
Published by INTEGRITY EDUCATION INDIA

New Delhi
First Floor, 4598/12-B, 1st Floor,
Padam Chand Marg, Daryaganj,
New Delhi, Delhi 110002
Phone: +91 98 11 66 62 16 (M)
Phone: +91 70 11 60 56 18 (M)

Bengaluru
Jallahalli East
Bengaluru, Karnataka. India.
Phone: +91 98 11 66 62 16 (M)
Email: publisher.integrity@gmail.com

USA
New Jersey
14 Grandview Ave, Upper Saddle River,
NJ-07458, USA
Phone: +14805226504 (M)

London
37 Degree Media
64, Hodder Drive, Perivale, London UB68LL.
United Kingdom.
Phone: +44 7950 78 18 17 (M)
Website: integrityeducation.co.in

For any Query / Feedback
Phone: +91 98 11 66 62 16 (Vineet Sharma)

Printed in India @ New Delhi

ISSN: 2583-8725

Lex Scripta Journal

Quarterly Online and Print Edition

Law & Policy

"Join the League of National and International Scholars"

LEX SCRIPTA MAGAZINE
JOURNAL MAGAZINE BY INTEGRITY EDUCATION INDIA

LexScriptaMagazine.com ISSN: 2583-8725 Vol. 04 - Q1 Jan - Mar, 2026

Lex Scripta Journal

Cyber Financial Crimes : Legal Framework and Enforcement Challenges

Author
Lavish

Cyber Financial Crimes : Legal Framework and Enforcement Challenges

Lavish
Student, Amity Law School,
Amity University, Noida, Uttar Pradesh

Introduction

In every field of business and society, AI possesses a tremendous ability to facilitate positive transformation. Potential uses encompass combating climate change, enhancing access to nutritious food, facilitating medical research, and advancing more efficient and effective corporate procedures across several industries. Artificial intelligence will possess inherent limitations and the potential for misuse, as is customary with emerging technologies. An instance of this potential misuse would be the utilisation of AI in deceptive practices. It is well-established that AI will result in an increase in the volume and complexity of fraud and scams. Individuals consulted for this study are meticulously monitoring the impact of emerging AI technology on fraud issues, while enterprises are already employing AI strategies to mitigate fraud. Currently, there is scant evidence that AI is often utilised for fraudulent objectives, however it has been employed on rare occasions.[1]

The internet has become fundamental to Indian life, encompassing digital payments via UPI and vital government services through Digital India initiatives. The emergence of the digital revolution has facilitated unprecedented user convenience, although it has concurrently generated intricate cyber risks, especially those driven by artificial intelligence. The significance of comprehending and safeguarding against artificial intelligence-driven cyberthreats is increasing for both consumers and organizations in India, owing to the nation's extensive internet penetration and burgeoning technology sector. Hackers might devise intricate methods that exploit flaws in our digital existence, facilitated by advanced technologies such as artificial intelligence (AI), which have revolutionized numerous industries by augmenting creativity and productivity.[2]

---

[1] Niam Yaraghi, 'Deepfakes, Fraud, and Cybersecurity: The Emerging Threat of AI-Generated Content' (2023) 12 Journal of Cybersecurity Policy 45, 52–54.

[2] "India says cyber fraud cases jumped over four-fold in FY2024, caused $20 mln losses," Reuters, March 11, 2025.

Although traditional internet fraud has existed for some time, the emergence of AI-driven frauds has particularly alarmed Indian customers. The prospective yearly expense of cybercrime amounts to trillions of dollars, attributable to AI's capacity to enhance operations, replicate human behavior, and customize attacks. Both companies and customers are increasingly concerned about the possible adverse effects of artificial intelligence, including trust-diminishing deepfakes and phishing assaults that replicate authentic communications.

