IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Doctrinal Study On The Legal Dimensions Of Financial Fraud

M.D.Dheerajkumar[1], Sudharsan Balaji.S[2], Abithaambigai R[3]

[1] B.A.LLB (Hons.) 1st year LLM Cyber law and security, SRM School of Law, Chennai-603203
[1] B.B.A.LLB (Hons.) 1st year LLM Cyber law and security, SRM School of Law, Chennai-603203
[1] B.A.LLB (Hons.) 1st year LLM Cyber law and security, SRM School of Law, Chennai-603203

ABSTRACT:-

A wide range of illegal behaviours involving money, markets, and financial services are included in financial crime, such as insider trading, tax evasion, money laundering, and fraud made possible via cyberspace. Due to the quick transition to digital transactions, especially during the COVID-19 pandemic, traditional financial crime has evolved into sophisticated cyberattacks that take advantage of flaws in payment systems, user behaviour, and organisational compliance. Although India's regulation has been reinforced by legal responses like the IT Act, 2000, the MEITY, and the establishment of specialized wings for cybercrime.Effective prevention is still hampered by jurisdictional conflicts, inadequate compliance frameworks, and low public awareness.Strong regulatory frameworks and cross-border collaboration improve resilience, but they are nonetheless hampered by the rate of technology advancement, according to comparative studies conducted in the USA, UK, and UAE. Deepfakes, cryptocurrency fraud, and AI-driven phishing are examples of emerging risks that highlight how urgent it is to implement sophisticated monitoring, real-time detection, and more robust data protection measures. This essay makes the case that, in order to reduce risks and safeguard economic stability in the era of cybersecurity, financial crime necessitates a flexible legal system and cooperative international approaches.

Keywords: - Financial Crime, Cybersecurity, Money Laundering, Digital Payments, Phishing.

[1] B.A.LLB (Hons.) 1st year LLM Cyber law and security, SRM School of Law, Chennai-603203
[2] B.B.A.LLB (Hons.) 1st year LLM Cyber law and security, SRM School of Law, Chennai-603203
[3] B.A.LLB (Hons.) 1st year LLM Cyber law and security, SRM School of Law, Chennai-603203

INTRODUCTION:-

A financial crime is any crime that involves money, financial services, or markets.It encompasses a variety of activities that take place in various nations. Such crimes have existed inside this very civilisation since money was found to be a valuable instrument of trade for things. These crimes are harder to uncover because they evolve with society. The entire legal system needs to alter in order to penalise those who commit these crimes. Financial crimes include things like bribery, tax evasion, insider trading, currency counterfeiting, and money laundering. These crimes are committed by individuals or by specific organised organisations and have an impact on people, businesses, and even the economy of a country.These offences, which at first included actual money, progressively evolved into network-based offences where the money was transformed into digital form. The prevalence of financial crimes in the digital sphere has increased, and the legal system's biggest obstacle is the jurisdiction and other unfilled gaps.

In India, financial crimes are dealt with by a number of laws and authorities. The UNCITRAL Model Law on E-commerce, which addressed crimes pertaining to computer systems held by people, corporations, and the government, was initially included in the Information Technology Act of 2000. Following the establishment of the Ministry of Electronics and Information Technology in 2016, several developments pertaining to cyberspace occurred. To look into any crimes involving the usage of cyberspace throughout India, each State Police Department has set up a distinct Cybercrime Wing.They primarily address two categories of offences: non-financial and financial crimes. financial crimes involving the theft of money via phishing or computer or mobile device hacking. The Cybercrime Wing will be notified of these kinds of issues using the helpline number 1930. Social networking site hacking and modification are considered non-financial issues and can be reported via the NCRB portal. Cybercrimes are included under Section 111 of the BNS, 2023, which addresses organised crime.

