VOL 9 | Issue 2 | July-Dec 2025

ISSN : 2581-6837

jims

JIMS JOURNAL OF LAW

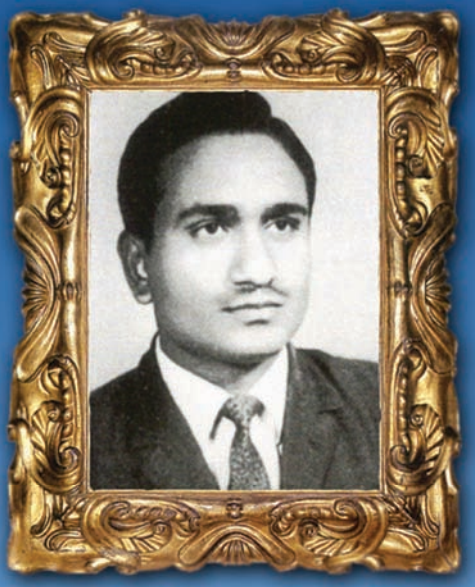
A Bi-Annual Peer Reviewed Journal

JIMS ENGINEERING MANAGEMENT TECHNICAL CAMPUS
48/4, KNOWLEDGE PARK III, Greater NOIDA 201308
www.jimsgn.org

A TRUE VISIONARY

"You see things and you say **Why***? But I dream of things that never were and say* **Why** *not?"*

- George Bernard Shaw



Shri Jagannath Gupta
(1950 - 1980)

Also a true visionary...who dared to dream!
He lives no more but his dreams live on....and on!

JIMS (Rohini)	**-**	**1993**
JIMS (Kalkaji)	**-**	**1997**
JIMS (Vasant Kunj)	**-**	**2003**
JIMS (Jaipur)	**-**	**2003**
JNIT (Jaipur)	**-**	**2004**
JIMS (Greater Noida)	**-**	**2008**
Jagannath University (Jaipur)	**-**	**2008**
Jagannath University (Bahadurgarh)	**-**	**2013**

And more dreams to come!

EDITORIAL BOARD MEMBERS

Editorial Office & Subscriber Service
JIMS Engineering & Management Technical Campus
48/4, Knowledge Park-III, Greater Noida, U.P. Phone #-01203819700,
lawjournal.gn@jagannath.org

From the desk of the Chief Editor

In our increasingly digital world, Socio-Economic crimes have evolved, expanding from traditional fraud to complex cyber offenses such as identity theft, cryptocurrency scams, and ransomware attacks. These crimes not only result in significant financial losses but also undermine public trust in digital systems, underscoring the urgent need for robust legal and regulatory responses. This edition features insightful contributions addressing the multifaceted nature of digital financial crimes and their socio-economic impact.

The paper *"Digital Financial Crimes and their Socio-economic Impact in Tamil Nadu"* offers strategic recommendations to mitigate the risks of cyber threats within the state. Similarly, *"The Road to Good Governance begins with Combating Corruption"* calls for integrated efforts to curb corruption through awareness and reform.

"Understanding the Socio-economic Impact of Cyber Financial Crimes" takes a multidisciplinary view, evaluating existing legal frameworks and emphasizing the need for stronger cyber governance and international collaboration. The article *"Case Studies on High Profile Financial Crimes and Their Legal Consequences"* explores real-world examples, revealing the complexities and legal ramifications of financial fraud.

In a forward-looking piece, *"Environmental Crimes as Socio-economic Offences: A Legal Analysis in the Context of Sustainable Development"* proposes reclassifying environmental crimes due to their impact on long-term economic goals. Finally, *"Digital Finance Crimes in Developing Economies: Socio-economic Risks and Challenges"* assesses the growing challenges faced by developing nations in managing these evolving threats.

I hope these contributions aid in reinforcing legal frameworks, improving enforcement, and fostering greater global cooperation. My sincere thanks to the authors for their valuable insights and to our readers for their continued support.

Sincerely,

Prof. (Dr.) Pallavi Gupta
Thanking You

Table of Contents

DIGITAL FINANCIAL CRIMES AND THEIR SOCIO-ECONOMIC IMPACT IN TAMIL NADU (2018–2025)

Veeranan Veeranan
Assistant Professor,
Department of Information Technology, P.K.N. Arts and Science College,
(Madurai Kamaraj University), Tirumanagalam, Madurai

ABSTRACT

Between 2018 and 2025, Tamil Nadu witnessed a significant rise in digital financial crimes, mirroring national trends while also highlighting local patterns. The most prevalent crimes included phishing, loan app fraud, ATM skimming, identity theft, cryptocurrency scams, and ransomware attacks. These crimes primarily affected the youth and middle-aged populations, with rural and elderly victims also experiencing notable losses. The socio-economic impact was profound, with over INR 120 crore lost in individual financial losses and substantial reputational damage to businesses. The state responded with legal and technological measures, including amendments to the IT Act, AI-driven fraud detection, and blockchain initiatives for land records. However, case resolution rates remained low until 2025, with continuous improvements in law enforcement collaboration and fraud detection technologies. This paper proposes strategic recommendations such as localized digital literacy programs, mandatory cybersecurity audits, and public-private partnerships to mitigate future risks and safeguard Tamil Nadu's digital ecosystem.

Key words: *Digital Financial Crimes, Tamil Nadu, Phishing, Ransomware, Legal Frameworks, Socio-Economic Impact, Technological Countermeasures, Public-Private Partnerships.*

Introduction

The rapid digitalization of India's financial ecosystem over the past decade has transformed the way individuals, businesses, and governments engage in monetary transactions. With the widespread adoption of Unified Payments Interface (UPI), mobile banking, and digital wallets, financial inclusion has deepened across states, including Tamil Nadu. However, this digital revolution has also opened new avenues for cybercriminals to exploit technological vulnerabilities and human behavior, leading to a sharp rise in digital financial crimes. From phishing scams and identity theft to ransomware attacks and cryptocurrency fraud, the nature of cyber threats has become increasingly sophisticated and pervasive.

Tamil Nadu, being one of India's more digitally advanced states, has not remained immune. The state has recorded a steady increase in cybercrime cases, particularly targeting urban populations, youth, and middle-aged professionals. While legal frameworks and cybersecurity mechanisms have evolved to combat these threats, the resolution rates remain modest, and the socio-economic consequences are significant. This paper aims to provide a comprehensive analysis of digital financial crimes in Tamil Nadu between 2018 and 2025, highlighting crime types, victim demographics, case studies, legal frameworks, and strategic recommendations for a safer digital future.

Types of Digital Financial Crimes in India (2018–2025)

Between 2018 and 2025, India experienced a dynamic shift in the spectrum of cyber-enabled financial crimes, with Tamil Nadu reflecting both national and localized patterns. Prominent crime types include:

Phishing & Social Engineering: A sharp rise in fraudulent messages and fake portals mimicking government subsidy websites and bank interfaces tricked citizens into revealing OTPs and credentials.[1]

Identity Theft: Aadhaar-based services became hotspots for fraud, with over 4,000 Aadhaar-linked scam cases reported in Tamil Nadu in 2023.[2]

Ransomware Attacks: Critical infrastructure, including cooperative banks and civic databases, were targeted, particularly during COVID-19 lockdowns.[3]

Cryptocurrency Scams: Ponzi schemes, fake exchanges, and unauthorized investment channels flourished despite regulatory warnings.[4]

ATM & POS Skimming: Criminals installed malicious hardware in devices across Chennai and Coimbatore to siphon off sensitive card data.[5]

Digital Money Laundering: UPI and mobile wallets were misused to launder illicit funds tied to gambling, fraudulent apps, and shell accounts.[6]

Techniques and Tools Used By Cybercriminals

With advancements in AI and mobile technology, cybercriminals adopted complex,evasive strategies:

AI and Deepfake Impersonation: Scammers used voice and facial deepfakes to impersonate government officials or bankers, effectively deceiving victims.[7]

Dark Web Transactions: Aadhaar, PAN, and banking credentials were sold on dark web platforms, with Tamil Nadu residents frequently listed among victims.[8]

Botnets & Scripts: Denial-of-service attacks and web portal breaches were orchestrated using automated tools targeting Tamil Nadu's e-Governance platforms.[9]

IoT Exploits: Vulnerable smart meters, surveillance systems, and budget smartphones served as access points in rural Tamil Nadu, leading to data theft and fraud.[10]

---

1 Tamil Nadu Cyber Crime Wing, *Annual cyber incident report* (2023).
2 UIDAI Tamil Nadu Office, *Fraudulent Aadhaar use complaints summary* (2023).
3 CERT-In, *Critical infrastructure cyber risk assessment* (2021–2024).
4 Reserve Bank of India, *Crypto fraud advisory reports* (2022–2025).
5 Chennai City Police, *ATM skimming case statistics* (2019–2024).
6 Ministry of Finance, India, *Online money laundering investigations*(2020–2025).
7 Data Security Council of India (DSCI), *AI threats and impersonation reports* (2024).
8 Cyber Peace Foundation, *Dark web data breach analysis* (2023).
9 TN e-Governance Agency, *Botnet incident response overview* (2022).
10 IoT Security Lab, IIT Madras , *Vulnerability study of rural IoT systems in TN* (2023).

SOCIO-ECONOMIC IMPACT IN TAMIL NADU (2018–2025)

The repercussions of digital financial crimes in Tamil Nadu were felt across individual, institutional, and state levels:

A. Individual Impact

Financial Losses: Between 2019 and 2024, estimated losses due to cyber fraud exceeded INR 120 crore in Tamil Nadu alone.[11]

Emotional Trauma: Victims often suffered from psychological distress, mistrust of digital services, and sleep disorders.[12]

Digital Exclusion: Older citizens and rural populations, fearing further loss, withdrew from digital engagement.1[3]

B. Business Impact

Reputational Damage: Startups and SMEs faced backlash due to data leaks and customer trust issues.[14]

Increased Cybersecurity Spending: SMEs increased their cybersecurity budgets by over 40% during 2020–2025.[15]

C. Statewide Economic Consequences

GDP Impact: Cybercrime contributed to an estimated 0.4% GDP loss in Tamil Nadu in 2024.[16]

Resource Allocation: The state had to divert funds to establish cybercrime cells, awareness drives, and digital policing units.[17]

---

[11] Tamil Nadu State Budget Report (2024).

[12] Iyer, N., & Raghavan, S. , "Mental health effects of digital fraud on victims", *Journal of Indian Psychology* (2022).

[13] Indian Institute of Public Administration, *Digital divide in rural Tamil Nadu* (2021).

[14] Tamil Nadu Fintech Association, *Compliance challenges in startups*.

[15] FICCI, *SME cybersecurity investment trends* (2024).

[16] Tamil Nadu Planning Commission, *Economic impact of cybercrime* (2024).

[17] Ministry of Home Affairs, *Cyber policing and outreach programs* (2023).

Trends and Demographics of Digital Financial Crimes in Tamil Nadu

Types of Digital Financial Crimes in Tamil Nadu (2025)

Table 1

Crime Type	Percentage (%)
Phishing	25%
Loan App Fraud	20%
ATM Skimming	15%
Identity Theft	18%
Crypto Scams	12%
Ransomware	10%

Victim Demographics in Tamil Nadu (2025)

Table 2

Victim Group	Percentage (%)
Youth (18–25)	30%
Middle-aged (26–45)	35%
Elderly (46+)	15%
Rural	10%
Urban	10%

Case Resolution Rates of Digital Financial Crimes in Tamil Nadu (2018–2025)

Table 3

Year	Resolution Rate (%)
2018	12%
2019	18%
2020	22%
2021	28%
2022	32%
2023	35%
2024	40%
2025	44%

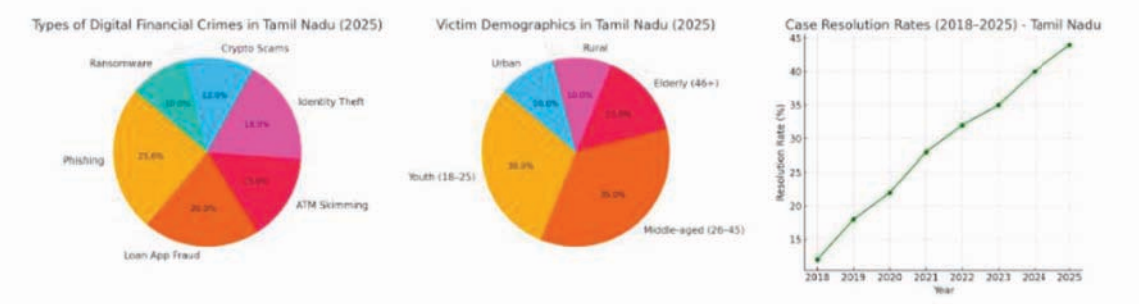


Figure 1

Case Studies in Tamil Nadu (2018–2025)

Tamil Nadu has experienced several major incidents that illustrate the evolving threat landscape:

***Chennai SIM Swap Scam* (2021)**: Fraudsters manipulated telecom agents to gain control of users' phone numbers and drained their bank accounts.[18]

***Coimbatore Loan App Scam* (2022)**: Over 200 complaints surfaced regarding loan apps that blackmailed users by accessing private data.[19]

TANGEDCO Ransomware Breach (2023): Over 9 lakh consumer records were compromised, highlighting poor cybersecurity in utilities.[20]

Thanjavur Rural Bank Phishing (2020): 80 farmers were defrauded of INR 1.2 crore, underlining the lack of digital literacy in rural banks.[21]

Legal Frameworks and Technological counter measures

A. Legal Infrastructure

IT Act Amendments: The Information Technology Act, complemented by the Digital Personal Data Protection (DPDP) Act of 2023, governs data protection and electronic evidence.[22]

State-Level Action: Tamil Nadu Cyber Crime Wings and TN-CERT enforce compliance and perform real-time audits.[23]

B. Technological Responses

AI-Driven Fraud Detection: Banks use ML algorithms to detect anomalies in user behavior and transactions.[24]

Blockchain for Land Records: Pilot initiatives by the Tamil Nadu Revenue Department utilize blockchain for tamper-proof land data.[25]

---

[18] Tamil Nadu Cyber Crime Wing, (2023), *Annual cyber incident report*.
[19] UIDAI Tamil Nadu Office, (2023), *Fraudulent Aadhaar use complaints summary*.
[20] CERT-In, *Critical infrastructure cyber risk assessment* (2021–2024).
[21] Reserve Bank of India, *Crypto fraud advisory reports* (2022–2025).
[22] Chennai City Police, *ATM skimming case statistics* (2019–2024).
[23] Ministry of Finance, India, *Online money laundering investigations* (2020–2025).
[24] Data Security Council of India (DSCI), *AI threats and impersonation reports* (2024).
[25] Cyber Peace Foundation, *Dark web data breach analysis* (2023).