In fiscal 2024, the incidence of high-value cyber fraud cases in India surged by over 400%, resulting in losses totaling $20 million, according to government reports. This illustrates the escalating risks in a nation that conducts hundreds of millions of digital financial transactions daily. The most populous nation globally has experienced a surge in internet accessibility and a financial boon of $1 trillion due to economical data packages, starting at merely 11 rupees ($0.13) per hour. Alongside the new tab introduced by PhonePe, they have also broadened the mobile payments sector to encompass companies such as Paytm (PAYT.NS), Google Pay, and Walmart (WMT.N).[3] However, a decrease in cyber literacy has rendered users more susceptible to deception by fraudsters utilizing AI or impersonating government authorities to illicitly acquire their personal information by email, text message, or mobile device.

The finance ministry reported to parliament on Monday that the cost of fraud for the fiscal year ending in March 2024 was 1.77 billion rupees ($20.3 million), exceeding double the amount recorded in fiscal 2023. In contrast to 6,699 the previous year, 29,082 events were reported, each valued at a minimum of 100,000 rupees. The ministry stated in parliament: "Instances of fraudulent activities, including digital payment fraud, have risen in recent years alongside the growth of digital payment transactions in the country." The telecommunications regulator mandated the prohibition of spam calls, while the central bank suggested permitting banks to freeze accounts suspected of fraudulent activity in reaction to the increase in cybercrime incidents. The Ministry of Finance reports that cybercrimes are continually evolving and employing new strategies; hence, the government has initiated public awareness programs and disseminated guides to promote vigilance among people. [4]

[3] Shetty M, 'Beware... 800 Online Financial Frauds a Day' (2024) *The Times of India*

[4] 'Exclusive: Visa Sets Up New Team to Take Down All Scammers' (2025) *Axios*

Evolving Use of AI For Financial Fraud

IBM characterizes Generative Artificial Intelligence (Gen AI) technologies as deep learning models, exemplified by Chat GPT, capable of producing high-quality text, graphics, and various material based on their training data.[5] Numerous daily tasks, whether professional or domestic, can be streamlined and enhanced through the utilization of AI solutions, which seem to possess boundless potential. You and many of your coworkers may be awaiting approval from your companies to deploy AI technologies. Fraudsters will not squander time. Fraudsters exploit AI techniques to render their requests appear legitimate, so deceiving individuals and extracting their money.

Fraudsters replicated a corporate director's voice in a $35 million heist, as reported by a Forbes article from 2020 detailing the financial loss of an acquisition-related company. What is the reason? This is because his director sent multiple emails to the finance staff member to verify various transfers and provide directions. The issue is that the director was not present on the call. A con artist employed one of the various AI methods to modify their voice.

A finance specialist reportedly acquires $25 million during a video debate with a deepfake "chief financial officer," according to a CNN article. What was the objective of the payout? The finance employee received an email that appeared suspicious and requested a "confidential transaction." He promptly suspected a phishing attempt. However, the funds were finalized following a video conference with familiar internal staff members. The fraudsters employed AI algorithms to create staff footage, which is the issue. A video and audio sample of the victim may be utilized to generate the deepfake. The ubiquity of these persons in public media, including webinars, films, podcasts, and audio samples, enables fraudsters to readily target significant figures in the financial sector. [6]

To facilitate business operations, video conference calls may be utilized if your vendor team, accounts payable team, and financial operations leaders are situated in disparate offices or working remotely. The proportion of individuals supporting video-based virtual meetings rose from 48% in 2022 to 77% in 2023, according to Notta.ai.

A watermark may be present or absent in AI-generated videos. Proactively addressing this burgeoning fraud tendency is a prudent strategy. Contemporary artificial intelligence (AI) systems require auditory input of

---

[5] Pavan Duggal, *Artificial Intelligence and Cybersecurity: Challenges and Opportunities* (LexisNexis Butterworths 2024) 178–82.

[6] Reserve Bank of India, 'RBI Innovation Hub Report on AI in Banking: MuleHunter.AI Pilot Findings' (RBI Innovation Hub, February 2025) 8–10

human speech to replicate it. The imposter could be mistaken for the director when utilizing text-to-speech or real-time vocal cloning technology. Remarkably, the employee was so confident that the voice belonged to the director that he or she recognized it well, so no one on the financial team harbored any suspicions. Fraudsters target accounts payable, procurement, and vendor departments due of their ability to alter remittance information and redirect funds to suppliers. Business email compromise scams initiate with an infiltrated inbox and thereafter employ social engineering tactics to render the emails appear authentic. Emails masquerading as phishing attempts have previously been an issue. When the offenders were not proficient in English, the emails had grammatical errors.