In the era of cybersecurity, a number of factors influence financial crimes. One of the most significant phases that contributed to the quick digitisation of banking, financial services, and e-commerce was the COVID-19 era. It greatly simplified the process and cleared the path for the advanced payment methods offered by UPI and net banking. However, it has also given cybercriminals a lot of chances to take advantage of weaknesses through ransomware, phishing, identity theft, and insider threats. Authorities must address these methods to prevent them in the first place because there are ways to obtain an OTP from a user and collect the user's details to commit a financial crime that is always changing. The risks are further increased by users' lack of cybersecurity awareness, organisations' lax compliance procedures, and jurisdictional issues in cross-border cybercrime investigations. Financial crime and fraud are a continuously changing problem in the digital age, despite the development of more robust data protection laws and sophisticated security frameworks. This is because cyber threats are always growing faster than defensive measures can be put in place.

There are financial crimes in many jurisdictions, and authorities respond to them quickly. While regulatory measures like the Information Technology Act, 2000, and RBI recommendations aim to stay up with emerging threats and the cybercrime department, India's growing digital usage through UPI and online banking has increased exposure to phishing and digital payment frauds. Because of the country's vastness and the fact that people are becoming more tech-savvy but also more susceptible to financial fraud, cyber fraud is more common in the USA. However, a thorough response is offered by strict data breach notification rules and vigorous enforcement by organisations like the FBI, SEC, and FinCEN.Notwithstanding the ongoing risks of money laundering and online banking fraud, the UK's developed financial system is more resilient because to preventive measures like the Economic Crime and Corporate Transparency Act and the National Cyber Security Centre. Due to its fast digital transition and status as a major international financial centre, the UAE is susceptible to fraud involving cryptocurrency and cyber-enabled money laundering. Strict cybercrime laws, financial oversight by the UAE Central Bank, and collaborations with Interpol to address transnational threats are the government's responses. When taken as a whole, these comparisons show how technological adoption, regulatory attentiveness, and legal understanding influence how well financial crime is prevented in the cybersecurity age.

Technology-driven dangers that take advantage of the expanding digital economy are on the rise, according to current trends in financial crime and fraud. Deepfake technology and artificial intelligence are being abused to produce incredibly realistic phishing scams, identity thefts, and impersonation schemes. As online transactions and fintech services grow, frauds involving digital payments, loans, and cryptocurrencies are becoming more prevalent. Fraudsters are also employing a wider range of scam techniques, such as social engineering through SMS, phone calls, and social media platforms; remote access applications, and phoney loan applications. Large-scale fraud networks are increasingly being made possible by mule accounts and phoney KYC data, which complicates identification and prevention. Financial institutions and regulators are responding by implementing AI-driven monitoring, real-time fraud detection systems, and more robust identity verification procedures; however, current security measures are being challenged by the ongoing evolution of threats and potential hazards like quantum computing.

OBJECTIVES:-

- To examine the legal framework in the digital age with regard to financial crimes.
- To investigate court rulings and legal interpretations that have shaped the understanding and application of financial crime laws in the digital era.
- To investigate new breakthroughs in digital forensics, AI-powered fraud detection, and cybersecurity as investigative and preventative tools.
- To research how financial fraud and scams have increased as a result of fast digitization.

REVIEW OF LITERATURE:-

The ongoing difficulty of finding practical ways to stop financial crimes. Fieldwork and literature on financial crime served as the study's foundation. According to the study, because financial crimes and commercial crimes share similar traits, they continue to be classified as part of the same family. A crucial component of the country's development, public savings continue to be a divisive issue. When we lose it to crooks, we risk more than simply our savings. Because criminals lack the capacity for long-term planning and do not uphold the will of the public, we put society at risk as a whole. As illicit earnings cease to exist and investor trust wanes, our economic systems become more susceptible.[4].A study on Indian financial fraud and scams and how they affect emerging nations. The study intends to add to international conversations on the difficulties encountered by developing countries and advance knowledge of financial scams in India. It looks into how various elements interact to create economic vulnerability in an effort to provide a foundation for practical countermeasures to financial fraud. The study highlighted the difficulties of financial misconduct in a globalised economy by examining several fraud typologies, methods of operation, economic repercussions, and regulatory reactions. The need for alertness and flexible defences against changing cyberthreats is highlighted by an examination of fraud types like Ponzi schemes, cyber frauds, and banking scams, as well as their methods of operation, which include social engineering and technology exploitation[5]. This study looks at how the Indian banking sector helps prevent financial crimes, paying special emphasis to regulatory barriers, compliance strategies, and possible future advancements. It discusses the challenges of implementing know-your-customer and anti-money laundering regulations, spotting suspicious activity, and promoting compliance. It also looks at the regulatory framework, specifically the FEMA and the PMLA.The study ends with suggestions for how banks, regulators, and policymakers may improve efficiency and guarantee the stability of the financial system by utilising technology, international collaboration, and capacity building to increase resilience[6]. The impact of money laundering and related crimes on the Indian economy from 2011 to 2021 was studied by the author of the research paper "An Empirical Study: The Impact of Financial Crime on the Indian Economy," The study examined the relationship between key socioeconomic characteristics and financial criminal activities using a Pearson Correlation Coefficient calculator.The conclusion that financial crime in India has no detrimental effects on the Indian economy was reached after all four of the hypotheses that were examined on its detrimental effects were disproved[7]. With an emphasis on its different forms,