Biometric KYC Authentication: Aadhaar-based e-KYC is used to protect access to banking and subsidy services.[26]

C. Institutional Collaboration

CERT-In and TN Police Coordination: Regular intelligence exchanges enhance incident detection and response.[27]

Inter-State Task Forces: Collaborative crackdowns help dismantle multi-state financial fraud networks.[28]

Strategic recommendations for Tamil Nadu

To effectively mitigate the rising threat, the following strategies are proposed:

1. **Localized Digital Literacy Programs**: Use Panchayats, schools, and SHGs to spread cyber awareness in Tamil.[29]
2. **Mandatory Cybersecurity Audits**: All state departments and digital service providers should undergo regular security audits.[30]
3. **Public-Private Partnerships (PPP)**: Foster innovation in secure transaction systems by engaging fintechs and academia.[31]
4. **Cryptocurrency Oversight**: Regulate crypto ATMs and run state-wide awareness drives to prevent investment fraud.[32]
5. **Real-Time Fraud Reporting**: Deploy WhatsApp helplines, 1930 emergency lines, and TN CyberSafe mobile apps for quick response.[33]

Conclusion

The surge in digital financial crimes in Tamil Nadu between 2018 and 2025 reflects the complex interplay between technological advancement and cyber vulnerability. While the adoption of digital financial platforms has improved efficiency and accessibility, it has also introduced new risks exploited by increasingly sophisticated cybercriminals. The dominance of phishing, loan app fraud, identity theft, and cryptocurrency scams indicates a need for stronger awareness and regulatory oversight. The data reveals that youth and middle-aged individuals, particularly in urban areas, are most frequently targeted, while rural and elderly populations remain highly vulnerable due to limited digital literacy.

---

[26] TN e-Governance Agency, *Botnet incident response overview* (2022).

[27] IoT Security Lab, IIT Madras, *Vulnerability study of rural IoT systems in TN* (2023).

[28] Tamil Nadu State Budget Report (2024).

[29] Tamil Nadu Cyber Crime Wing (2023), *Annual cyber incident report*.

[30] UIDAI Tamil Nadu Office (2023), *Fraudulent Aadhaar use complaints summary*.

[31] CERT-In. (2021–2024) *Critical infrastructure cyber risk assessment*.

[32] Reserve Bank of India (2022–2025), *Crypto fraud advisory reports*.

[33] Chennai City Police (2019–2024), *ATM skimming case statistics*.

Although the state's case resolution rates have improved—from 12% in 2018 to 44% in 2025—much work remains to be done. Legal reforms, institutional collaboration, and technological interventions such as AI-based fraud detection and blockchain integration have laid the foundation for a more resilient digital infrastructure. Moving forward, Tamil Nadu must prioritize localized digital education, enforce mandatory cybersecurity audits, and enhance real-time response systems to prevent and mitigate digital financial crimes. A proactive, inclusive, and collaborative approach will be essential to ensuring digital safety and economic stability in the years to come.

THE ROAD TO GOOD GOVERNANCE BEGINS WITH COMBATING CORRUPTION

Ashna Siddiqui
Assistant Professor, Birla School of Law

ABSTRACT

India, a developing country remains not a developed country majorly because of the biggest challenge that it faces today in the form of corruption. Corruption directly affects the delivery of public services. It essentially raises trust issues in institutions. It breaks down the speed of development of the country. To take care of the issue India has taken measures in the form of reforming institutions, aiming at advanced governance. The paper intends to highlight the role that Good Governance and robust institutions can help in shrinking corruption and encourage accountability and transparency in the country. Various legislative and policy reforms have been introduced over the last few decades to eradicate corruption from the very root of it. Legislations like Right to Information Act (RTI), the Prevention of Corruption Act have made the lives of citizens, aiming for better transparency in governance easier. Another landmark step was formation of Lokpal and Loktyukta where the ombudsman's role in achieving accountability and holding official responsibility, was something to look forward to. The advent of technology and the crucial role that it played in Digitalisation of systems, portals, tracking systems for any susceptible case of bribery and corruption. Regardless of the significant reforms, the challenges remain. The influence of powerful political parties, the delayed process of investigation and most importantly, too many agencies and lack of coordination among them weaken India's fight against corruption. Lack of awareness among citizens becomes another important reason for continued corruption, the process and the rights need to be highlighted to make citizens more conscious and aware. There is a dire need of better awareness and stricter implementation of legislative reforms that have been introduced. The paper shall aim to suggest that the best way to transform is to have holistic development backed by effectively implemented legislations, technology not promoting digital divide, and of course a common moral compass among institutions to work together to combat corruption.

Key words: *Corruption, Good Governance, Transparency, Accountability, Legislative Reforms.*

Introduction

Governance denotes the procedures and arrangements over which decisions and choices are taken, made, and implemented in a nation. Good governance implies answerability, transparency, approachability, rule of law, fairness, and contribution. Corruption weakens each of these essentials by twisting decision-making, dwindling institutions' framework, and permitting personal interests to supersede public good. Despite significant growth economically in a nation like India and its significant institutional development, corruption remains a problem to deter better progress. Consequently, fighting corruption is not merely a fitting imperative but a developmental inevitability.

According to the United Nations, Office of the High Commissioner for Human Rights (OHCHR), "the key question for assessing good governance is: Are the institutions of governance effectively guaranteeing the right to health, adequate housing, sufficient food, quality education, justice and personal security? Core elements of good governance include transparency, integrity, lawfulness, sound policy, participation, accountability, responsiveness, and the absence of corruption and wrongdoing."[1] India definitely needs to assess its condition relating to health, housing, education among others, and then understand how much corruption has harmed.

[1] Office of the United Nations High Commissioner for Human Rights, Good Governance (OHCHR) https://www.ohchr.org/en/good-governance/about-good-governance accessed 4 July 2025.

The World Bank defines "Good governance in terms of the traditions and institutions by which authority in a country is exercised. This includes 1) the process by which governments are selected, monitored and replaced; 2) the capacity of the government to effectively formulate and implement sound policies; and 3) the respect of citizens and the state for the institutions that govern economic and social interactions among them."[2]

The Nature and Impact of Corruption in India

Understanding the fabric of socio-economic conditions pertaining to India helps in highlighting the impact of deep-rooted corruption in the country. Many development projects do not see the light of the day as the fund allotted for the same gets diverted elsewhere, leading to massive delay in progress of the project and ultimately increasing the very cost of the project, it not just undermines development, but it also deepens in equality. As this entire plot of corruption tend to affect the poor strata of the society, unimaginably, more than anyone else, as the poor rely more on the services for public development. The act of corruption not just takes away the trust of the public from the institutions. It also weakens the very social contract that is important and crucial between the state and the citizens.

The representatives are chosen by the citizens in order to lead public institutions in a fair and just manner. The practice of corruption, so deeply embedded, ranges sometimes from the very bottom to the top level; it could be found in a petty matter or a massive scandal involving crucial authorities.

No sector remains untouched, be it education, and infrastructure projects, healthcare or distribution system. The petty bribery has become an acceptable form these days for the smallest of things just in order to get things done faster. Time and its shortage has led to thriving practice of corruption even if it's in a minor form. What remains uncontested is the impact this systematic practice of corruption is having on the fabric of the society.

Legislative Measures Undertaken to Combat Corruption

It is not like India has not tried to curb the practice of prevalent corruption. It indeed has brought many legal reforms via legislation and policies, particularly aiming to promote transparency and ensure accountability.

One of the most renowned and spoken about legislation remains the Right to Information Act 2005. This act is the result of a long historic fight that various leaders and organisations had fought. MKSS and leaders like Aruna Roy, Nikhil Dey, Shankar Singh among other activists had fought legally to bring this Act to its life[3]. The Act is a masterpiece, empowering the public to demand relevant information from public authorities. The act massively helps in understanding the irregularities and exposing the same, if any. RTI empowers in the simplest way possible as a tool for any information that's required even at a grassroot level. It's an extremely cost-effective mechanism to know of the funds allocated and distributed, the seats reserved and allotted among other things. It's a tool that ensures the public authorities are on their toes and abide by the

[2] Daniel Kaufmann, Aart Kraay and Pablo Zoido-Lobatón, 'Governance Matters' (World Bank Policy Research Working Paper No 2196, World Bank 1999) https://doi.org/10.1596/1813-9450-2196.

[3] RTI Act 2005, s 3 – 'Right to information'. See also Aruna Roy et al., *The RTI Story: Power to the People* (Rupa 2018).

requirement of the Act and display the information at all platforms or provide the correct data, if demanded for.

Another act is the Prevention of Corruption Act[4] which has seen recent amendments, making it evolve better. This Act criminalises any corruption or bribery in the smallest of the behaviour among public servants. Any offenders under this act shall not be spared from punishment. The act is appreciated for its criminal punishment to the offenders, regardless of the position they hold as public authorities.

One of the key provisions in the act is Section 7 that ensures the fine and punishment for the offence relating to a public servant being bribed.

"[*7. Offence relating to public servant being bribed.—Any public servant who,— (a) obtains or accepts or attempts to obtain from any person, an undue advantage, with the intention to perform or cause performance of public duty improperly or dishonestly or to forbear or cause forbearance to perform such duty either by himself or by another public servant; or (b) obtains or accepts or attempts to obtain, an undue advantage from any person as a reward for the improper or dishonest performance of a public duty or for forbearing to perform such duty either by himself or another public servant; or (c) performs or induces another public servant to perform improperly or dishonestly a public duty or to forbear performance of such duty in anticipation of or in consequence of accepting an undue advantage from any person, shall be punishable with imprisonment for a term which shall not be less than three years but which may extend to seven years and shall also be liable to fine.*"[5]

Another key provision of the Act that holds the public servant responsible for their unlawful act and punishes them is the provision mentioned herein below.

"*13. Criminal misconduct by a public servant —1 [(1) A public servant is said to commit the offence of criminal misconduct,— (a) if he dishonestly or fraudulently misappropriates or otherwise converts for his own use any property entrusted to him or any property under his control as a public servant or allows any other person so to do; or (b) if he intentionally enriches himself illicitly during the period of his office. (2) Any public servant who commits criminal misconduct shall be punishable with imprisonment for a term which shall be not less than [four years] but which may extend to [ten years] and shall also be liable to fine."*[6]

India witnessed one of the greatest showdowns where social activists, leaders, and the general public all came together to protest against the rampant corruption that's been going on. As a result of that and more like fulfilling a demand of that protest, Lokpal and Lokayukta came into picture. The highlight is the creation of an independent anticorruption Lokpal that is ombudsman at the central level and at the state level, in the form of Lokayuktas. This independent ombudsman shall help in investigating the complaints in a fair and just manner against the public officials or servants.

---

[4] Prevention of Corruption Act 1988, Act No. 49 of 1988.https://www.indiacode.nic.in/bitstream/123456789/9317/1/corruptiona1988-49.pdf accessed 1 July 2025.

[5] Prevention of Corruption Act 1988, s 7.

[6] Prevention of Corruption Act 1988, s 13.

Whistleblowers play a vital role in any country. Section 11 of the Whistle Blower Protection Act ensures that the person who has made the disclosure is protected. *"11. Safeguards against victimisation. -(1) The Central Government shall ensure that no person or a public servant who has made a disclosure under this Act is victimised by initiation of any proceedings or otherwise merely on the ground that such person or a public servant had made a disclosure or rendered assistance in inquiry under this Act. (2) If any person is being victimised or likely to be victimised on the ground that he had filed a complaint or made disclosure or rendered assistance in inquiry under this Act, he may file an application before the Competent Authority seeking redress in the matter, and such authority shall take such action, as deemed fit and may give suitable directions to the concerned public servant or the public authority, as the case may be, to protect such person from being victimised or avoid his victimisation:"*[7]

The Central vigilance commission is a commission that ensures vigilance in central government organisation and the commission helps in executing the vigilance work in a proper and transparent manner, owing all the transparency and accountability[8].

Digital Governance: A Hopeful Tool for Better Governance

As the time is changing, and everything is at fingertips, therefore, the present definition of good governance must include digital governance. Digital governance must act as a tool to curb and ultimately remove corruption from the system that it is deeply embedded in.

India has moved towards digitalisation with its landmark initiatives like E procurement portals, Digi locker[9] and ultimately became a flag bearer in achieving reduced human interface and simplified access to services.

The Aadhaar based identification[10] helps in reduction of chances of corruption as it removes any intermediary and directly gets credited to the beneficiary, minimising any chance of leakage in the system in between. This idea of direct transfer of benefits to the public has helped many citizens and is appreciated worldwide.

Digitalisation not just helps in distribution of help or benefits. It also helps in tracking and monitoring dashboard where in the public grievances could be made and honest feedback could be taken and real time issues could be speedily redressed at the public grievance redressal systems online

It's still not a bed of roses as the challenges remain in combatting corruption, despite multiple reforms. Corruption is so deeply embedded in the society that even with legal reforms and digitalisation, the goals remain unachieved. Cronyism in politics, in funding, in patronage networks, continue to influence public appointments in an unjust and unfair manner. It undermines the efforts made by a meritorious candidate and prefers the one who has taken the corrupt ladder.

---

7 Whistle Blower Protection Act, s.11.

8 Commonwealth Human Rights Initiative, 'A Review of the Whistleblower Protection Act' (2021).

9 Ministry of Electronics and IT, 'Digital India Initiatives' https://digitalindia.gov.in accessed 1 July 2025.

10 UIDAI v Justice KS Puttaswamy (Retd) and Ors (2019) 1 SCC 1.

The nation may have witnessed introduction of multiple legislations, but the enforcement of the same and effective implementation remains in question. The political pressure and interference highlights the lack of autonomy and ultimately results in weak enforcement of potential game changing reforms.

No law or any legislative provision can work on its own until the citizens that it is made for exercises it. The lack of awareness of these laws and reforms continue to make the citizen feel less empowered and fearful. No Citizen, unless made truly aware of their protection, shall raise a finger be it in the form of RTI, or as a Whistleblower, against a strong crony system.

And as they say, too many cooks spoil the broth, similarly, too many agencies and not so clear mandates have made effective investigation leading to prosecution a far-fetched dream.

Conclusion & Suggestion

When there is a will, there is a way and the only way forward is via strengthening governance and integrity systems. The political will and electoral reforms shall play the most crucial role in achieving transparency and accountability. There is a requirement of robust transformation in funding related to politics, selection of the candidates in an open and transparent manner and strict punishment for any malpractice specifically relating to electoral discrepancies. Awareness campaigns at public level. Effective participation at the grassroot level and education relating to laws and policies is the only way to empower citizens to ask the right question and demand transparency and accountability.

Autonomy to the institutions and agencies must be ensured and effective training of staff must be provided to map and highlight any corruption related activities. For any case that requires speedy disposal, a special fast track court should be instituted, especially for high profile cases, to set a precedent. The Whistleblower Protection Act lies in the corner, without any effective implementation. That act is extremely important to instill courage among individuals to not fear and act as a whistle blower wherever required. Similar Act in various other countries has seen able implementation and has worked extremely well in maintaining transparency.

Good governance is also achievable when the corporates and private sector start adhering to the regulation honestly. It must be highlighted that with increased corporate involvement as for increase in privatisation, the corporate malfeasance plays an aid in getting at an even more corrupt system.