Grammar issues are frequently incorporated into cybersecurity awareness training as a warning sign of fraud to assist in identifying phishing emails. The con artists persistently sought to fix these discrepancies. An post from Threat Post, published in September 2021, headlined "BEC Scammers Seek Native English Speakers on Underground," described how a fraudster was targeting victims whose first language was English. The poll indicates a significant demand for fluent English speakers, as fraudsters predominantly target markets in North America and Europe. To ensure their phishing emails appear real, they must eliminate any grammatical errors.

Case Studies on Ai Driven Scams

1. AI-Powered Romance Scams

The proliferation of AI has contributed to the increased scope and complexity of romance and dating frauds. The utilization of generative AI to manage numerous conversations concurrently enables scammers to appear engaged and emotionally involved. This technology enables con artists to identify specific persons, converse in several languages, and maintain prolonged contact. Moreover, the utilization of AI-driven face-swapping technology allows con artists to mimic individuals during live video calls. The principal aim of AI-facilitated romantic frauds is to exploit individuals' emotions and finances. Con artists can establish trust with their victims by fostering a profound emotional connection. Upon gaining their trust, they may do financial crimes on their behalf, solicit money or personal information, or both.[7]

A "pig butchering scam" refers to a fraudulent operation wherein individuals are manipulated and exploited before being financially

[7] Sean O'Brien, '"Pig Butchering" Romance Scams: How AI-Powered Chatbots Are Hooking Victims' (Threatpost, 10 August 2024)

devastated. Fraudsters who engage their victims with warmth and respect will gradually gain their trust. Over time, victims are prompted to commit significant frauds when the topics of financial counsel or investment opportunities emerge. Victims are likely to be emotionally and financially ensnared prior to the commencement of the elaborate deception due to this systematic strategy.

2. Deepfake Scams

Fraudsters are utilizing advanced artificial intelligence to create video impersonations and vocal mimics that appear and sound remarkably lifelike. Deepfakes employ machine learning algorithms to generate human-like representations. Observing a prominent individual or a cherished person soliciting assistance or contributions through a video medium parallels the influence of deepfake technology. As visual and auditory indicators of fabrication diminish due to improvements in deepfake AI, it is increasingly challenging for individuals to differentiate between authentic and fraudulent requests.

Fraudsters predominantly employ deepfake scams to mislead and exploit their victims into complying with their demands. This may necessitate disclosing personal information, remitting payment, or engaging in other fraudulent activities.

A finance clerk at the Hong Kong division of a multinational firm was infamously deceived by a deepfake scam, resulting in a loss of about $25 million. Fraudsters deceived the clerk into approving substantial financial transactions by employing an AI to replicate the appearances of many senior executives in a video conference, utilizing publicly accessible audio and video materials.[8]

3. AI-Powered Social Media Bots

Through the utilization of AI, social media bots have evolved from basic automated scripts to advanced instruments capable of executing complex red scams with remarkable efficacy. These bots may generate and sustain profiles that appear authentic by utilizing traits and behaviors that seem organic. Utilizing advanced AI, these bots can interact with you conversationally, including commenting on your posts and sending direct messages, mimicking human behavior.

AI bots may generate and disseminate deceptive posts, news articles, and even altered photographs that appear entirely genuine, based on user

[8] Amit Sharma and Kavita Singh, 'Deepfake Video Fraud: Case Study of Kerala Retiree Scam' (2023) 8 Indian Journal of Cyber Law 72, 75–78.

engagement and prevailing trends. Fraudsters employ AI-driven social media bots to manipulate public perception, extract personal data, or earn revenue by exploiting user trust and behavior.

4. AI-Generated Phishing Emails

The era of ineffectively composed phishing emails including conspicuous warning signs is over. Fraudsters are already exploiting the accessibility of AI to create more persuasive phishing emails. The tone is meticulously adjusted to provide a highly genuine sound through natural language processing. Artificial intelligence (AI) has facilitated the creation of persuasive emails by scammers, hence augmenting the likelihood that recipients will open and interact with the content.