[4] Michel, P. (2008). Financial crimes: the constant challenge of seeking effective prevention solutions. *Journal of Financial Crime*, *15*(4), 383–397. https://doi.org/10.1108/13590790810907227

[5] Siddiqui, A., & Srivastava, J. (n.d.). A Study of Financial Fraud and Scam in India and its impact on Developing Countries. Retrieved September 15, 2025, from https://ijrpr.com/uploads/V5ISSUE4/IJRPR25772.pdf

[6] Tewatia, -. Lakshay. (n.d.). Combating financial crimes in the Indian banking sector: Regulatory challenges, compliance strategies, and future directions. Retrieved September 15, 2025, from https://ijalr.in/wp-content/uploads/2024/05/COMBATING-FINANCIAL-CRIMES-IN-THE-INDIAN-BANKING-SECTOR-REGULATORY-CHALLENGES-COMPLIANCE-STRATEGIES-AND-FUTURE-DIRECTIONS.pdf

[7] Shah, S. (2024). An empirical study: The impact of financial crime on the Indian economy. *Proceeding of the International Conference on Business, Management and Finance*, *1*(1), 58–70. https://doi.org/10.33422/icbmf.v1i1.556

prevalence, repercussions, and enabling economic/market mechanisms, the empirical environment of financial fraud as reported in scholarly research. Financial statement fraud, financial fraud, and fraudulent financial mis-selling are the three categories into which the review classifies financial fraud. According to this description, financial fraud is a complicated problem that differs based on the financial instruments, market segments, and actors involved.Recent developments that have been found to support financial fraud include the emergence of new conflicts of interest and perverse incentives, the entry of unsophisticated market participants, the increased complexity brought about by rapid innovation and a wider range of financial products, and the increased use of justified secrecy through confidentiality rules, off-balance-sheet constructions, and shell companies in secrecy jurisdictions[8]. The international framework for fighting financial crime and found that there is increasing agreement that the efforts being made now are not enough. The report emphasises the need for stronger national, regional, and international efforts to detect and stop illegal financial flows, which endanger financial stability and inclusion while also feeding social issues including smuggling, exploitation, and terrorism. Notwithstanding substantial investment, the author makes the case for a stronger focus on enhancing the legal, regulatory, and risk management toolbox as well as assisting law enforcement through private sector cooperation. Three main topics are examined: the constraints of the current global risk management framework, the systemic and societal effects of financial crime, and possible enhancements to this framework[9].Techniques, Trends, and Case Studies in Fraud Detection and Forensic Accounting. This article examines the techniques, trends, and case studies of forensic accounting and fraud detection. To combat financial crimes, forensic accounting combines accounting, auditing, and investigation. In order to prevent, identify, and look into practices like corporate fraud, embezzlement, and money laundering, forensic accountants are required due to the rise in financial fraud. Prominent scandals like Satyam and Enron have highlighted the necessity of effective fraud detection. Detailed financial analysis and data analysis to spot fraudulent trends are important strategies. One instance where forensic accounting revealed a substantial accounting fraud is the Satyam incident. According to the paper's conclusion, forensic accounting is essential for contemporary fraud prevention and detection, and as technology advances, its efficacy is increased, guaranteeing a sustained need for forensic accountants[10].(Agorbia-Atta & Atalor, 2024) In order to address the shortcomings of conventional approaches against complex criminal strategies, the study investigates how combining Artificial Intelligence (AI) and Cloud Technologies is improving Anti-Money Laundering (AML) capabilities in the financial sector. It highlights AI's effectiveness in real-time threat detection and reducing false positives by identifying complex activity patterns, while Cloud Technologies provide scalable and secure solutions for managing evolving risks and regulatory demands. The