One of the many criticisms of the legal reforms that have been happening is its adherence to the format of legislation, but its lack of substance that is required and desired for an actual solution. The Lokpal Act, RTI, Prevention of Corruption Act among others, line up as proper legislations with correct intention but lack any implementation quality. Lokpal must be criticised for not achieving the goal of the very envisioned anticorruption ombudsman. The anticorruption ombudsman remains an idea that has not seen the light effectively due to lack of autonomy, under experienced staff more than that, the political will to not proceed for it. RTI act criticised for being not protective of the activists it intended to be helpful for. RTI as a tool may have given

a voice to the activists, but it has failed to give them a safe shelter for raising these much-required questions. It is important to understand that the institutions are present, but their effectiveness remains questionable.

Digitalisation in form of Aadhaar, direct benefits form or grievance redressal portals online may have reduced interface-based corruption. However, it is also to be noted that digitalisation has introduced exclusion and challenges concerning the digital divide where the poor have not been benefited from schemes that they otherwise could have been. As much as we appreciate the digital governance tools, one cannot sideline the fact that digital divide is a reality and one must criticise it for the same.

Corruption is not petty always, nor is it transactional always, it is extremely strategic and involves high-level players that may govern digital presence or digitalisation cannot deter or hinder. As much as one needs to appreciate technology, but anything over is injurious and that needs to be remembered, so that overdependence on technical fixes do not take away the human dimensions, aiding better ways of corruption, which is so deeply rooted in politics. Digitalisation may help us address some symptoms, but it does not help in addressing the causes of corruption that lies deep in commodification of public office and impunity among other things.

The opaque political funding majorly dominated by cash-based donations and electoral bonds need to be questioned. One of the biggest criticisms is the encouragement of quid pro quo arrangements that essentially helps in returning the favour, mostly by electoral bonds or cash.

These bonds are in a very recent and landmark judgement of 'Association for Democratic Reforms v Union of India' are criticised and considered unconstitutional. The political economy of corruption is such that it is not just a hindrance, but an enabler of survival of political parties and maintenance of the power that they enjoy. The anti-corruption gestures are often made instrumental in picking against opponents or merely showing compliance with international rules and standards. Any institutional reform up until today remains just a mask underneath which lies the nexus of politics, power, and money leading to corruption.

One of the criticisms remains the campaign done by political parties and the money involved in them. Lack of transparency in campaigns promotes corruption in a very institutionalised format.

One must not only hold the political bodies guilty for the practice of corruption but one must look closer, and within sometimes, where they often normalise bribery in their everyday life. Be it getting a service done faster or be it trying to get out of a situation, which has legal repercussions in the form of the simplest of fines. The need of the hour is not just accountability at the procedural level but accountability of each and every individual to aim towards a value based public service culture that shall automatically transition and reflect in an ethical, transparent and accountable governance.

Citizens and civil societies have been demanding transparency, but the shrinking space in democracy has led to activism feeling threatened. Multiple restrictions on NGO, attacks on activists, surveillance of societies have all led to a shrunk civic space. This space ultimately aids in shielding corrupt practices from public eyes.

The public may have pressurised and gotten laws like RTI, but the disconnect between institution and civic empowerment is real and it reveals that good governance remains a distant dream until institutional transparency and citizen freedom gets the front seat.

The road to good governance definitely begins with corruption being combatted, but the road is not an easy one. The way forward is not merely legislative reforms in pen and paper but in practice, in effective implementation.

UNDERSTANDING THE SOCIO-ECONOMIC IMPACT OF CYBER FINANCIAL CRIMES

Chandrani Chakraborty
Research Scholar, Department of Law, Motherhood University,
Roorkee, Uttarakhand

ABSTRACT

Cyber financial crimes have emerged as a significant threat in the digital age, targeting individuals, corporations, and governments alike. These crimes, which include identity theft, online fraud, phishing scams, ransomware attacks, and financial data breaches, not only disrupt economic stability but also erode public trust in digital financial systems. This paper explores the socio-economic impact of such crimes, examining their effects on financial institutions, national economies, and vulnerable populations. It delves into the loss of revenue, increased operational costs, reputational damage, and the psychological toll on victims. Moreover, the study highlights the widening digital divide and the disproportionate burden borne by marginalized communities. Through a multidisciplinary lens, the paper assesses current regulatory frameworks and technological safeguards, emphasizing the urgent need for robust cyber governance, public awareness, and international cooperation. The findings underscore that combating cyber financial crimes is not merely a technological challenge, but a socio-economic imperative essential for sustainable digital growth. These crimes not only cause substantial monetary losses but also erode public trust in digital platforms, impede financial inclusion, and place a heavy burden on legal and regulatory frameworks.

Key words: *Socio-economic, Financial Crimes, Crime, Digitalization, Public Awareness, Legal Reforms, Cyber Crimes, Cybersecurity, Policies.*

Introduction

The 21st century has been marked by an exponential rise in the use of digital technologies that have revolutionized nearly every facet of human life, most notably the global financial system. From mobile wallets to internet banking, from cryptocurrency trading to instant money transfers, the digitalization of financial services has made economic transactions faster, more accessible, and convenient. This transformation is particularly significant in developing economies like India, where digital inclusion is rapidly increasing due to government initiatives such as Digital India, Jan Dhan Yojana, and Aadhaar-enabled payment systems. However, with these advancements comes an equally significant and insidious threat: cyber financial crimes.

Cyber financial crimes refer to unlawful acts carried out using digital technologies to gain unauthorized access to financial information or services, usually for monetary gain. These include a wide range of activities such as phishing, identity theft, credit card fraud, unauthorized access to bank accounts, cryptocurrency scams, and business email compromises. Unlike traditional forms of crime, cyber financial crimes are borderless, difficult to trace, and often involve sophisticated networks that exploit both human and technical vulnerabilities. The use of artificial intelligence (AI), the dark web, and cryptocurrencies has further complicated the landscape, enabling perpetrators to commit crimes anonymously and escape jurisdictional enforcement.

The socio-economic impact of cyber financial crimes is far-reaching and multifaceted. Economically, it results in substantial financial losses to individuals, corporations, and governments. These crimes compromise the integrity of financial systems, lead to customer attrition, and damage investor confidence. They also increase the operational costs for financial institutions, which must now invest heavily in cybersecurity infrastructure and insurance. Socially, cyber financial crimes cause psychological trauma, loss of trust in digital platforms, and

contribute to the digital divide by discouraging digital adoption among vulnerable groups.

Despite their growing prevalence, cyber financial crimes are often underreported due to fear of reputational damage, lack of awareness, or perceived ineffectiveness of law enforcement agencies. This impedes the formulation of robust policy responses and data-driven prevention mechanisms. Additionally, the legal and regulatory framework in many countries, including India, remains inadequate and fragmented, struggling to keep pace with the rapidly evolving cyber threat landscape.

Given these pressing challenges, it becomes imperative to study the socio-economic dimensions of cyber financial crimes in a comprehensive manner. This paper aims to explore the nature, types, and causes of cyber financial crimes; examine their direct and indirect impacts on various socio-economic actors; analyze the existing legal frameworks; and propose actionable policy recommendations. By shedding light on both the micro and macro-level consequences of cyber financial crimes, this research seeks to underline the urgent need for an integrated, multi-stakeholder approach to combating this digital menace.

Defining And Classifying Cyber Financial Crimes

Cyber financial crimes can be broadly defined as illegal acts committed using digital technologies with the aim of financial gain. These crimes typically involve unauthorized access to financial data, manipulation of banking software, or deception of users to extract sensitive information. The key classifications include:

2.1 Phishing and Vishing

Phishing refers to the act of sending fraudulent communications, often via email, that appear to come from reputable sources with the intent to trick individuals into revealing personal and financial information. Vishing, or voice phishing, is a telephone-based version of phishing, where scammers impersonate bank officials to extract data[1].

2.2 Identity Theft

Cybercriminals steal personal data such as Aadhaar numbers, PAN cards, and credit card details to impersonate victims and conduct fraudulent transactions. The consequences can be devastating, including unauthorized loans or tax fraud[2].

2.3 Credit Card and Debit Card Fraud

Using spyware or skimming devices, criminals capture card information and carry out unauthorized transactions. These are among the most commonly reported types of financial cybercrimes globally[3].

2.4 Online Banking Frauds

These involve breaches in internet banking portals or mobile applications, often through malware attacks or social engineering tactics, resulting in unauthorized fund transfers[4].

---

[1] Gaurav Gupta, *Cybercrime in India: Trends and Preventive Measures*, 45 ILI Law Review 123 (2023).

[2] Rina Dhawan, "Identity Theft in Digital Age: Legal Challenges and Remedies," (2022) 38(2) Delhi Law Journal 117.

[3] Rahul Mehra, "Credit Card Fraud and Indian Law," (2021) 13 SCC J 98.

[4] IT Ministry Report, *National Cyber Security Policy*, (2023), p. 12.

2.5 Cryptocurrency Scams

As cryptocurrency platforms remain largely unregulated, they have become breeding grounds for Ponzi schemes, pump-and-dump scams, and fraudulent Initial Coin Offerings (ICOs)[5].

2.6 Business Email Compromise (BEC)

A cyberattack where hackers spoof or infiltrate a company's email system to instruct unauthorized transfers of company funds. These attacks are often sophisticated and well-targeted[6].

Economic Impact of Cyber Financial Crimes

3.1 Direct Monetary Losses

Cybercrimes lead to significant direct financial losses for individuals, corporations, and governments. According to the FBI's Internet Crime Complaint Center (IC3), global losses from cyber financial crimes crossed $12.5 billion in 2022 alone[7]. These figures are often underreported as many victims, especially in developing countries, do not report such incidents due to stigma or lack of awareness.

3.2 Cost of Data Breaches

Beyond theft, cybercrimes often involve massive data breaches, affecting millions of customers and costing companies millions in remediation. According to IBM's Cost of a Data Breach Report 2023, the average cost of a data breach was $4.45 million, with the financial sector ranking among the most affected[8].

3.3 Impact on Financial Institutions

Banks and financial service providers face increased expenditure on cybersecurity infrastructure, legal settlements, and customer compensation. These costs often get passed on to consumers in the form of higher fees or reduced services. Furthermore, cyberattacks erode trust in banking systems, leading to reduced customer engagement and hesitation in adopting digital finance[9].

3.4 Insurance and Compliance Costs

Cyber insurance has become a necessity, but premiums are rising steeply due to increasing incidents. Regulatory compliance costs have also surged as governments mandate stricter cybersecurity protocols and data protection laws. These overheads affect business competitiveness, especially for smaller firms[10].

---

5 *Ibid.*

6 FBI Annual Report, "Business Email Compromise" (2023), www.ic3.gov.

7 *Ibid.*

8 IBM Security, Cost of a Data Breach Report 2023, www.ibm.com/security/data-breach.

9 Reserve Bank of India, Cybersecurity Guidelines (2020).

10 OECD Digital Economy Outlook, 2022.

Socio-Economic Consequences

4.1 On Individuals

The most immediate victims of cyber financial crimes are often individual users—particularly the elderly, digitally illiterate, or economically vulnerable. A single incident can wipe out savings, lead to debt traps, and even result in psychological trauma. Moreover, victims often face bureaucratic hurdles when attempting to reclaim their money[11].

4.2 On Businesses

Small and medium enterprises (SMEs) are highly vulnerable due to limited cybersecurity resources. Cyber incidents often disrupt operations, result in IP theft, or cause customer attrition due to reputational harm. For many small firms, a single cyberattack can lead to bankruptcy[12].

4.3 On the State and Society

At the macro level, frequent cyber financial crimes can erode investor confidence in a country's digital economy, affect GDP growth, and undermine national security. For example, attacks on payment infrastructure can cripple entire economic sectors and cause widespread panic, as seen in the ransomware attack on Costa Rica's Ministry of Finance in 2022[13].

Case Studies

5.1 Bangladesh Bank Heist (2016)

In one of the most audacious cyber financial crimes in history, hackers used the SWIFT network to transfer $81 million from Bangladesh Bank's account in the U.S. to fictitious accounts in the Philippines and Sri Lanka[14]. The breach revealed gaping vulnerabilities in interbank communication systems and prompted global financial institutions to revisit their cybersecurity strategies.

5.2 Equifax Data Breach (2017)

Equifax, a major U.S.-based credit reporting agency, suffered a cyberattack that compromised the personal data of 147 million people[15]. The incident led to a $575 million settlement and caused irreparable reputational harm.

5.3 India's UPI and Phishing Epidemic

As India rapidly adopted UPI-based digital transactions, fraudsters exploited the system's popularity through phishing scams, impersonation, and malicious apps. According to the National Crime Records Bureau (NCRB), digital payment frauds in India surged by 30% in 2022 alone[16].

---

[11] National Crime Records Bureau, Cyber Crime Statistics Report (2023).

[12] *Ibid.*

[13] UNODC Cybercrime Database, 2023.

[14] *Supra* note 6.

[15] Equifax Breach Report, U.S. Federal Trade Commission (2019).

[16] NCRB Annual Cybercrime Report (2022).

Legal Aspects of Cyber Financial Crimes

Cyber financial crimes present a unique legal challenge, requiring a responsive and adaptive legal framework that can address the ever-evolving nature of digital offences. The legal response must balance technological advancement, individual rights, and national security. In India, a combination of statutory laws, regulatory guidelines, and judicial interpretations form the core of the legal regime addressing cyber financial crimes.

6.1. Statutory Framework in India

6.1.1. Information Technology Act, 2000

The **Information Technology Act, 2000 (IT Act)** is the principal legislation governing cyber activities in India. Enacted to provide legal recognition to electronic transactions, the Act also criminalizes various cyber offences, including those of a financial nature.

- **Section 43** penalizes unauthorized access to computer systems, downloading, or extracting data without consent, which is a common preliminary step in financial cyber frauds[17].
- **Section 66** makes hacking a punishable offence where dishonesty or fraud is involved[18].
- **Section 66C** penalizes identity theft, an act often used in phishing scams and digital wallet frauds[19].
- **Section 66D** specifically targets cheating by personation using computer resources[20].
- **Section 72A** deals with breach of confidentiality and privacy[21].

While the IT Act provides the foundational structure, critics argue that its provisions are vague, technologically outdated, and often incapable of dealing with advanced cyber financial crimes such as cryptocurrency frauds or cross-border scams.

6.1.2. Indian Penal Code, 1860 (IPC)

Traditional criminal provisions are also invoked in cyber financial crime cases. These include:

- **Section 420 IPC** (cheating and dishonestly inducing delivery of property)[22].
- **Section 406 IPC** (criminal breach of trust)[23].
- **Section 468 IPC** (forgery for the purpose of cheating)[24].

These sections are often read in conjunction with IT Act provisions during prosecution. However, procedural complexities and the lack of specialized cybercrime cells in every jurisdiction often delay effective implementation.

---

[17] Information Technology Act, 2000, s. 43.
[18] *Ibid*, s. 66.
[19] *Ibid*, s. 66C.
[20] *Ibid*, s. 66D.
[21] *Ibid*, s. 72A.
[22] Indian Penal Code, 1860, s. 420.
[23] *Ibid*, s. 406.
[24] *Ibid*, s. 468.