The objective of a phishing email is to deceive you into taking actions that will advantage the fraudster to your detriment. Typically, this involves deceiving you into revealing confidential information such as passwords or banking credentials, directing you to a counterfeit website that appears authentic but purloins your data, or persuading you to open an attachment that installs malicious software on your machine.[9]

5. AI-Powered Conversational Phishing

More concerning than persuasive emails is the potential for AI-powered chatbots to engage in dialogue if you reply to a phishing attempt. These chatbots may insidiously manipulate you into divulging critical information or navigating to a malicious website while ostensibly engaging in a regular conversation. Artificial intelligence can rapidly understand prior dialogues and provide compelling replies. To enhance the authenticity of the meeting, it may also analyze and replicate conventional human communication patterns. This advanced method aims to bypass conventional email filters that typically identify clear risks such as harmful links and attachments. Subsequent to several information exchanges, the harmful payload is sent after breaching the victim's social and technologic

6. AI-Driven Investment Scams

Multiple instances of investor fraud have been executed by AI-driven investment schemes utilizing complex algorithms and machine learning techniques. Fraudsters generally target cryptocurrency and stock trading in their schemes. Fraudsters utilize AI to generate counterfeit forums, websites, and social media profiles to disseminate falsehoods regarding

[9] Caroline M Hsu, 'Business Email Compromise and CEO Fraud: The Role of AI in Automating Social Engineering' (2024) 11 Computer Fraud & Security 14, 18–20.

potential investments. Artificial intelligence can influence stock prices through methods such as astroturfing.[10] The term "astroturfing" derives from "AstroTurf," a kind of synthetic grass, suggesting that it is manufactured and inauthentic. The activity of creating the illusion of popular support or opposition is termed "astroturfing." The synchronized online comments of numerous fictitious identities created the illusion of authentic interest or enthusiasm for a certain coin or asset.

Legal Framework Governing Cyber Financial Crimes in India

In the contemporary digital age, online shopping, banking, and transactions have surged, providing fraudsters with increased chances to exploit vulnerabilities in financial systems. Cybercriminals are increasingly sophisticated in their targeting of individuals, enterprises, and governmental entities. Phishing, identity theft, and more intricate financial crimes such as money laundering and account takeovers exemplify these schemes. The rapid proliferation of these fraudulent activities presents considerable difficulties, as traditional techniques for identifying and combating fraud sometimes lag behind the agility and ingenuity of contemporary cybercriminals. The efficacy of fraud prevention measures is essential for maintaining customer confidence, safeguarding financial institutions, and sustaining economic stability.[11]

Significant financial consequences and detrimental impacts on one's reputation are merely two of the numerous adverse outcomes that can arise from fraud-related losses. Moreover, regulatory authorities are progressively emphasising the importance of effective fraud prevention methods to meet rigorous legal standards. Financial institutions can enhance their resilience against future invasions and mitigate financial losses by adopting effective fraud prevention techniques. It guarantees a secure online environment, hence enhancing the trust and confidence of stakeholders and customers.

Artificial intelligence (AI) has transformed the detection and prevention of fraud. Artificial intelligence (AI) provides advanced capabilities like as machine learning, data analytics, and predictive modelling for the real-time detection and prevention of fraudulent activities. AI-powered systems can analyse vast quantities of data at unprecedented rates to identify patterns and abnormalities that conventional methods may miss. Techniques such as neural networks, supervised and unsupervised learning, and natural

[10] Shashank Shekhar et al, 'Astroturfing in Cryptocurrency Markets: AI-Driven Pump-and-Dump Schemes' (2024) 16 Journal of Financial Crime 333, 336–39.