[8] Reurink, A. (2016). Financial Fraud: A Literature Review. MPIfG Discussion Paper. Retrieved from https://www.researchgate.net/publication/303517861_Financial_Fraud_A_Literature_Review

[9] Muminovic, H. (n.d.). *THE GLOBAL FRAMEWORK FOR FIGHTING FINANCIAL CRIME*. Retrieved from https://jlp.ibupress.com/uploads/pdf/39.pdf.pdf

[10] Govt Polytechnic. (n.d.). Forensic accounting and fraud detection: Techniques, trends, and case studies. Retrieved September 15, 2025, from https://ijrar.org/papers/IJRAR19D5110.pdf

report highlights obstacles such data privacy issues and the requirement for specialized expertise, despite the fact that these technologies provide notable improvements in the prevention of financial crime. It comes to the conclusion that while strategic adoption is important, further study and development are necessary to fully realize its potential in protecting the financial system[11].This research examines forensic accounting in the digital age, focusing on U.S. perspectives of digital financial fraud prevention. A systematic literature review (2015-2022) reveals that financial fraud has become more complex due to advanced technologies. Forensic accounting has evolved by integrating new tools and techniques for detection and prevention. The study identifies prevalent digital fraud types in the U.S., assesses current practices, and discusses the importance of continuous skill and tool enhancement. With AI and predictive analytics predicted to enhance fraud detection, forensic accounting has a bright future. However, accountants must adjust to these new technologies. Recommendations include continuous learning, technology adoption, and stronger regulatory frameworks, with future research targeting the effectiveness of new technologies and regulatory impacts[12].Online scams and cryptocurrency fraud are two examples of the rise in economic crime in the digital age.The digital age has brought about significant changes in financial transactions, fostering innovation but also enabling economic crime, particularly cryptocurrency fraud and online scams. These crimes leverage the anonymity and global reach of digital platforms, with cryptocurrency fraud exploiting the decentralized and opaque nature of blockchain for schemes like Ponzi schemes and fake ICOs. Online scams, including romance fraud and phishing, utilize social engineering to exploit emotions and trick victims into revealing information or sending money. The increasing use of digital communication and mobile devices facilitates the global execution of these schemes. The paper advocates for stronger laws, enhanced enforcement, and public education, along with international cooperation and improved security measures, to combat these evolving digital financial threats[13].A bibliometric analysis of emerging threats in digital payments and financial crime. This bibliometric analysis looked at research on digital payment fraud, financial crime, and online payment fraud using Publications data analyzed with R and VOSviewer. It was able to pinpoint key themes, noteworthy contributors, and research gaps by using network analysis, collaboration mapping, and theme mapping. Among the primary areas of focus were information security, fraud risk in e-commerce, digital banking risk management, and fraud detection/prevention systems. Common study areas included blockchain, artificial intelligence, digital signatures, and credit card fraud.The subjectivity of bibliometric

[11] Agorbia-Atta, C., & Atalor, I. (2024). Enhancing anti-money laundering capabilities: The strategic use of AI and cloud technologies in financial crime prevention. *World Journal of Advanced Research and Reviews*, *23*(2), 2035–2047. Retrieved from https://www.researchgate.net/profile/Cedrick-Agorbia-Atta/publication/383561175_Enhancing_anti-money_laundering_capabilities_The_strategic_use_of_AI_and_cloud_technologies_in_financial_crime_prevention/links/66e3df81b1606e24c22666d0/Enhancing-anti-money-laundering-capabilities-The-strategic-use-of-AI-and-cloud-technologies-in-financial-crime-prevention.pdf