6.1.3. Substantive Criminal Provisions: Bharatiya Nyaya Sanhita, 2023

Under the new penal code, cyber financial frauds fall under several redefined and expanded sections:

1. **Section 318(4)** criminalises "cheating and dishonestly inducing delivery of property", a digital-era adaptation of the erstwhile Section 420 of IPC[25]. It is frequently invoked in phishing, UPI frauds, and deceptive online platforms.
2. **Section 336** addresses *forgery of documents and electronic records*, encompassing manipulation of e-invoices, QR codes, and blockchain logs[26]. This provision is crucial in curbing synthetic identity fraud and invoice-based tax scams.
3. **Section 344** targets *falsification of accounts*, including tampering with electronic ledgers[27]. It can be used against online betting platforms or fintech entities engaged in money laundering.
4. **Chapter XX** of BNS criminalizes *organized digital crimes* by syndicates. This enables law enforcement to prosecute large-scale cyber heists involving crypto wallets, ransomware groups, and mule account networks[28].

6.1.4. Procedural Changes: Bharatiya Nagarik Suraksha Sanhita, 2023

The BNSS introduces procedural modernization conducive to digital crimes:

1. **Section 532** enables full digitalization of criminal proceedings, allowing electronic FIRs, virtual hearings, and remote cross-examinations[29]. This ensures that geographically dispersed victims, especially in online banking frauds, can participate without logistical constraints.
2. The provision for **videography of search and seizure** supports admissibility and integrity of evidence collected from data centers or server farms during raids[30].
3. The new custody model allows **15-day custody at any stage within 60 days**, facilitating decryption of seized devices and real-time cooperation with CERT-In and RBI's Cyber Security Operations Center[31].

6.1.5. Evidentiary Reforms: Bharatiya Sakshya Adhiniyam, 2023

Digital evidence now enjoys parity with traditional evidence under the BSA:

1. **Section 63** accords *electronic records the status of primary documents*, provided the system integrity is proved via metadata, hash values, or chain-of-custody logs[32].
2. **Section 57** recognizes *digital signatures* as self-authenticating, enabling faster verification of forged transactions or digital contracts[33].

---

[25] Bharatiya Nyaya Sanhita, 2023, s. 318(4).
[26] *Ibid*., s. 336.
[27] Ibid., s. 344.
[28] Ibid., Chapter XX on Organised Crime.
[29] Bharatiya Nagarik Suraksha Sanhita, 2023, s. 532.
[30] BNSS, 2023, Chapter X: Search and Seizure Procedures.
[31] BNSS, s. 187 – Custody and Remand.
[32] Bharatiya Sakshya Adhiniyam, 2023, s. 63.
[33] Ibid., s. 57.

3. **Section 65 and 66** permit *expert certifications* from notified government cyber-forensic units like CERT-In and state cyber labs. This reduces reliance on slow and discretionary private expert reports[34].

6.1.6. Reserve Bank of India (RBI) Guidelines

The **RBI**, as the central banking authority, issues guidelines to regulate cybersecurity in the financial sector:

- The **Cyber Security Framework in Banks (2016)** mandates banks to develop cyber resilience and monitor unusual transactions in real time[35].
- The **Digital Payment Security Controls (2021)** instructs banks and non-bank financial companies to adhere to minimum security requirements for internet and mobile banking platforms[36].
- RBI's guidelines also provide grievance redressal mechanisms, including *Zero Liability* and *Limited Liability* provisions for digital fraud victims under its 2017 circular[37].

Despite these efforts, there is criticism that enforcement remains weak, especially concerning fintech startups and peer-to-peer lending platforms operating outside the regulatory perimeter.

6.2. International Legal Instruments

Since cyber financial crimes are transnational in nature, effective regulation requires international cooperation.

- The **Budapest Convention on Cybercrime, 2001**, although not signed by India, remains the most comprehensive treaty addressing global cybercrime and offers legal tools for extradition, search and seizure, and data preservation[38].
- The **United Nations Convention against Transnational Organized Crime (UNTOC)** offers a framework to tackle crimes involving criminal organisations using cyberspace for financial gains[39].

India's hesitancy in signing such treaties is driven by concerns of sovereignty and data privacy. However, participation in global legal frameworks can enhance cross-border investigation capabilities.

6.3. Judicial Interpretations

The Indian judiciary has gradually begun to engage with cybercrimes, although jurisprudence remains relatively underdeveloped.

- In *Shreya Singhal v. Union of India*, the Supreme Court struck down Section 66A of the IT Act for being vague and infringing on free speech. While the case was not about financial crimes, it underlined the need for clarity and precision in cyber legislation[40].

---

[34] Ibid., ss. 65–66; see also Ministry of Electronics and Information Technology (MeitY) Notification on "Cyber Forensic Examiners", 2024.

[35] Reserve Bank of India, *Cyber Security Framework in Banks*, RBI Circular, June 2016.

[36] RBI, *Digital Payment Security Controls – Directions for Banks and NBFCs*, Circular, Feb. 18, 2021.

[37] RBI, *Customer Protection – Limiting Liability of Customers in Unauthorized Electronic Banking Transactions*, Circular DBR.No.Leg. BC.78/09.07.005/2017-18, July 6, 2017.

[38] Council of Europe, *Convention on Cybercrime*, ETS No.185, Budapest, 23.XI.2001.

[39] United Nations, *United Nations Convention Against Transnational Organized Crime and the Protocols Thereto*, 2000.

[40] Shreya Singhal v. Union of India, AIR 2015 SC 1523.

- In *State of Tamil Nadu v. Suhas Katti*, one of India's first cybercrime convictions, the accused was sentenced for sending obscene messages via email. The court's reliance on digital evidence laid a precedent for future cyber trials[41].
- The Delhi High Court in *K. N. Govindacharya v. Union of India* dealt with data security issues, indirectly linking surveillance vulnerabilities with increased cyber risks in financial operations[42].

The absence of a cyber-specific judicial tribunal or fast-track courts has hampered timely justice, leaving victims of financial cyber frauds with limited recourse.

6.4. Enforcement Agencies and Institutional Mechanisms

Several agencies play a role in implementing cybercrime laws:

- The **Indian Computer Emergency Response Team (CERT-In)**, under the Ministry of Electronics and Information Technology, coordinates responses to cybersecurity incidents.
- **Cyber Crime Investigation Cells**, under state police departments, investigate cases under both IPC and IT Act provisions.
- **Financial Intelligence Unit (FIU-IND)** and **Enforcement Directorate (ED)** track suspicious transactions under the Prevention of Money Laundering Act, especially in digital asset fraud cases.

However, institutional gaps such as lack of trained personnel, technical infrastructure, and cross-border coordination continue to hinder effective enforcement.

Conclusion

In the age of digital transformation, where technological integration with financial services has become both inevitable and indispensable, the rise of cyber financial crimes presents a formidable challenge. As the financial sector continues to evolve with innovations such as blockchain technology, AI-driven fintech applications, and real-time global payment systems, the sophistication of cybercriminals has also evolved correspondingly. The landscape of financial crime is no longer confined to physical theft or fraud within banking halls; it now transcends physical boundaries and manifests in invisible, intangible, and complex digital threats that are capable of paralyzing entire economic ecosystems.

The economic consequences of cyber financial crimes are not merely confined to the immediate losses suffered by victims. These crimes have a cascading effect on national economies, investor confidence, the reputation of financial institutions, and the overall health of the digital financial ecosystem. The need for businesses to continuously invest in cybersecurity measures, coupled with rising cyber insurance premiums and compliance burdens, translates into increased costs that often get passed on to consumers. Furthermore, small businesses, lacking the resources to implement robust security infrastructure, remain disproportionately vulnerable, and often suffer existential threats due to a single successful cyberattack.

---

[41] State of Tamil Nadu v. Suhas Katti, CC No. 4680 of 2004, Metropolitan Magistrate, Egmore, Chennai.

[42] K. N. Govindacharya v. Union of India, W.P. (C) 3325/2012, Delhi High Court.

From a societal perspective, the consequences are equally grave. Victims of cyber financial crimes, especially those from economically weaker sections or with limited digital literacy, face not only financial ruin but also emotional and psychological trauma. The erosion of public trust in digital financial systems hampers progress towards financial inclusion and digital empowerment. Moreover, underreporting, inadequate law enforcement capacity, and jurisdictional hurdles in prosecution allow cybercriminals to operate with impunity, further entrenching a culture of digital lawlessness.

While legislative and regulatory frameworks exist, their efficacy is diluted by outdated provisions, bureaucratic inertia, and a reactive rather than proactive approach to enforcement. India's IT Act, for example, while pioneering in its inception, has not kept pace with newer forms of cyber threats such as AI-generated deepfakes, decentralised finance (DeFi) scams, and social engineering tactics. Globally, although treaties like the Budapest Convention provide a framework for cooperation, there is a pressing need for more inclusive, coordinated international efforts that address the cross-border nature of cybercrimes.

In light of these realities, the need for a comprehensive, multi-dimensional approach to combat cyber financial crimes cannot be overstated. This includes legislative reform, institutional capacity-building, public-private collaboration, awareness campaigns, and international cooperation. Most importantly, the state must adopt a rights-based approach that balances the need for robust cybersecurity with the protection of civil liberties and the promotion of digital inclusion.

In conclusion, the socio-economic impact of cyber financial crimes extends beyond monetary loss; it strikes at the very foundations of digital trust, governance, and social stability. Addressing this challenge requires not only technological solutions but also a holistic understanding of its human, legal, and systemic dimensions. Only through an integrated approach—anchored in awareness, accountability, and adaptive policy-making—can we safeguard the future of digital finance and ensure that the benefits of technology are equitably and securely shared.

CASE STUDIES ON HIGH-PROFILE FINANCIAL CRIMES AND THEIR LEGAL CONSEQUENCES

Laxmi Prasad Boda
Research Scholar,
University College of Law Osmania University

ABSTRACT

"In the digital age, Fraud is a crime that can be committed by anyone, anywhere, at any time. It is a crime that knows no boundaries."

High-profile financial crimes have significant implications for economies, businesses, and public trust, often leading to extensive legal repercussions. This abstract explores notable case studies, including the Enron scandal, the Bernie Madoff Ponzi scheme, and the 1MDB scandal, each illustrating the complexities of financial fraud and its far-reaching consequences.

The Enron scandal, which involved accounting fraud and corporate malfeasance, resulted in the bankruptcy of one of the largest companies in the U.S. and led to the dissolution of Arthur Andersen, one of the five largest audit and accountancy partnerships. This case prompted the Sarbanes-Oxley Act, which instituted stricter regulations on corporate governance and financial disclosures.

[1]Similarly, Bernie Madoff's Ponzi scheme, one of the largest in history, defrauded thousands of investors and resulted in a 150-year prison sentence for Madoff. This case highlighted the need for enhanced regulatory oversight and investor protection measures.

The 1MDB scandal, involving the embezzlement of billions from a Malaysian sovereign wealth fund, underscored the global nature of financial crime and the challenges of international law enforcement. These case studies collectively emphasize the necessity for robust regulatory frameworks and the ongoing evolution of legal responses to safeguard against financial misconduct.

Key words: *Financial Crimes, Legal Consequences, Corporate Fraud, Regulatory Frameworks, Accountability.*

Introduction

Financial crimes encompass a wide range of illicit activities, including fraud, money laundering, embezzlement, and insider trading. These crimes can have devastating effects on economies, eroding public trust in financial institutions and leading to significant financial losses. High-profile cases often attract media attention, revealing the vulnerabilities within financial systems and the challenges faced by regulatory authorities.

In India, several high-profile financial crimes have come to light in recent years, including the Nirav Modi and Vijay Mallya scandals.

These cases not only highlight the complexities of financial misconduct but also raise questions about the effectiveness of the legal frameworks in place to address such issues. Globally, cases like the Enron scandal, the Bernie Madoff Ponzi scheme, and the 1MDB scandal illustrate the far-reaching implications of financial crimes and the necessity for international cooperation in legal proceedings.

[1] **Cohen, L. (2010).** *The Madoff Chronicles: Inside the Secret World of Bernie Madoff's Ponzi Scheme*. New York: HarperCollins.

1.1 Financial crimes have emerged as a significant concern in the global economy, affecting not only the financial institutions involved but also the broader societal fabric. This study examines high-profile financial crimes, focusing on notable cases in India and around the world, and analyzes their legal consequences. By exploring the intricacies of these cases, the research aims to highlight the effectiveness of existing legal frameworks and the need for reforms to prevent future occurrences. The findings underscore the importance of international cooperation in combating financial crimes and the necessity for robust regulatory mechanisms to safeguard economic integrity.

This study aims to provide a comprehensive analysis of high-profile financial crimes, examining the legal consequences and the lessons learned from these incidents. The following sections will delve into specific case studies, exploring the legal frameworks involved and the broader implications for society.

Case Studies in India:

2.1 Nirav Modi and the PNB Scam:

The Nirav Modi case is one of the most notorious financial frauds in India, involving a complex scheme that exploited the internal processes of Punjab National Bank (PNB). The fraud came to light in early 2018, revealing that Modi, a prominent diamond jeweller, had orchestrated a scam worth approximately ₹14,000 crores (around $2 billion) through the issuance of fraudulent Letters of Undertaking (LoUs).

2.1.1 Background:

[2]Nirav Modi, who gained fame for his luxury jewellery brand, allegedly colluded with bank officials to secure loans without proper collateral. The scam involved the issuance of LoUs, which are guarantees provided by banks to facilitate overseas credit. By manipulating the bank's internal controls, Modi was able to obtain these guarantees without the necessary approvals.

The modus operandi of the scam involved a network of companies owned by Modi and his uncle, Mehul Choksi. They created a web of transactions that obscured the true nature of the loans and the financial health of their businesses. The fraudulent LoUs were issued without the knowledge of the bank's core banking system, allowing them to bypass standard checks and balances.

2.1.2 Legal Proceedings:

Following the revelation of the fraud, the Indian government initiated investigations led by the Central Bureau of Investigation (CBI) and the Enforcement Directorate (ED). Modi fled India shortly before the scam was exposed, prompting the Indian authorities to issue a Red Corner Notice through Interpol for his arrest.

In 2019, the Indian government filed a case against Modi under the Prevention of Money Laundering Act (PMLA) and the Indian Penal Code (IPC). The legal proceedings have been complicated by Modi's extradition from the United Kingdom, where he was arrested in 2019. The UK courts have been involved in determining the

[2] Ghosh, S.. "Nirav Modi and the PNB Scam: A Case Study" 53(12) *Economic and Political Weekly*, 45-50 (2018).

legality of the extradition request, with arguments presented regarding the fairness of the Indian legal system and the potential for a fair trial.

The case has raised questions about the effectiveness of international legal cooperation and the challenges of extraditing high-profile fugitives. The Indian government has emphasized the need for stringent measures to prevent such financial crimes in the future, including reforms in banking regulations and enhanced scrutiny of financial transactions.

2.2 Vijay Mallya and Kingfisher Airlines:

Vijay Mallya, the former chairman of United Breweries Group, became synonymous with financial mismanagement and corporate fraud following the collapse of Kingfisher Airlines. The airline, which was once a prominent player in the Indian aviation sector, defaulted on loans amounting to approximately ₹9,000 crores (around $1.3 billion), leading to its eventual shutdown in 2012.

2.2.1 Background:

[3]Mallya's lavish lifestyle and high-profile persona masked the financial troubles of Kingfisher Airlines. The airline faced operational challenges, including mismanagement and mounting debts, which ultimately led to its downfall. Mallya's inability to repay loans taken from various banks raised concerns about corporate governance and accountability.