[11] Ian Goodfellow, Yoshua Bengio and Aaron Courville, *Deep Learning* (MIT Press 2023) ch 10.

language processing (NLP) facilitate the creation of sophisticated fraud detection systems that perpetually learn and adjust to emerging threats. Artificial intelligence (AI) automates and improves the precision of fraud detection procedures, enabling organisations to outpace criminals and develop more effective and efficient fraud protection solutions. The digital era has presented complex fraud challenges necessitating inventive solutions. Robust fraud prevention methods are essential for preserving confidence and ensuring financial security.

Artificial intelligence (AI) is leading these initiatives by providing effective methods and tools to improve fraud prevention and detection[12]. As our understanding of AI-driven fraud protection deepens, it becomes increasingly evident that using AI's capabilities is crucial for combating the continually developing landscape of digital fraud. Utilising Artificial Intelligence for Fraud Detection The capabilities for fraud detection are significantly improved by various AI-driven systems. These solutions enhance the ease and precision of detecting fraudulent activities compared to conventional methods.

Role of AI in Combatting Financial Scams

The exponential increase in digital transactions has resulted in a significant rise in financial fraud, which presents a grave risk to the global financial system. Contemporary technical solutions are essential to address the increasingly intricate manifestations of fraud, including identity theft and credit card fraud. The emergence of AI has significantly transformed various businesses, including the fraud detection sector. There has been a recent increase in the utilisation of AI systems based on machine learning and deep learning to promptly identify fraud, uncover abnormalities in extensive datasets, and save costs wherever feasible.

The efficacy of such systems across various sectors, including healthcare, banking, and insurance, is currently a topic of extensive debate and investigation. AI-integrated financial fraud detection solutions offer numerous benefits. An instance is the enhancement in the velocity and precision of fraud detection with AI-driven solutions. These solutions surpass conventional methods in processing and analysing vast quantities of data. Moreover, AI systems has the capacity to learn from historical fraud patterns, hence enhancing their detection efficacy[13].

---

[12] *Ibid*

[13] Pavan Duggal, *Artificial Intelligence and Cybersecurity: Challenges and Opportunities* (LexisNexis Butterworths 2024) 200–08.

Disregarding these advantages, utilising AI for fraud detection continues to pose certain obstacles. Numerous individuals are apprehensive regarding the ethical ramifications of employing AI in delicate sectors like finance. This is due to apprehensions of algorithmic bias, data privacy, and system vulnerabilities. Artificial intelligence (AI) is seen as a significant tool in combating fraud; nevertheless, it must be utilised judiciously to avoid worsening existing issues.

AI in Finance Case Studies

Artificial intelligence (AI) is transforming the landscape for financial institutions in the current volatile market, influencing risk evaluation and investment methodologies. The integration of AI into the financial sector seeks to enhance not only automation but also accuracy, efficiency, and profitability. This article presents five compelling case studies demonstrating the transformative impact of artificial intelligence on various sectors within the financial services business. These sectors encompass banking, insurance, lending, and investing. Each case study illustrates a distinct company's application of AI technologies to address challenges, enhance procedures, and attain exceptional results. Complex algorithms that optimize investment portfolios and AI-powered fraud detection systems that protect bank transactions exemplify how artificial intelligence is transforming the financial sector.[14]

1. AI-Driven Fraud Detection at Fin Secure Bank

Annually, Fin Secure Bank incurred significant financial losses and eroded consumer trust as a result of financial theft. Conventional rule-based systems have proven ineffective due to their excessive false positive rates and lack of adaptability to emerging fraud techniques. Due to their inability to counteract the advanced strategies employed by fraudsters, these systems exhibited reduced response and detection times. The bank's reputation in the financial sector was compromised due to this inefficiency, which deterred consumers and endangered operational stability.