[12] Daraojimba, R. E., Farayola, O. A., O., O. F. M., Mhlongo, N., & L., O. T. T. (2023). Forensic accounting in the digital age: a US perspective: scrutinizing methods and challenges in digital financial fraud prevention. Finance & Accounting Research Journal, 5(11), 342–360. Retrieved from https://www.academia.edu/download/117505228/780.pdf

[13] *The Rise of Economic Crime in the Digital Age: Cryptocurrency Fraud and Online Scams*. (n.d.).

analysis and the study's reliance on English-language publications and the Scopus database were among its drawbacks. The results help financial institutions improve payment security and customer retention by offering recommendations for managerial risk assessment, technology investment, and training[14]. Digital assets and space transition are old scams with a new twist.This study uses space transition theory to investigate how fraud schemes have changed from using physical fiat money to digital crypto-assets. It concludes that because of anonymity and obfuscation, the digital environment and resources facilitate criminal activity under pseudonyms, posing regulatory difficulties. To prevent fraud and lessen societal harm, regulators and experts fighting financial crime must comprehend these schemes.The paper is noted as the first to detail this evolution and apply space transition theory to digital asset fraud[15].Legal Analysis Of The Transformation of Economic Crimes In The Digital Era (Cybercrime).Digitalization has facilitated economic transactions and global market access, but has also led to an increase in cybercrime, which threatens Indonesia's economic stability. While national legal regulations exist, their effectiveness is hampered by suboptimal implementation, insufficient infrastructure, and a lack of international cooperation. Addressing these challenges requires collaboration among the government, the private sector, and society to enhance digital literacy, strengthen regulations, and improve digital security systems[16]. Analyzing Digital Financial Literacy of Bank Indonesia in Preventing Digital Financial Crimes: A Qualitative Case Study in Banten Province.This study examined Bank Indonesia's initiatives in Serang City to boost digital financial literacy as a means of preventing digital financial crimes. Employing a qualitative case study, it found a direct correlation between improved digital financial literacy and a decrease in such crimes. The research highlights the effectiveness of localized digital literacy programs, offering valuable insights for policymakers and financial institutions, though its findings are specific to the study's context and may not be universally applicable[17].An Analysis of Cybercrimes in the Digital Age.This study examines high-tech crimes in the digital age, detailing their characteristics, categories, extent, and patterns, with a focus on Nigerian legal frameworks and global trends. Using a mixed-methods approach, the research identifies hacking, identity theft, and ransomware as significant global issues necessitating international collaboration. Effective responses include robust legal structures, enhanced cybersecurity, strategic partnerships, and public education. The study concludes that combating these crimes requires international cooperation, multifaceted strategies, technological progress, and increased public awareness

[14] Laxman, V., Ramesh, N., Jaya Prakash, S. K., & Aluvala, R. (2024). Emerging threats in digital payment and financial crime: A bibliometric review. Journal of Digital Economy, 3, 205–222. https://doi.org/10.1016/j.jdec.2025.04.002

[15] Dupuis, D., Smith, D., & Gleason, K. (2023). Old frauds with a new sauce: digital assets and space transition. Journal of Financial Crime, 30(1), 205–220. https://doi.org/10.1108/jfc-11-2021-0242

[16] Andini, T. W., & Yusuf, H. (2025). Legal analysis of the transformation of economic crimes in the digital era (cybercrime). *NOTARIIL Jurnal Kenotariatan*. https://doi.org/10.22225/jn.10.1.2025.1-6

[17] Analyzing Digital Financial Literacy of Bank Indonesia in Preventing Digital Financial Crimes: A Qualitative Case Study in Banten Province. (n.d.).

SUBSTANTIAL LEGAL ISSUES: -

In the digital realm, financial crimes raise a number of significant legal concerns. Cyberspace, as we all know, is a virtual environment in which people do not physically interact. Here, crime occurs everywhere in the world and cannot be solved by a single nation. There is a legal problem here with regard to jurisdiction. IPR laws use jurisprudence, such as copyright infringement, to identify jurisdiction, but there are no appropriate rules that govern the region of jurisdiction in cyber law. As a result, justice cannot be guaranteed to everyone in cyberspace.