The airline's financial woes were exacerbated by a combination of factors, including rising fuel prices, intense competition, and regulatory challenges. Mallya's management decisions, including aggressive expansion and high operational costs, contributed to the airline's unsustainable business model.

2.2.2 Legal Proceedings:

In 2016, the Indian government initiated legal action against Mallya, accusing him of financial fraud and money laundering. The Enforcement Directorate filed a case under the PMLA, and Mallya was declared a "fugitive economic offender" in 2019. He fled to the United Kingdom, where he has been fighting extradition to India.

The legal proceedings against Mallya have highlighted the challenges of recovering debts from high-profile individuals and the complexities of international law. The Indian government has sought to strengthen its legal framework to address such cases, emphasizing the need for stricter regulations in corporate governance.

Mallya's case has also sparked debates about the accountability of corporate leaders and the responsibilities of financial institutions in lending practices. The fallout from the Kingfisher Airlines debacle has prompted calls for reforms in the aviation sector and greater oversight of corporate governance.

[3] *Enforcement Directorate v. Vijay Mallya*, Westminster Magistrates' Court, London (2020).

Global Case Studies:

3.1 Enron Scandal (USA):

The Enron scandal, which came to light in 2001, is one of the largest corporate frauds in history. Enron Corporation, once a leading energy company, engaged in accounting fraud to hide its financial losses, leading to its bankruptcy and significant legal reforms in the United States.

3.1.1 Background:

[4]Enron used complex financial structures and accounting loopholes to inflate its profits and hide debts. The company's executives misled investors and analysts, creating a false image of financial stability. When the fraud was uncovered, Enron's stock plummeted, resulting in massive losses for shareholders and employees.
The scandal involved the use of special purpose entities (SPEs) to conceal debt and inflate profits. Enron's accounting firm, Arthur Andersen, was complicit in the fraud, providing misleading financial statements that obscured the company's true financial condition.

3.1.2 Legal Proceedings: The fallout from the Enron scandal led to the indictment of several top executives, including CEO Jeffrey Skilling and Chairman Kenneth Lay. The legal proceedings resulted in convictions for fraud and conspiracy, with Skilling sentenced to 24 years in prison.

The scandal also prompted significant regulatory changes, including the Sarbanes-Oxley Act of 2002, which aimed to enhance corporate governance and accountability. The Act introduced stricter regulations for financial reporting and increased penalties for corporate fraud.

The Enron scandal underscored the need for greater transparency in financial reporting and the importance of ethical conduct in corporate leadership. It also highlighted the role of auditors in ensuring the integrity of financial statements and the need for independent oversight of financial practices.

3.2 Bernie Madoff Ponzi Scheme (USA):

The Bernie Madoff Ponzi scheme is one of the largest and most infamous financial frauds in history. Madoff, a former chairman of NASDAQ, orchestrated a massive Ponzi scheme that defrauded thousands of investors out of billions of dollars over several decades.

3.2.1 Background

Madoff's investment firm promised consistent, high returns to investors, which attracted a large number of clients. However, instead of generating profits through legitimate investments, Madoff used the money from new investors to pay returns to earlier investors, creating the illusion of a profitable business.

The scheme began to unravel during the financial crisis of 2008 when Madoff was unable to meet withdrawal requests from investors. As a result, he confessed to his sons that the investment business was a fraud, leading to his arrest on December 11, 2008.

3.2.2 Legal Proceedings

Madoff was charged with multiple counts of fraud, including securities fraud, investment advisor fraud, and money laundering. In March 2009, he pleaded guilty to 11 felony counts and was sentenced to 150 years in prison. The legal proceedings against Madoff also involved efforts to recover funds for defrauded investors. The court-

[4] Klein, A. , "The Enron Scandal: Lessons Learned." 154(3) *Journal of Business Ethics*, 1-15 (2019).

appointed trustee, Irving Picard, has been working to recover assets and distribute them to victims of the scheme. As of 2021, billions of dollars have been recovered, but many investors have still not received full restitution.

The Madoff case has prompted discussions about the need for stronger regulatory oversight in the financial industry and the importance of investor education to prevent similar frauds in the future.

3.3 1MDB Scandal (Malaysia): [5]The 1Malaysia Development Berhad (1MDB) scandal is one of the largest financial frauds in history, involving the embezzlement of billions from a Malaysian government fund. The scandal implicated high-ranking officials, including former Prime Minister Najib Razak, and raised concerns about corruption and governance in Malaysia.

3.3.1 Background:

1MDB was established in 2009 to promote economic development in Malaysia. However, it became a vehicle for massive corruption, with billions of dollars misappropriated for personal gain by officials and their associates. The funds were allegedly used to finance luxury purchases, including real estate and artwork.

The scandal came to light in 2015 when investigative journalists began uncovering irregularities in the fund's financial dealings. The revelations sparked widespread outrage and led to calls for accountability from the Malaysian government.

3.3.2 Legal Proceedings:

The scandal led to investigations in multiple countries, including the United States, Switzerland, and Singapore. In 2018, Najib Razak was arrested and charged with corruption and money laundering. The legal proceedings have highlighted the challenges of prosecuting high-profile individuals and the need for international cooperation in addressing financial crimes.

The U.S. Department of Justice (DOJ) launched an investigation into the misappropriation of 1MDB funds, resulting in the seizure of assets worth over $1 billion, including luxury properties and artworks. The DOJ's actions underscored the global nature of financial crimes and the importance of cross-border collaboration in investigations.

The 1MDB scandal has prompted calls for reforms in Malaysia's governance and regulatory frameworks, emphasizing the importance of transparency and accountability in public institutions. The case has also raised questions about the effectiveness of anti-corruption measures and the need for stronger legal frameworks to combat financial crimes.

Legal Frameworks and Consequences:

4.1 Regulatory Responses in India:

In response to the increasing prevalence of financial crimes, the Indian government has implemented various legal frameworks aimed at enhancing accountability and preventing fraud. Key regulations include:

4.1.1 Prevention of Money Laundering Act (PMLA):

[6]The PMLA, enacted in 2002, aims to prevent money laundering and provide for the confiscation of property derived from criminal activities. The Act empowers law enforcement agencies to investigate and prosecute money laundering offenses, enhancing the government's ability to combat financial crimes.

---

[5] Davis, K. (2019) "The 1MDB Scandal: A Case Study in Corruption." 40(2) *Harvard International Review*, 34-39.

[6] Prevention of Money Laundering Act, 2002.

The PMLA has been instrumental in addressing financial crimes, providing a legal framework for the investigation and prosecution of money laundering offenses. The Act mandates reporting requirements for financial institutions and establishes a framework for the identification and tracking of proceeds of crime.

4.1.2 Insolvency and Bankruptcy Code (IBC):

[7]The IBC, introduced in 2016, provides a framework for the resolution of insolvency and bankruptcy cases. The Code aims to streamline the process of recovering debts and protecting the interests of creditors, thereby enhancing the accountability of corporate entities.

The IBC has been a significant step towards improving the ease of doing business in India, providing a time-bound process for the resolution of insolvency cases. The Code has also facilitated the recovery of dues for creditors, promoting financial discipline among corporate entities.

4.2 International Legal Frameworks:

International cooperation is crucial in addressing financial crimes, particularly in cases involving cross-border transactions. Key frameworks include:

4.2.1 United Nations Convention against Corruption:

[8]The United Nations Convention against Corruption, adopted in 2003, aims to promote international cooperation in combating corruption and financial crimes. The Convention provides a framework for countries to enhance their legal and regulatory frameworks, facilitating cross-border investigations and prosecutions.

The Convention emphasizes the importance of preventive measures, including the establishment of effective legal frameworks and the promotion of transparency and accountability in public institutions. It also encourages international cooperation in the investigation and prosecution of corruption-related offenses.

4.2.2 Financial Action Task Force (FATF):

The FATF is an intergovernmental organization that sets standards for combating money laundering and terrorist financing. The FATF's recommendations provide a framework for countries to strengthen their legal and regulatory measures, enhancing global efforts to combat financial crimes.

The FATF conducts regular evaluations of member countries' compliance with its recommendations, promoting accountability and transparency in financial systems. The organization's work has been instrumental in fostering international cooperation in the fight against financial crimes.

Case Laws:

5.1 Nirav Modi Case:

In the case of Nirav Modi, the Indian courts have been involved in various proceedings related to the extradition request made by the Indian government. The Westminster Magistrates' Court in London has been hearing the extradition case, with arguments presented regarding the fairness of the Indian legal system and the potential for a fair trial. The case has highlighted the complexities of extradition law and the challenges of prosecuting financial crimes across borders.

---

[7] Insolvency and Bankruptcy Code, 2016.

[8] United Nations Convention against Corruption, 2003.

5.2 Vijay Mallya Case:

The case of Vijay Mallya has also seen significant legal developments, with the UK courts involved in determining the legality of the extradition request. Mallya was declared a "fugitive economic offender" under the Fugitive Economic Offenders Act, 2018, which allows for the confiscation of properties of individuals who flee the country to evade legal proceedings. The legal proceedings have raised questions about the adequacy of existing laws in addressing financial crimes and the need for reforms to enhance accountability.

5.3 Enron Scandal:

[9]The Enron scandal led to numerous legal proceedings against top executives, including Jeffrey Skilling and Kenneth Lay. The case resulted in significant convictions for fraud and conspiracy, with Skilling sentenced to 24 years in prison. The legal outcomes of the Enron scandal prompted widespread reforms in corporate governance and financial reporting, including the enactment of the Sarbanes-Oxley Act.

5.4 Bernie Madoff Ponzi Scheme:

The legal proceedings against Bernie Madoff involved multiple charges, including securities fraud, investment advisor fraud, and money laundering. Madoff's guilty plea in 2009 resulted in a 150-year prison sentence. The case also led to extensive civil litigation as the court-appointed trustee sought to recover funds for defrauded investors. The Madoff case has prompted discussions about the need for stronger regulatory oversight in the financial industry and the importance of investor education to prevent similar frauds in the future.

5.5 1MDB Scandal:

The 1MDB scandal has seen legal actions taken in multiple jurisdictions, with investigations conducted by the U.S. Department of Justice, Swiss authorities, and others. The legal proceedings have resulted in the seizure of assets and ongoing investigations into the roles of various individuals and institutions involved in the scandal. The case has underscored the need for international cooperation in addressing financial crimes and the complexities of prosecuting high-profile individuals.

Conclusion:

High-profile financial crimes pose significant challenges to legal systems worldwide, highlighting the need for robust regulatory frameworks and international cooperation. The case studies examined in this research underscore the complexities of prosecuting financial misconduct and the importance of accountability in corporate governance.

As financial crimes continue to evolve, it is imperative for governments and regulatory authorities to adapt their legal frameworks to address emerging threats. By learning from past incidents and implementing effective measures, societies can work towards safeguarding economic integrity and restoring public trust in financial institutions.

6.1 Final Thoughts:

The analysis of high-profile financial crimes reveals a pressing need for comprehensive reforms in legal frameworks and regulatory practices. The cases of Nirav Modi, Vijay Mallya, Enron, Bernie Madoff, and 1MDB serve as stark reminders of the vulnerabilities within financial systems and the potential for abuse by individuals in positions of power.

---

[9] **Klein, A. (2019).** "The Enron Scandal: Lessons Learned." *Journal of Business Ethics*, 154(3), 1-15.

To combat financial crimes effectively, it is essential to foster a culture of transparency and accountability within organizations and financial institutions. This includes implementing stringent compliance measures, enhancing oversight mechanisms, and promoting ethical conduct among corporate leaders.

Furthermore, international cooperation is crucial in addressing the global nature of financial crimes. Countries must work together to strengthen legal frameworks, share information, and coordinate investigations to ensure that perpetrators are held accountable, regardless of their location.

Ultimately, the fight against financial crimes requires a multi-faceted approach that combines legal, regulatory, and societal efforts. By prioritizing integrity and accountability, societies can build resilient financial systems that protect the interests of all stakeholders and contribute to sustainable economic growth.

ENVIRONMENTAL CRIMES AS SOCIO-ECONOMIC OFFENCES: A LEGAL ANALYSIS IN THE CONTEXT OF SUSTAINABLE DEVELOPMENT

Keerthana PD
LLM Student, CSI Law College, MG University

ABSTRACT

The Bhopal Gas Tragedy of 1984, the most catastrophic industrial accidents in history, revealed the horrific effects of environmental disregard as well as the profound socio-economic ramifications of corporate wrongdoing. Countless individuals lost their lives, and future generations still endure chronic health issues, poverty, and displacement-highlighting that environmental crimes are not merely infractions against nature; but are serious offenses against society and progress. Environmental offenses, including illegal mining, hazardous waste disposal, deforestation, and pollution from industries, frequently cause excessive damage to marginalized communities, deplete natural resources, and jeopardize the health and well-being of populations. These illegal activities endanger food security, public health, and economic stability-fundamental aspects of sustainable development-leading to enduring social and economic challenges. Although there exist environmental regulations in place, the insufficient enforcement, and the perception of these actions as simple regulatory oversights enable violators to avoid genuine responsibility. This article contends that environmental offenses should be reclassified and treated as socio-economic crimes, considering their potential to hinder sustainable development objectives and the development of the nation. Through the examination of legislation and sustainable development initiatives, and recognizing the difficulties in tackling environmental crime as a socio-economic offense, this article emphasizes the critical necessity of integrating environmental safeguarding into the wider goals of socio-economic fairness and sustainable advancement by giving various legal and policy recommendations that can foster the overall national development.

Key words: *Environment, Crimes, Enforcement, Sustainable Development, Socio-Economic.*

Introduction

"We are the first generation to feel the effect of climate change and the last generation who can do something about it," American President Barack Obama, during his address at United Nations Climate Change Summit on September 23, 2014, in New York City[1], attributed this statement, emphasizing the urgency of addressing climate change, indeed a by-product of environmental crime.

Environmental crime encompasses unlawful activities that directly damage the environment, including illegal logging, pollution, trafficking of wildlife, and improper waste disposal. These violations are not just environmental concerns, but they also have significant socio-economic repercussions. They hinder sustainable development, which can be defined as a development approach that meets the needs of the present generation without compromising the ability of future generations to meet their own needs. Further they disrupt the livelihoods of rural and indigenous populations, and place a strain on public health services. Environmental crime, commonly defined as the unlawful use or devastation of natural assets, goes beyond ecological limits and profoundly influences both social structures and economic systems and hence these crimes can be coined in the ambit of socio-economic offences as these activities frequently breaches various environmental regulations and laws, enabling wrongdoers to profit economically while transferring the environmental and human

[1] **Cohen, L. (2010).** *The Madoff Chronicles: Inside the Secret World of Bernie Madoff's Ponzi Scheme*. New York: HarperCollins.

repercussions. The social aspect of these crimes becomes apparent when we consider their disproportionate impact on vulnerable and marginalized groups. Communities reliant on natural resources for their livelihoods including farmers, fishermen, indigenous populations, and economically disadvantaged urban residents, experience displacement, health risks, and economic hardship as a result of environmental degradation.