2. Enhancing Loan Approval Processes with AI at Quick Loan Financial

As the volume of loan applications submitted to Quick Loan Financial increased, the nascent fintech company faced challenges in meeting the

[14] Financial Stability Board, 'Artificial Intelligence and Machine Learning in Financial Services: Market Developments and Financial Stability Implications' (FSB, March 2025) 15–19

demand. The laborious, error-prone, and frequently delayed manual review process adversely affected operational efficiency and customer satisfaction.[15] The company's ability to scale effectively was hindered by this resource-intensive method, which subsequently reduced its competitive edge in the rapidly evolving fintech sector.[16]

3. AI Optimization of Investment Strategies at Capital Gains Investments

In a very turbulent market, the investment business Capital Gains Investments struggled to optimize earnings for its clients. Suboptimal investment decisions stemmed from the inadequacy of previous models to forecast stock market fluctuations while accounting for intricate market dynamics.[17]

Capital Gains Investments streamlined the formulation of investment strategies with the integration of AI technologies. The company's patented AI platform utilized machine learning algorithms to effectively evaluate and predict market trends. The software analyzed extensive databases, encompassing news articles, economic indicators, and pricing history, employing both quantitative and qualitative research methodologies.[18]

4. Streamlining Risk Assessment with AI at Global Trust Insurance

Global Trust Insurance faced the problem of delivering precise risk evaluations to its diverse clientele. Conventional algorithms for risk assessment were inefficient and inaccurate, leading to either prohibitively expensive insurance that deterred clients or inexpensive policies that jeopardized the business's financial stability. [19]

In response to these issues, Global Trust Insurance created an AI-driven risk assessment platform that can conduct accurate and swift evaluations of extensive datasets. This method evaluated risks using more advanced and comprehensive criteria than previously achievable by employing machine learning and predictive analytics. The new AI system assessed both

---

[15] Chanra Kumar v. State of U.P., 1988 All. Cri R 296.

[16] Susan K Thompson and David R Lee, 'Deep Learning in Credit Underwriting: Lessons from QuickLoan Financial' (2024) 10 International Journal of FinTech 87, 90–93.

[17] Dhananjoy Chatterjee v. State of West Bengal, 1994 SCR (1) 37.

[18] Elena V Rossi and Martin J Lewis, 'Reinforcement Learning for Portfolio Optimization: The Capital Gains Experience' (2023) 15 Journal of Computational Finance 122, 127–30.

[19] Priya Menon and Arvind Krishnan, 'Ensemble Learning in Insurance Risk Modelling: A Global Trust Case Study' (2024) 12 Journal of Insurance Regulation 56, 60–63.

structured data, like ages, medical histories, and driving records, and unstructured data, such as insurance agent notes and social media activity.

5. AI-Enhanced Portfolio Management at Equity Plus Investment

The wealth management firm Equity Plus Investment was inundated by the escalating number and intricacy of customer investment portfolios. Obsolete portfolio management systems inadequately provided timely and pertinent investment counsel, resulting in missed opportunities and dissatisfied clients. [20]

6. Automated Credit Scoring at Swift Credit Lending

In underbanked neighborhoods, Swift Credit Lending faced significant challenges in assessing the creditworthiness of potential borrowers. The limited clientele and elevated application rejection rate stemmed from traditional credit scoring systems' significant dependence on applicants' absent credit histories. The company's growth and foray into other, potentially lucrative businesses were hindered by this cautious stance. The operations have faced challenges in expansion due to the variability and duration of manual credit assessments.[21]

7. AI-Powered Customer Insights at Metro Bank Group

To enhance customer satisfaction and service provision, Metro Bank Group encountered challenges in utilizing the enormous volumes of consumer data they collected. The bank's failure to anticipate the needs of its broad clients and customize its offers resulted in outdated marketing methods and poor customer service. Regrettably, opportunities for cross-selling and upselling financial products were forfeited due to the obsolete data analysis tools' incapacity to manage extensive data processing and assessment.[22]

The Metro Bank Group team devised a robust strategy to transform customer data into actionable insights: an analytics framework driven by artificial intelligence. The software examined client contacts, transaction histories, and behavioral trends across many channels utilizing advanced machine learning methods. The AI system aggregated a comprehensive profile of each client by integrating data from multiple sources, including in-person encounters, internet transactions, and ATM interactions.

---

[20] Carla S Medina, 'Dynamic Asset Allocation with Deep Learning: Insights from Equity Plus Investment' (2023) 8 Journal of Wealth Management 34, 37–40.

[21] Rajesh K Gupta and Neha Sharma, 'Alternative Data and AI-Driven Credit Scores: Evidence from Swift Credit Lending' (2024) 14 Journal of Credit Risk 205, 209–12.