Another area where there are numerous issues to address in relation to cyberspace is the advancement of technology. Laws must be swiftly adopted whenever new technology is launched anywhere in the world because as technology advances more often, so do the methods for committing cyberfraud. However, the methods for preventing these frauds do not change with the times. When it comes to financial fraud, transaction complexity is another issue. For example, when money from a scam is deposited into the bank accounts of innocent people, the cybercrime wing freezes their accounts.Numerous writ petitions have been filed before state high courts, and there is a growing body of jurisprudence in this area where the court has ruled that the police must defreeze the bank account and guarantee that the person retains the money deposited there until the case is looked into and a chargesheet is brought against the accused. The use of Virtual Private Networks (VPNs) to mask the attacker's identity and hacks to hide the IP address of the devices used for such actions present further challenges for the authorities in proving Mensrea.

Sheeba C.E. v. National Cybercrime Reporting Portal (2024) dealt with the Union Bank of India blocking a petitioner's bank account after receiving police requisitions about online financial scams.Under S.102(3) of the CRPC,1973, the Kerala High Court considered whether police could freeze bank accounts, whether timely reporting to the magistrate was required, and whether freezes should protect people who are not accused of crimes. The Court upheld the notion that bank accounts are "property" that can be seized with due process, citing prior rulings. A seizure may be unlawful under Article 300A if there is a complete failure to report, even while delays in reporting to the magistrate constitute anomalies. The Court ordered police to notify the bank about reporting the seizure to the magistrate in order to maintain a balance of power. To strengthen procedural compliance and protect individual rights, the freeze must be lifted if no report is submitted within a month[18].

The petitioners claimed that SIM swapping fraud resulted in illegal internet transactions in Tony Enterprises v. Reserve Bank of India, and they requested zero liability under RBI circulars. The court emphasised banks' fiduciary duty to protect clients by viewing SIM swapping as identity theft. It made clear that banks must follow RBI guidance even though direct contractual responsibility adjudication is not conceivable under

[18] W.P(C)25512 of 2024 Sheeba vs. National Cybercrime Reporting Portal,https://www.casemine.com/judgement/in/66e72db09d92026d6a3818c7

Article 226. According to the court, RBI circulars that classify transactions contaminated by fraud as "disputed transactions" require zero customer culpability for fraud without contributory negligence. The idea that consumers cannot be billed for transactions tainted by fraud unless liability is established in civil proceedings was reinforced when banks were ordered to return incorrectly debited funds to petitioners within two weeks and were allowed to seek civil recovery from fraudsters rather than consumers[19].

SUGGESTIONS:-

When it comes to cyberspace, there are numerous areas to manage. Court rulings and the ideas used in other areas, such as criminal law and intellectual property rights, can be used to correctly study jurisdictional concerns. Additionally, the government may use an escrow account-based victim compensation approach to reimburse victims of bank account freezing violations. To decide each issue, it is essential to conduct research on the various laws in India and other nations. Investigating new technological fields is also essential to guaranteeing optimal cybersecurity. Comparative research between nations is unquestionably required in the field of cyberspace in order to introduce new protocols and alternative approaches to threat management.

CONCLUSION:-

Money laundering, tax evasion, insider trading, internet fraud, and other illicit activities involving money, financial markets, and services are all included in the broad category of financial crime. These offences have evolved into increasingly sophisticated, technology-driven attacks that target flaws in payment infrastructure, human behaviour, and regulatory compliance processes as a result of the increased acceptance of digital transactions, particularly in the post-COVID period. Clear jurisdictional frameworks, legal direction, and tech-driven cybersecurity measures are necessary to address cyberspace concerns. Implementing strategies such as comparative legal studies and escrow models can enhance victim compensation and fortify fraud prevention.In conclusion, India has a system in place to deal with cybercrimes pertaining to present technology; nevertheless, as technology is always changing and new means of committing these crimes may emerge, it is undoubtedly necessary to deal with these offences. Laws will need to change appropriately to deal with these kinds of acts and respond quickly.

[19] Tony Enterprises v. Reserve Bank of India https://www.casemine.com/judgement/in/5e0203748ef1525824884 2f8