For example, the illegal disposal of hazardous waste or air pollution from unregulated industries can lead to chronic health issues, contaminate water sources, and ruin agricultural land, resulting in enduring socio-economic challenges. Furthermore, environmental crimes impose financial strains on public health systems, hinder workforce productivity, and impede national progress by damaging essential ecosystems and infrastructure. They also contribute to global challenges like climate change, which exacerbates poverty, food scarcity, and forced migration. Moreover, numerous environmental offenses are associated with organized crime and corruption, weakening governance and legal frameworks. Considering the intertwining of economic exploitation, social inequality, and environmental damage, it is evident that environmental crime is well resonating into the cluster of socio-economic offences which is generally defined as any crime, committed with the intention of gaining financial or material benefit, which causes harm not just to individuals but to society and the economy at large[2].

Protecting the environment is of vital importance both nationally and globally, serving as a fundamental element for sustainable development, ecological harmony, and public health. At the national level, safeguarding the environment guarantees the preservation of natural resources that are crucial for a country's economic development, agricultural efficiency, energy stability, and public welfare. In developing countries like India, where many people rely on natural resources for their livelihoods, environmental degradation directly obstructs national development objectives such as reducing poverty, enhancing health, and advancing infrastructure. Furthermore, unrestrained industrial growth, deforestation, and pollution not only harm ecosystems but also strain healthcare systems and diminish quality of life. On a global scale, environmental protection plays a critical role in addressing climate change, conserving biodiversity, and avoiding ecological crises that cross national borders. Problems such as increasing sea levels, severe weather patterns, and worsening air and water quality go beyond national limits and necessitate international collaboration and regulatory frameworks. Therefore, incorporating environmental protection into national policy is not merely an ecological duty but a strategic investment in economic resilience, social fairness, and worldwide peace. A nation's dedication to environmental sustainability signifies its responsibility towards both its citizens and the global community.

Environment Crime as a Socio-Economic Crime

Socio-economic offenses refer to illegal activities that adversely impact the social and economic welfare of people, communities, or the government. Unlike traditional crimes, which often involve physical injury or violence, socio-economic offenses are generally non-violent and committed for financial benefit, typically characterized by deceit, misuse of power, or breaches of regulations. Examples of these offenses include corruption, tax fraud, money laundering, false representation, hoarding, black market activities, and environmental violations. They often threaten economic stability, diminish public confidence in institutions, and

[2] Pradeep Kumar Singh, Socio-Economic Crimes: Analysis of Causation, (2022) 8(II) Athens Journal of Law 237, 336 (Athens Journal of Law, July 2022), available at: https://www.athensjournals.gr/law (last accessed 13 June 2025).

exacerbate social inequalities[3]. Due to their involvement with powerful individuals, corporations, or organized groups, socio-economic offenses can be challenging to identify and prosecute. Their effects are far-reaching, influencing the economy, governance, and the rights and well-being of everyday citizens. As a result, they are taken seriously by the legal system and necessitate rigorous enforcement, regulatory scrutiny, and public responsibility.

The environmental crimes can be undoubtedly grouped into the pact of socio-economic crimes and its traces can be found in the very nature of these crimes. The nature of environmental offenses is intricate, diverse, and frequently spans international boundaries, involving unlawful actions that either directly or indirectly jeopardize the environment and breach environmental regulations. These offenses are defined by deliberate, careless, or reckless behaviors that lead to considerable harm to natural resources, including air, water, land, and biodiversity. They can be perpetrated by individuals, organized crime groups, corporations, or even government entities, often motivated by financial profit, regulatory loopholes, and inadequate enforcement measures. The environment crimes can be seen in various forms such as, air pollution comprising of unlawful emissions from industrial facilities, automobiles, or incineration processes that surpass allowable limits, along with the illicit discharge of hazardous gases such as sulfur dioxide or chlorofluorocarbons, are significant issues. Intentional incineration of dangerous waste or agricultural residuals, particularly within industrial or farming contexts, is also categorized as air-related environmental offenses, resulting in respiratory diseases, acid rain, and impacts on climate change. Water pollution crimes involving the release of untreated sewage, industrial waste, or chemical pollutants into bodies of water like rivers, lakes, or oceans. Unlawful oil spills, disposal of plastic waste, and the pollution of groundwater with toxic substances are frequent occurrences. These activities endanger marine and freshwater ecosystems, negatively affect aquatic organisms, and jeopardize sources of drinking water. The land degradation and waste disposal offences culminate a set of offences including unlawful mining activities, deforestation, land intrusion, and the incorrect disposal of hazardous or biomedical materials pose significant risks. Landfills that operate without following environmental guidelines can release harmful substances into the soil and water supplies, impacting agriculture and public health[4]. Uncontrolled sand mining further weakens riverbanks and contributes to erosion. Crime against biodiversity and wildlife are another set of illegal activities such as poaching, unlawful wildlife commerce, unauthorized timber harvesting, and the destruction of safeguarded environments contribute to the extinction of species, disturb ecosystems, and breach international agreements like CITES[5]. Crimes against biodiversity also support illicit markets and can be connected to larger criminal syndicates, which include trafficking and corruption.

These environmental crimes significantly jeopardize public health, resulting in a rise in respiratory conditions, waterborne illnesses, and exposure to harmful substances, particularly among marginalized and low-income communities. This imposes a considerable strain on public healthcare systems and diminishes workforce efficiency. Practices that harm the environment also interfere with agricultural operations by depleting soil quality and polluting water supplies, thereby endangering food security and the livelihoods of rural populations. In areas reliant on tourism and biodiversity, such as forest reserves or coastal regions, illegal activities like

[3] Durga Bhardwaj, Socio-economic Offences and Its Ground Level Reality, (2023) 6(II) International Journal of Law Management & Humanities 2292, 2298, available at: https://www.ijlmh.com/publications/volume-vi-issue-ii/ (last accessed 13 June 2025).

[4] Linert Lireza & Gentian Koçi, Environmental Crimes: Their Nature, Scope, and Problems in Identification, 10(1) S1 Interdisciplinary Journal of Research and Development 237 (2023), *available at*: https://www.journaluamd.org/index.php/IJRD/article/view/247(last accessed 13 June 2025).

[5] The Convention on International Trade in Endangered Species.

logging, poaching, and pollution reduce the appeal of natural attractions, leading to substantial economic downturns and job losses. Furthermore, the exhaustion of natural resources due to illegal mining or lack of regulation in industrial practices creates long-term economic uncertainty and disparity, exacerbating the divide between the affluent and the impoverished. These offenses also encourage corruption and undermine the rule of law, diminishing public confidence in institutions. Consequently, environmental crimes are not just ecological concerns but are fundamentally intertwined with socio-economic challenges that require immediate policy intervention and inclusive strategies for sustainable development.

Idea of Sustainable Developmental and Environment Justice

Sustainable development is an all-encompassing idea that highlights the importance of achieving economic and social progress in a way that does not exhaust natural resources or inflict irreversible damage on the environment. The concept gained prominence through the Brundtland Commission Report[6], which described sustainable development as "development that fulfills the needs of the present without jeopardizing the capacity of future generations to satisfy their own needs." It promotes a balanced strategy that incorporates three fundamental pillars namely economic Sustainability, fostering long-term economic growth while preserving environmental resources, Social Sustainability, guaranteeing fairness, social inclusion, and equity for all communities, including those that are marginalized and environmental Sustainability, Safeguarding ecosystems, biodiversity, and natural resources to uphold ecological balance[7]. The Sustainable development advocates for the mindful use of resources, minimizing waste and pollution, utilizing renewable energy, and implementing inclusive policies aimed at alleviating poverty and inequality.

In this era of the world witnessing alarming rise in the environmental crimes, degrading the planet's natural ecosystem and threatening the survival of millions of species including humans, the idea of sustainable development has become an urgent global necessity rather than a developmental goal. One of the most urgent reasons for embracing sustainable development is the swift exhaustion of natural resources. Forests are being cleared at an alarming pace, waterways are tainted with hazardous industrial waste, and the consumption of fossil fuels continues to escalate. These actions jeopardize the Earth's capacity to regenerate and sustain ecological equilibrium. Sustainable development advocates for responsible consumption, the promotion of renewable energy, and the conservation of natural resources, ensuring that future generations inherit a viable planet[8]. Furthermore, climate change, primarily fueled by unsustainable human practices, has surfaced as a significant global menace. Rising sea levels, severe weather occurrences, and frequent natural disasters are directly associated with the environmental exploitation resulting from unlawful and careless activities. Sustainable development offers a framework for integrating climate initiatives with economic and social policies, promoting low-carbon growth, reforestation efforts, and adaptation techniques. Environmental crimes possessing a deeper socio-economic context, disproportionately impact marginalized and vulnerable populations. The illegal

---

6 Iris Borowy, The Brundtland Commission: Sustainable Development as Health Issue, 10 Michael 198 (2013) https://www.michaeljournal.no/article/2013/03/The-Brundtland-Commission-Sustainable-development-as-health-issue (last visited 15 June 2025).

7 United Nations, Transforming Our World: The 2030 Agenda for Sustainable Development, A/RES/70/1, United Nations General Assembly (2015), https://sustainabledevelopment.un.org/post2015/transformingourworld (last visited 15 June 2025).

8 Anna Pros kova Anna Proskova, Embracing Sustainable Development is an Ethical Decision, 2015/01 CRIS Bulletin 61 (2015), available at: https://archive.sciendo.com/CRIS/cris.2015.2015.issue-1/cris-2015-0006/cris-2015-006.pdf (last visited 15 June 2025).

dumping of waste in impoverished regions, excessive resource extraction from indigenous territories, and the denial of clean air and water to disadvantaged groups contribute to environmental injustice. With its focus on equity and inclusion, sustainable development seeks to rectify these disparities by advocating for fair access to resources, participatory governance, and environmental rights for every citizen. Moreover, environmental crimes frequently involve organized criminal groups, corruption, and insufficient enforcement of environmental regulations. These systemic challenges impede national development by undermining the rule of law and reallocating resources away from education, healthcare, and infrastructure, thereby promoting institutional transparency, legal accountability, and international collaboration, making it an essential approach to combat environmental crimes on both national and global fronts[9].

Further, keeping the idea of sustainable development in the right track will lead to a healthy and stable environment, which is necessary for the survival of humanity and the continuity of social and economic progress by facilitating the effective utilization of resources like water, air, soil, and forests, making sure that these resources are neither overused nor contaminated, while also permitting them to recover and stay accessible for future generations. Environmental protection through sustainable development also, safeguarding the environment aids in alleviating the harmful impacts of climate change, an important objective of sustainable development. This involves lowering greenhouse gas emissions, preserving forests, and supporting green infrastructure, wholly contributing to a better public health thus supporting the social dimension of sustainable development.

Current Legal Status of Environment Protection

India, known for its rich biodiversity and large population reliant on natural resources, has developed a strong legal framework to address environmental offenses and encourage sustainable development. Several national laws are designed to safeguard air, water, land, forests, and wildlife from damage, overuse, and pollution resulting from unlawful or careless human actions.

One of the earliest and most important pieces of legislation is the Environment (Protection) Act, 1986, which was enacted in response to the Bhopal Gas Tragedy. It acts as comprehensive legislation, granting the central government the authority to take necessary actions to safeguard and enhance the environment. This act lays the groundwork for establishing environmental quality standards, regulating hazardous materials, and penalizing offenders. The Act was enacted under Article 253 of the Indian Constitution to implement the commitments made during the United Nations Conference on the Human Environment at Stockholm, 1972, where India agreed to undertake concrete actions for environmental protection. It addresses the shortcomings of previous legislation such as the Water Act of 1974 and the Air Act of 1981. It grants extensive powers to the central government to take necessary actions to safeguard and enhance environmental quality, as well as to prevent, control, and mitigate pollution. The notable features of the Act include, authorizing the Central Government to establish environmental standards, oversee the management of hazardous substances, and suspend or ban activities that

[9] Derica Lambrechts, "Environmental Crime in Sub-Saharan Africa – A Review and Future Challenges", Politikon: South African Journal of Political Studies, Vol. 43, No. 2 (2016), pp. 155–158, available at: https://www.tandfonline.com/doi/full/10.1080/02589346.2016.1213692(last visited 15 June 2025).

pose risks to the environment, provisions to establish protocols and safeguards to avert accidents involving hazardous materials, the capacity to appoint officials, issue directives, and impose penalties, which may include imprisonment of up to five years and financial fines for breaches[10]. The Act also lays the foundation for several environmental regulations and notifications, including the EIA Notification 2006, Hazardous Waste Rules, and Noise Pollution Rules. Another particularly progressive element of the Act is that it permits public involvement i.e. any individual can approach the courts to enforce environmental regulations, provided a notice of 60 days is given to the relevant authorities. In spite of its advantages, the Environment Protection Act has encountered challenges in its implementation and enforcement, mainly due to bureaucratic delays, insufficient awareness, and limited resources. Nevertheless, it remains a fundamental component of India's environmental legal framework, enabling a broad spectrum of administrative and legal measures to combat pollution, environmental harm, and ecological damage.

The Water Prevention and Control of Pollution Act, 1974, along with the Air Prevention and Control of Pollution Act, 1981, represents significant environmental legislation in India aimed at combating pollution and safeguarding public health and natural ecosystems. These laws were some of the first legislative measures implemented by the Indian government for the purpose of environmental protection. These legislations, focus on controlling pollution in water bodies and the air, respectively. These statutes led to the formation of the CPCB[11] and SPCBs[12], which oversee, regulate, and enforce pollution control standards[13]. The Act grants these boards the authority to examine sewage and industrial waste, uphold pollution control regulations, and take legal action against offenders. It bars the release of hazardous substances into water bodies without prior approval and outlines penalties that can include jail time and fines.

In a similar vein, the Air Act of 1981 was enacted to address, manage, and diminish air pollution. This Act acknowledges that air pollution is a significant environmental and public health dilemma, primarily stemming from industrial emissions, vehicle exhaust, and the combustion of fossil fuels. It enhances the capabilities of the CPCB and SPCBs to assess air quality, set air quality benchmarks, and control emissions from factories and vehicles. Furthermore, the Act permits state governments to designate specific areas as zones for air pollution control, where more stringent standards and regulations are enforced. Both Acts are essential in governing environmental issues in India. They lay down a legal framework for controlling pollution, penalizing offenders, and enhancing public awareness. However, their success often relies on the robustness of enforcement, cooperation among various agencies, and the political determination to take action against influential polluters.

The Wildlife Protection Act of 1972 is a significant law in India focused on the conservation and safeguarding of wild animals, birds, and plants. Passed by Parliament, it was introduced at a time when wildlife in India faced severe dangers from rampant hunting, loss of habitat, and illegal trafficking. The Act establishes an extensive

---

[10] Anirban Dhulia and Rajiv Ganguly, "Critical Assessment of Existing Environmental Legislation and Policies in India-Its Benefits, Limitations, and Enforcement", in Handbook of Environmental Materials Management, C. M. Hussain (ed) (Springer, 2018), pp. 1–4. available at: https://link.springer.com/referenceworkentry (last visited 15 June 2025).

[11] Central Pollution Control Board.

[12] State Pollution Control Boards.