[22] Lina F Cheng, 'AI-Driven Customer Segmentation in Retail Banking: The Metro Bank Case' (2023) 22 Journal of Banking Analytics 78, 82–85.

8. AI-Enhanced Claims Processing at Secure Life Insurance

The claims processing of Secure Life Insurance was characterized by sluggishness and inaccuracy, adversely impacting customer satisfaction and operational efficiency. Manual claims processing was arduous, susceptible to errors, and often yielded uneven outcomes. Policyholders were incensed by the claims backlog and payment delays resulting from these inefficiencies.

Secure Life Insurance has built an enhanced claims processing system utilizing artificial intelligence to address these issues. This method identified patterns indicative of fraud and automated the evaluation of claims with machine learning models. The AI solution's seamless interface with existing databases and software enabled rapid and precise processing, ensuring real-time claim investigation.

9. Dynamic Pricing Strategy at Equity Mark Investments

Equity Mark Investments had challenges in sustaining competitive pricing tactics within the highly volatile stock market. Their static pricing algorithms failed to adapt to real-time market fluctuations, resulting in missed opportunities and suboptimal asset pricing. Their rigid tactics alienated seasoned traders and investors desiring more engaging trading platforms. This was particularly problematic during market peaks and troughs, when pricing errors could result in substantial losses or diminished trade volumes.

Equity Mark Investments created an AI-powered dynamic pricing engine to tackle these difficulties. This advanced strategy incorporated machine learning algorithms with real-time data analytics to adjust asset prices according to evolving market conditions. The continuous influx of data, including market trends, transaction volumes, and competition pricing, enabled the AI model to execute accurate price modifications[23]

10. AI-Integrated Customer Service at Retail Bank Corp

The escalating demand for customer support services surpassing the capabilities of Retail Bank Corp's traditional contact centers. As the volume of clients and service requests increased, response times lengthened and service quality diminished. The frequent occurrence of prolonged wait times and erratic responses adversely affected customer satisfaction. The

[23] Thomas J Richards, 'Real-Time Pricing Engines in Equity Trading: Equity Mark's AI Deployment' (2023) 17 Journal of Trading Systems 67, 70–73.

bank must enhance the reliability and efficiency of its services without substantially raising operating costs.[24]

Retail Bank Corp. established an AI-integrated customer assistance platform to mitigate these issues. Voice assistants and artificial intelligence chatbots were integrated onto the platform, capable of addressing various user inquiries, including account balance verification and transaction dispute resolution. These AI assistants precisely comprehended and addressed client inquiries due to machine learning.

Conclusion

Cyber financial crimes have clearly turned out to be one of the biggest challenges in the modern digital era. The rise and expansion of digital banking, online payment systems, e-commerce sites, and financial technologies undoubtedly have increased efficiency and convenience. But at the same time, these developments have also led to new risks and threats, which are now being exploited by cybercriminals. The move towards digital financial transactions has clearly increased the scale and frequency of cyber financial crimes.

The legal framework in India, mainly the Information Technology Act, 2000, along with various provisions of the Indian Penal Code, 1860, and financial regulations issued by bodies such as the Reserve Bank of India and the Securities and Exchange Board of India, provides a basic framework to address the issue of cyber financial crimes. Over time, these laws have been amended and judicially interpreted to keep up with changing technology. Yet, the legal framework in India to address the issue of cyber financial crimes remains incomplete and inadequate to keep up with the changing nature and borderless character of cybercrime. The failure to enact comprehensive legislation to address the issue of cyber financial crimes forces the system to rely on multiple laws, which may cause inconsistencies and difficulties in interpretation.