[13] Prakash Chand, "Environmental Protection and Regulations in India: Role of the Central Pollution Control Board", Indian Journal of Public Administration, Vol. 64, No. 3 (2018), pp.4, available at: https://doi.org/10.1177 (last Visited 15 June 2025).

legal foundation for protecting biodiversity and maintaining the rich ecological legacy of the nation. It facilitates the establishment of protected regions like national parks and wildlife sanctuaries, along with imposing severe penalties for offenses against wildlife. One of the main aspects of the Act is the establishment of a network of Protected Areas, which encompasses National Parks, Wildlife Sanctuaries, Conservation Reserves, and Community Reserves. These regions are legally protected from any activities that could endanger the habitats or species that inhabit them. The Act also establishes the WCCB[14] to oversee and combat illegal poaching and trafficking of wildlife and animal products. The Wildlife Act defines schedules I to VI that classify animals and plants according to the level of protection they need. Species listed in Schedule I and II, such as tigers and elephants, are granted the highest level of protection, with any violations resulting in severe penalties, including imprisonment and substantial fines[15]. The Act prohibits the hunting of wild animals unless it is conducted for scientific research, education, or population management under government oversight. Over the years, multiple amendments have reinforced the Act, including harsher penalties for poachers and increased protection for additional species. It also fosters community involvement and acknowledges the importance of local and tribal communities in wildlife conservation efforts.

Despite its advantages, issues such as habitat encroachment, human-wildlife conflict, and inadequate enforcement remain significant challenges. Nonetheless, the Wildlife Protection Act, 1972 continues to be a vital component of India's environmental laws and has played a crucial role in the preservation and recovery of numerous endangered species.

The Forest Conservation Act, 1980 is a significant law passed by the Government of India aimed at protecting the nation's forest resources. Acknowledging the concerning speed at which forests were being destroyed for numerous developmental activities, this Act was implemented to curb deforestation and promote the sustainable management of forest land. The Act, governs the conversion of forest land for purposes other than forestry and mandates that such actions receive approval from the central government. Its goal is to preserve ecological equilibrium and avert deforestation. By consolidating decision-making authority, the Act seeks to ensure consistency and avert arbitrary forest destruction by state governments or private organizations. The Act also grants the government the power to regulate and oversee any activities that could result in forest degradation. It requires compensatory afforestation in cases where forest land is converted for development projects. This stipulation means that developers must plant additional trees to counterbalance the loss of forest area, thus fostering ecological harmony. Over time, the Forest Conservation Act has been instrumental in controlling deforestation and promoting the sustainable management of forest ecosystems. It has been bolstered by later policies and amendments designed to enhance forest governance and boost public involvement in forest conservation[16].

---

[14] Wildlife Crime Control Bureau.

[15] Ranjan Chatterjee and Saumya Seal, “Empowering or Encumbering? An Insight into the Impact of the Wildlife (Protection) Act of 1972 on Denotified, Nomadic, and Semi-Nomadic Tribes of India”, Impact and Policy Research Review (IPRR), Vol. 3, Issue 1 (Jan–June 2024), p. 64, available at: https://iprr.impriindia.com/wp-content/uploads/2024/07/PP2-Empowering-or-Encumbering-IPRR-V3_I1.pdf (last visited 15 June 2025).

[16] “Forest Conservation Act in India: Objectives, Key Provisions & Legal Framework for Environmental Protection”, Law Blend (Apr 2025), available at: https://lawblend.com/articles/forest-conservation-act-in-india (last visited 15 June 2025).

The Public Liability Insurance Act, 1991 and the National Green Tribunal Act, 2010 contribute further to the environmental legal framework. The former is an important environmental law established by the Government of India to offer prompt assistance to individuals impacted by incidents involving hazardous materials. This legislation was introduced following the Bhopal Gas Tragedy in 1984, which revealed the catastrophic effects of industrial irresponsibility and the pressing requirement for a legal framework to safeguard the public. The main goal of the Act is to ensure that industries dealing with hazardous chemicals and materials are held accountable for any incidents that may happen. According to the Act, the owners of these industries must secure insurance coverage to provide compensation to victims in cases of death, injury, or property damage resulting from an industrial incident. A distinctive and forward-thinking feature of the Act is its establishment of "no-fault" liability, which allows victims to obtain compensation without needing to establish negligence or wrongdoing on the industry's part. This streamlines the legal procedure and guarantees prompt assistance to those affected. Furthermore, the Act resulted in the formation of the Environmental Relief Fund, which aids in providing compensation that exceeds the limits of insurance coverage. Ultimately, the Public Liability Insurance Act, 1991 acts as both a preventive and protective measure, motivating industries to maintain safety while ensuring justice and support for the community in the event of industrial accidents. It strengthens the concept of "the polluter pays" and fosters accountability, thereby enhancing environmental governance and public safety in India. The National Green Tribunal Act, 2010 is an important piece of legislation enacted by the Government of India to enhance the country's environmental justice framework. This Act resulted in the creation of the National Green Tribunal, a dedicated judicial entity focused on resolving issues related to environmental protection, forest conservation, and sustainable development. The primary aim of the NGT Act is to establish an efficient and prompt system for addressing environmental disputes[17]. Before this Act, cases concerning the environment often faced significant delays in conventional courts due to procedural hurdles and insufficient expertise. The NGT, formed under this legislation, facilitates expedited justice by comprising judges and environmental specialists capable of effectively tackling technical matters. The Act grants the NGT authority over all civil matters connected to environmental laws outlined in Schedule I, including the Water Act, Air Act, Environmental Protection Act, Forest Conservation Act, and the Biological Diversity Act. It possesses the ability to issue directives, mandate compensation, and take notice of environmental issues on its own initiative. Notably, the Tribunal operates under the principles of natural justice, sustainable development, the precautionary principle, and the polluter pays principle. The National Green Tribunal has been instrumental in protecting India's environment by addressing various concerns such as industrial pollution, illegal mining, deforestation, and inadequate waste management.

In addition to these laws, numerous sector-specific and state-level regulations and notifications such as the E-Waste Management Rules, to manage e-waste in an environmentally sound manner. Plastic Waste Management Rules, to manage plastic waste responsibly and reduce its impact on the environment and Biomedical Waste Management Rules for proper handling, segregation, treatment, and disposal of waste generated from healthcare activities to prevent harm to human health and the environment have been instituted to tackle new environmental challenges.

---

[17] Swapan Kumar Patra and V. V. Krishna, "National Green Tribunal and Environmental Justice in India", Indian Journal of Geo-Marine Sciences, Vol. 44, No. 4 (Apr. 2015), p. 4, available at: https://www.researchgate.net/publication/266676371_National_Green_Tribunal_and_Environmental_Justice_in_India (last visited 15 June 2025)

Despite these extensive laws, enforcement remains problematic due to issues related to awareness, administrative inefficiencies, and insufficient resources. Nonetheless, India's environmental legislation demonstrates a strong legal commitment to preventing environmental offenses and promoting ecological sustainability. Strengthening enforcement through harsher penalties, public involvement, and inter-agency collaboration is vital for maintaining the environmental rule of law in the nation.

Challenges in addressing Environmental Crime as Socio-Economic Offence

Tackling Environmental crime as a socio-economic issue presents a complex challenge. Crimes against the environment such as unlawful deforestation, mining, wildlife trafficking, waste disposal, and pollution not only harm ecosystems but also jeopardize the livelihoods, health, and cultural rights of communities. By viewing these offenses as socio-economic issues, we acknowledge the damage they inflict beyond the environment impacting social justice, economic fairness, and human rights. Nonetheless, effectively addressing them in this wider context entails considerable difficulties.

One significant challenge is that, in many legal frameworks, environmental crimes are not specifically classified as socio-economic offenses. Although environmental protection legislation exists, it frequently regards violations as regulatory breaches instead of criminal actions with social and economic impacts. This inadequate classification restricts the capacity to enforce stringent criminal penalties, overlooks the comprehensive harm inflicted on communities, especially marginalized populations, and results in these cases being given lower priority in law enforcement and judicial systems[18].

Insufficient legislation or ineffective enforcement of current laws creates challenges for prosecution. Numerous environmental regulations are civil rather than criminal, resulting in minimal penalties or fines instead of jail time. In many countries, environmental laws are either outdated, fragmented, or lack the necessary scope to cover the wide range of environmental crimes occurring today. These laws often impose minimal penalties, which fail to deter offenders, especially powerful corporations or organized crime groups involved in activities like illegal mining, deforestation, or industrial pollution. Furthermore, environmental crimes are often classified as civil or administrative infractions instead of serious criminal offenses that can lead to significant socio-economic repercussions, including dislocation, loss of income, or health risks for vulnerable populations. Even where laws are in place, enforcement can be lacking due to poor inter-agency coordination, insufficient funding, a dearth of trained staff, and corruption. Environmental enforcement officers and police may lack the technical knowledge or legal understanding necessary to effectively investigate and prosecute intricate environmental crimes. In addition, the judiciary may not possess specialized courts or the insight to handle such matters with the urgency and seriousness they warrant. This creates a disconnect between legal standards and real-world situations, enabling wrongdoers to operate without consequences while impacted communities persist in facing the lasting socio-economic effects of environmental harm.

[18] Saurabh Pandey and Mahima Tripathi, “Environmental Crimes Vis-A-Vis Socio-Economic Offences”, International Journal of Research and Analytical Reviews (IJRAR), Vol. 7, Issue 3 (2020), pp. 277–280. (last visited 15 June 2025).

Complexity and transboundary nature of environmental crimes stand as another challenge in identifying it as a socio-economic offence. The environmental offenses frequently transcend national boundaries and involve complex networks of participants, such as corporations, organized crime syndicates, and individuals from various countries. Activities like illegal logging, e-waste disposal, wildlife trafficking, and marine pollution are examples of crimes that span jurisdictions, complicating the efforts of national authorities to monitor, investigate, or prosecute effectively. The lack of robust international collaboration mechanisms, or the ineffectiveness of those in place, further obstructs the ability to tackle these crimes in a thorough manner. The socio-economic consequences also cut across borders, disproportionately impacting marginalized communities and the global commons[19].

One of the most significant and ongoing difficulties in recognizing environmental crime as a socio-economic offense is the strong influence of economic motivations and corporate interests. These two factors frequently work together to hide, normalize, or validate actions that cause considerable harm to the environment while also yielding substantial profits for individuals and companies. This deeply rooted situation complicates the detection, regulation, and prosecution of environmental offenses, especially when they are presented as common business practices or lawful economic activities. Environmental offenses like illegal mining, unauthorized land development, industrial waste discharge, illegal logging, and wildlife trafficking are extremely lucrative activities. The financial gains considerably outweigh the potential consequences or chances of getting caught, particularly in nations where environmental regulations are lenient and enforcement is sporadic. As a result, both legitimate and illegitimate businesses are motivated to breach environmental laws to enhance their profits. This profit-driven mindset turns environmental damage into a rational economic choice, thereby integrating crime into business practices rather than treating it as a separate unlawful action.

In numerous rural and marginalized areas, communities rely directly on natural resources for their livelihood. Practices like illegal sand mining, unregulated logging, charcoal production, small-scale poaching, or informal e-waste dismantling often represent primary or supplementary income sources. While these activities are harmful to the environment, they are perceived as economically vital. When individuals depend on such actions to provide for their families, support their children's education, or pay off debts, the distinction between a survival tactic and a criminal behavior becomes both ethically and legally complicated[20]. This reliance on these practices creates a moral ambiguity, making it challenging to categorize these actions solely as socio-economic crimes without recognizing the existing poverty and systemic exclusion. Weaker local communities are frequently exploited or pressured by more powerful entities, such as illegal operators, contractors, and even political figures. These individuals take advantage of the economic vulnerability of these communities by providing financial incentives or deceptive promises in exchange for their participation in or indifference to environmental offenses. For instance, tribal members might be recruited for labor in illegal mining activities, or fishermen could receive

[19] Konstantin Sych and Vladimir Sych, “Environmental Crime and Influence of Socio-Economic Factors on the Development of Punishment System”, (2021) Jurisprudence and Criminology Research Journal. PP 124, available at: https://doi.org/10.1051/e3sconf/202124412022 (last visited 15 June 2025).

[20] “Socio-economic and environmental implications of Artisanal and Small-scale Mining (ASM) on agriculture and livelihoods” (2020) https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7642777/ (last visited 15 June 2025).

compensation for aiding in wildlife trafficking. In these circumstances, the local population becomes involved not out of choice but due to necessity or coercion. This situation blurs the distinction between victim and perpetrator, complicating the identification and resolution of environmental crimes as intentional socio-economic transgressions.

The successful identification and prosecution of environmental crimes, particularly those that are socio-economic in nature, increasingly rely on the application of modern technology and dependable data. Nevertheless, numerous countries especially in the Global South continue to face challenges due to inadequate technological capabilities, poor data infrastructure, and a lack of integration of digital tools into their systems of environmental governance. This shortfall greatly obstructs the capacity to detect, monitor, and address environmental crimes, posing a significant obstacle to recognizing and tackling these offences within their larger socio-economic framework. Innovative technologies like satellite imagery, drones, GPS mapping, and remote sensing could transform the detection of environmental crimes. These technologies can monitor illegal activities such as deforestation, land invasions, mining, marine pollution, and wildlife movements almost in real-time[21]. Nonetheless, in many areas, these technologies are often inaccessible or not fully utilized because of their high costs, the shortage of skilled workers, and insufficient infrastructure. Consequently, illegal operations go unnoticed in remote or ecologically delicate regions, hindering prompt action and leading to extensive environmental harm that remains unrecorded.

Environmental crimes frequently result in extensive social and economic repercussions, impacting public health, livelihoods, natural ecosystems, and fairness for future generations. Nevertheless, a significant obstacle in addressing environmental crimes as socio-economic violations is the inadequacy of the judicial system and the mild penalties applied. These elements impede the acknowledgment of the gravity of these offenses and hinder effective legal deterrence, which ultimately undermines the broader environmental justice framework. One of the main judicial challenges is the insufficient specialized knowledge of environmental science, policy, and the socio-economic impacts of environmental degradation among judges and legal professionals. Many courts, particularly at lower levels, lack expertise in environmental issues and address such cases as ordinary civil or regulatory matters, rather than recognizing them as complex offenses with broader socio-economic repercussions. This leads to a minimization of the long-term effects of environmental crimes and a failure to categorize them as serious offenses that affect public welfare, economic growth, and human rights.

Tackling environmental crimes as socio-economic offenses necessitates a comprehensive strategy that combines legal reforms, enhancement of institutions, public education, technological advancements, and socio-economic growth. It is essential to understand that these offenses are not solely environmental concerns but are intricately connected to corruption, inequality, and social injustice. Effective reduction of environmental crimes and the achievement of environmental justice can only be realized through coordinated efforts at both global and local levels, guided by socio-economic contexts.

[21] "The Role of Technology in Revealing and Handling Environmental Crime: A Literature Review" (Sinergy Conference, 2024) https://sinergyconference.com/role-of-technology-environmental-crime (last visited 15 June 2025).