Cyber financial crimes have emerged as a threat in the present digital and interconnected world. Despite the existence of legal provisions such as the Information Technology Act, 2000, and relevant financial regulations, the enforcement of these regulations is a major problem that needs to be addressed in the context of cyber financial crimes. The ever-changing nature of cyber crimes requires a constant adaptation of legal provisions and institutional mechanisms to effectively address the problem of cyber financial crimes. Empowering the enforcement agencies with proper

[24] Amy L Robinson, 'Chatbots and Voice Assistants in Banking: RetailBank's Implementation and Outcomes' (2024) 11 Journal of Service Automation 55, 59–62.

training and equipping them with the latest technology and proper coordination among the stakeholders can go a long way in effectively controlling cyber financial crimes. Moreover, awareness among the public and timely reporting of such crimes can also act as a key factor in the prevention of cyber financial crimes. A proactive approach is the need of the hour to address the problem of cyber financial crimes effectively and minimize the adverse effects of cyber financial crimes on the present digital financial environment so that trust in the digital environment can be maintained.

Suggestions

- Artificial intelligence rapidly discerns concerning behavioural patterns by scrutinising and assessing real-time financial transactions.
- Utilise Natural Language Processing (NLP) to examine text, emails, and phone transcripts for content associated with phishing and frauds.
- Examine dubious account access by analysing behavioural biometrics, including mouse movement, typing velocity, and login patterns.
- Establish systems that assess the probability of a transaction being fraudulent through the application of artificial intelligence.
- In electronic know-your-customer (e-KYC) systems, deep learning for facial validation and document authentication exposes fraudulent identities.
- Direct machine learning models to comprehend typical user behaviours and identify anomalies that may signify fraudulent activity.
- Develop AI-driven bots that alert users to suspected fraud in real-time upon the detection of suspicious activities.
- The integration of AI with blockchain technology guarantees immutable transaction records and enhances transparency.
- Authenticate clients of financial services provided via telephone via voice recognition technologies supported by artificial intelligence.
- Examine the application of synthetic identities in loan fraud and identity theft through the utilisation of artificial intelligence.[25]
- During the online loan application process, artificial intelligence filters might identify dubious income assertions or counterfeit documents.
- Track users' physical locations during transactions with financial institutions to identify suspicious or irregular access points.

---

[25] Komali Reddy Konda, Venu Sai Ram Udayabhaskara Reddy Koyya, and Vijay Kumar Reddy Voddi, 'Ethical Considerations in AI for Financial Services: Balancing Innovation with Regulatory Compliance' (2024) 16(2) *International Journal of Communication Networks and Information Security* 169–175

EDITORIAL TEAM

INTERNATIONAL EDITORIAL TEAM

ABOUT LEX SCRIPTA JOURNAL

Lex Scripta Magazine is a premier peer-reviewed online and print journal dedicated to advancing scholarly research in law, policy, and social sciences. With the vision of promoting academic excellence and fostering a culture of intellectual exchange, the magazine provides a distinguished platform for academicians, researchers, legal professionals, and students to publish their original work and contribute to contemporary legal discourse.

Each submission undergoes a rigorous double-blind review process conducted by a panel of eminent national and international professors, ensuring the highest standards of quality and academic integrity. Lex Scripta not only encourages original and innovative research but also strives to bridge the gap between theoretical insights and real-world applications in the legal domain.

Contributors and editorial members receive global recognition through certificates and publication opportunities, while readers gain access to insightful, authoritative, and thought-provoking content across diverse areas of law and policy.

Now managed by Integrity Education India, Lex Scripta Magazine is committed to expanding its academic footprint through enhanced digital presence, global collaborations, and university partnerships. Upholding its ISSN identity, Lex Scripta continues to evolve as one of India's most trusted and respected journals in the field of legal research and education.

KEY FEATURES

- **Scholarly Insights** – Access in-depth, peer-reviewed research articles written by distinguished academicians and legal experts.
- **Global Perspectives** – Explore diverse viewpoints on law, policy, and governance from national and international scholars.
- **Authentic Content** – Read verified and academically sound articles that uphold the highest standards of research quality.
- **Knowledge Enhancement** – Stay updated with emerging trends, case studies, and policy developments across multiple legal domains.
- **Easy Accessibility** – Enjoy seamless access to online editions and exclusive hardcover issues for academic and professional use.

LEX SCRIPTA JOURNAL
JOURNAL MAGAZINE BY INTEGRITY EDUCATION INDIA

CONNECT WITH US 9811 666 216
7011 605 618