Legal and Policy Recommendations

Recognizing environmental crimes as socio-economic offenses presents a groundbreaking method for managing environmental issues by acknowledging the extensive and profound effects these crimes have on both society and the economy. Historically viewed as violations of regulations or administrative errors, environmental offenses such as illegal mining, pollution, deforestation, and improper waste disposal often lead to prolonged damage to public health, livelihoods, food security, and community resilience particularly affecting marginalized groups. By reinterpreting these crimes through a socio-economic perspective, policymakers and law enforcement can treat them as significant dangers to human welfare rather than merely threats to ecological stability. This change allows for the imposition of harsher penalties, tailored legal measures, and comprehensive policies aimed at promoting environmental justice, sustainable development, and social equity, thus creating a more integrated and effective framework for environmental protection[22].

Below are various policy suggestions to improve the identification and management of environmental crimes within the framework of socio-economic offences:

Broaden the Legal Definition of Environment Crime

Revise current environmental regulations and criminal laws to clearly categorize environmental offenses as crimes with socio-economic impacts. This change will make sure that activities like illegal mining, improper disposal of hazardous waste, and pollution are regarded not just as regulatory infractions but also as actions that negatively affect public health, economic stability, and community welfare.

Strengthen Inter-Disciplinary Investigations

Create collaborative task forces that incorporate environmental scientists, economists, sociologists, and law enforcement personnel. This approach will guarantee that the examination and categorization of environmental crimes consider their social, economic, and health consequences, thus acknowledging them as socio-economic offenses.

Develop Integrated Data and Monitoring systems

Allocate resources to national and regional data networks that connect environmental metrics such as air and water quality, deforestation levels with socio-economic indicators including income, health, and displacement. This combination will simplify the process of illustrating how environmental harm affects human well-being, allowing for more effective legal and policy responses.

Introduce Stricter penalties with Socio-Economic considerations

Revise the penalty systems to incorporate compensation for impacted communities, impose criminal responsibility on repeat or large-scale offenders, and increase fines for corporate offenses. Penalties designed to deter should take into account the socio-economic consequences of the crime, which will enhance its seriousness and deter further violations.

[22] EFFACE, "Addressing environmental crime through the criminal justice system", Policy Brief, http://efface.eu/publications/policy-brief-addressing-environmental-crime-through-criminal-justice-system (last visited 15 June 2025).

Mandate Social Impact Assessment for Environment Violations

Require SIAs[23] to be mandatory in cases of environmental litigation or investigations to evaluate effects on livelihoods, health, displacement, and financial loss. Acknowledging and recording these effects enhances the recognition of environmental damage as a socio-economic crime.

Build Capacity in the Judiciary and Law Enforcement

Organize ongoing training sessions for judges, prosecutors, and law enforcement officials regarding the connections between environmental damage and socio-economic challenges. This enhances the judicial comprehension and aids in categorizing these offenses within the socio-economic crime framework.

Empower Local Communities and Whistle Blowers

Enhance legal safeguards and incentives for community reporting, whistleblowers, and environmental advocates. Often, marginalized communities directly observe environmental offenses. Safeguarding and empowering these groups promote prompt reporting and highlights socio-economic effects.

Create a National Socio-Environmental offences Registry

Establish a public registry of environmental violations that includes recorded socio-economic impacts, involved offenders, and judicial results. Transparency in law enforcement aids in recognizing trends, pinpointing high-risk locations, and enhancing policy responses.

Integrate Environment Crime into a National Crime Statistics

Incorporate environmental offenses, particularly those that have evident socio-economic impacts, into official crime statistics and national crime surveys. This emphasizes the importance of environmental crimes in the development of policies and the strategic planning of law enforcement.

Promote Cross-Border Cooperation

Partner with adjacent nations and global organizations to monitor transboundary environmental offenses like wildlife smuggling or the illicit e-waste trade. Numerous environmental crimes carry worldwide socio-economic consequences and necessitate regional collaboration for successful categorization and intervention.

Conclusion

Environmental crimes, when assessed solely as regulatory breaches, do not adequately reflect the comprehensive damage they cause to human communities, economies, and ecosystems. Reframing these acts as socio-economic offences exposes a more profound and urgent truth, where environmental degradation is a direct contributor to poverty, health emergencies, displacement, inequalities in resources, and social turmoil. This redefinition is not simply a matter of terminology, it represents a vital transition that aligns environmental law with the fundamental principles of sustainable development, which necessitate harmonizing ecological health with economic advancement and social equity.

[23] Social Impact Assessments

By categorizing environmental crimes as socio-economic offences, legal frameworks can shift from merely reacting to violations to proactively safeguarding the environment, addressing the underlying causes and cumulative effects of ecological harm. This approach fosters a more holistic system of accountability—holding corporate polluters, illegal resource exploiters, and negligent officials liable not only for environmental damage but also for jeopardizing lives and livelihoods. Furthermore, it promotes stronger legal recourse, enhances community engagement, and improves access to justice for marginalized groups who are often the first and most severely impacted.

Additionally, acknowledging environmental crimes as socio-economic offences aids in fulfilling international obligations like the United Nations SDGs[24], especially those focused on environmental sustainability[25], governance[26], poverty alleviation[27], and public health. In light of the worsening climate crisis, loss of biodiversity, and pollution challenges, the legal framework must adapt to encompass the interconnections between the environment, society, and economy.

Thus, it is crucial for policymakers, judges, and law enforcement bodies to embrace a multidisciplinary and equity-centric strategy toward environmental crime—rooted in evidence, driven by justice, and aimed at sustainability. Only by classifying environmental crimes as socio-economic offences can we effectively safeguard not only the environment but the future of humanity itself.

[24] Sustainable Development Goals.
[25] SDG 13, 14, 15.
[26] SDG 16.
[27] SDG 1.

DIGITAL FINANCIAL CRIMES IN DEVELOPING ECONOMIES: SOCIO-ECONOMIC RISKS AND CHALLENGES

Anoushka Chakladar
Amity Law School, Amity University, Noida

ABSTRACT

The rapid advancement of digital technologies has revolutionized financial systems, enabling faster and more efficient transactions. However, this transformation has also given rise to a surge in digital financial crimes, including online fraud, identity theft, ransomware attacks and cryptocurrency-related offenses. This research paper explores the evolving landscape of digital financial crimes and examines their far-reaching socio-economic consequences. By analyzing global trends, real-world case studies, and the limitations of current regulatory frameworks, this study highlights the economic burden on individuals, businesses and governments as well as the broader social implications such reduced trust in digital platforms and barriers to financial inclusion. This paper also evaluates mitigation strategies including legal reforms, cybersecurity investments and public-private partnerships. Ultimately, the research emphasizes the urgent need for coordinated international efforts and proactive policies to address the threat of digital financial crimes in the digital-age.

Key words: *Digital Financial Crimes, Cryptocurrency, Fraud, Identity Theft, Cybersecurity Investments.*

Introduction

The digital evolution has significantly changed a part of modern society, including how financial transactions are conducted. With the emergence of internet banking, mobile wallets, cryptocurrency platforms and real time payment gateways, services of the finances have become faster, accessible and more efficient[1]. However, the increased dependence on digital infrastructure has also given rise to a new and sophisticated class of crimes-digital financial crimes. These are not limited to identity theft, phishing attacks, unauthorized fund transfers, ransomware attacks, ATM skimming and cryptocurrency fraud[2]. The growth of the digital financial ecosystem, though cathartic, has unintentionally created a fertile ground for cybercriminals to exploit technological loopholes, jurisdictional ambiguities and regulatory gaps.

India, in particular, has witnessed a significant surge in digital transactions following the Digital India initiative and the COVID-19 pandemic, which catalyzed a shift towards contactless and online banking[3]. Despite the fact that this transition has contributed to financial inclusion, millions of people have been exposed to cyber risks. Data from the Indian Computer Emergency Response Team (CERT-In) and the Reserve Bank of India (RBI) show that digital payment frauds have increased at an exponential rate over the past decade[4]. The threat is not limited to individuals; small businesses, banks, and even government institutions have fallen prey to elaborate financial cybercrimes, often orchestrated from transnational networks[5]. The socio-economic impact of such crimes is multifaceted. At the economic level, the victims incur direct financial losses, their businesses are

[1] S. Saxena, *Digital Payments in India: Evolution, Challenges and Way Forward*, RBI Occasional Papers, Vol. 41(1), 2020, p. 13.
[2] CERT-In, *Annual Report 2022*, Ministry of Electronics and Information Technology, Government of India, p. 22.
[3] Ministry of Electronics and Information Technology, *Digital India: Power to Empower*, 2020.
[4] Reserve Bank of India, *Report on Trend and Progress of Banking in India 2021–22*, RBI Publications, p. 84.
[5] The Hindu, "Cyberattacks Surge on Indian Financial Institutions," May 15, 2022.

disrupted, cybersecurity costs rise, and investor confidence declines. Small and medium-sized businesses (SMEs), which frequently lack the resources necessary to implement robust cybersecurity systems, suffer the most from these consequences. Digital financial crimes damage public confidence in technology and financial institutions, widen the digital divide, and cause victims psychological trauma. These issues are further compounded by the complexities of investigation and enforcement, which are hindered by anonymity on the internet, lack of technical expertise among law enforcement agencies, and overlapping jurisdictional concerns. Digital financial crimes not only have a negative impact on society and the economy, but they also present significant legal challenges. The existing statutory framework in India, primarily the Information Technology Act, 2000[6] and relevant sections of the Indian Penal Code, 1860, has often been criticized for its inadequacy in addressing modern cyber threats. Additionally, the lack of specialized cybercrime courts has resulted in adjudication delays and inconsistent judicial responses[7]. Internationally, while conventions like the Budapest Convention on Cybercrime provide a collaborative framework for tackling digital crimes, India is yet to become a signatory, citing sovereignty concerns.

This research paper seeks to explore the contours of digital financial crimes and their socio-economic implications in a comprehensive manner. It aims to:

- Examine the various forms and methods of digital financial crimes prevalent today;
- Analyse the economic and social consequences on individuals, businesses, and the broader economy;
- Assess the efficacy of existing legal and regulatory mechanisms in India and compare them with international best practices; and
- Propose policy recommendations for improving legal, technical, and institutional responses to these crimes.

The methodology employed is primarily doctrinal, supported by empirical data where relevant. Case laws, government reports, legal statutes, and academic literature form the core of this study's research base. Particular attention is paid to the intersection of law, technology, and public policy, with an emphasis on how a balanced regulatory framework can mitigate both the incidence and impact of digital financial crimes.

In an era where the global economy is increasingly digitized, the battle against financial cybercrime is not merely a matter of technology or regulation—it is a question of national security, economic stability, and public trust. A comprehensive, multi-stakeholder strategy that takes into account substantial legal reform, international cooperation, increased public awareness, and strategic investments in cybersecurity infrastructure are the points made in this paper. Only then can we hope to create a secure and equitable digital financial ecosystem that serves the needs of all citizens.

---

[6] Information Technology Act, 2000, ss. 43, 66, 66C, 66D; Indian Penal Code, 1860, ss. 420, 465, 468.

[7] *Shreya Singhal v. Union of India*, AIR 2015 SC 1523.

Conceptual Framework

Understanding Digital Financial Crimes

Digital financial crimes refer to illegal activities that exploit internet-based financial systems to defraud, steal, or unlawfully manipulate monetary resources[8]. These crimes are executed using computers, mobile devices, digital platforms, and emerging technologies such as block chain and artificial intelligence. Digital variants, in contrast to conventional financial crimes, operate outside of physical borders and in environments that are decentralized and frequently anonymous, making detection and enforcement significantly more difficult[9].

These crimes encompass a wide range of malicious actions, including data breaches, hacking into financial systems, creating fake websites or payment portals, and using malware to extract personal and financial information. These crimes are not limited to theft or fraud alone. In recent years, the evolution of digital payment systems, online banking, and cryptocurrencies has expanded the attack surface available to cybercriminals.

Types and classification of Digital Financial Crimes

Digital financial crimes can be broadly categorized based on their method of execution and target:

a) ***Phishing and social Engineering Scams***

By posing as a legitimate organization, phishers trick users into divulging sensitive information like passwords, credit card numbers, or bank login credentials[10]. Typically, these are carried out via forged websites, text messages, or emails.

b) ***Identity theft and account takeover***

In this form, cybercriminals gain unauthorized access to personal or financial information and use it to impersonate the victim for illicit financial transactions.

c) ***Ransomware and Malware Attacks***

Ransomware locks or encrypts digital systems and demands payment—usually in cryptocurrency—to restore access. These attacks have severely impacted financial institutions and corporations globally.

d) ***Cryptocurrency-Related Crimes***

These include Ponzi schemes, pump-and-dump frauds, crypto-jacking (unauthorized use of a computer to mine cryptocurrency), and money laundering using digital currencies.

The Digital Financial Ecosystem

The digital financial ecosystem comprises a network of banks, non-banking financial companies (NBFCs),

---

8 R. Subramanian, *Cyber Crimes and Digital Fraud*, Eastern Book Company, 2021, p. 11.

9 N. Singh, "Digital Crime and the Law: Challenges in the Indian Context," (2022) 14(1) *Journal of Law and Technology* 19.

10 CERT-In, *Cyber Security Annual Report 2022*, Ministry of Electronics and IT, p. 36.

fintech startups, digital payment providers, customers, and regulatory bodies[11]. Nevertheless, financial transactions have become more risky as a result of the integration of blockchain-enabled platforms, IMPS (Immediate Payment Service), and the Unified Payments Interface (UPI). While democratizing access, the rapid digitization of finance has also outpaced the creation of corresponding legal safeguards. Cybercriminals have been able to take advantage of technical and legal loopholes as a result of this imbalance, particularly in regions with inadequate regulatory frameworks or inadequate cybersecurity infrastructure.

Differences between Traditional and Digital Financial Crimes

While both traditional and digital financial crimes aim to achieve financial gain through unlawful means, the methods, speed, anonymity, and scalability of digital financial crimes make them uniquely threatening. Digital crimes can be executed remotely, in real-time, and can impact millions simultaneously[12]. In addition, they frequently involve cutting-edge technologies that make investigation and traceability challenging. Digital crimes can be carried out by individuals or organized cybercriminal networks from all over the world. Unlike traditional fraud, which may involve forged checks or insider theft, digital crimes frequently make use of the dark web, encrypted communication, and cryptocurrency wallets that cannot be traced.

The Legal Significance of Definitions

The lack of universally accepted legal definitions is a critical issue when dealing with digital financial crimes. Different jurisdictions interpret and classify these crimes differently, which creates significant obstacles in extradition, mutual legal assistance, and prosecution of cross-border offenders. Not only does this legal ambiguity make it harder to enforce, but it also causes judicial decisions to be inconsistent.

Causes and Enablers of Digital financial Crimes

The exponential increase in digital financial crimes are closely tied to a host of structural, technological, legal, and behavioural factors. Understanding the key drivers behind such crimes is essential for the creation of effective legal and policy mechanisms. The development of robust cybersecurity architecture has lagged behind the rapid pace of digitalization. Outdated software, misconfigured systems, and poorly protected APIs leave digital financial platforms exposed to hacking, malware, and unauthorized access[13]. The possibility of being exploited is raised by the fact that many financial technology and banking institutions place a greater emphasis on speed of service than on complete security. The growing use of mobile devices, cloud computing, and Internet of Things (IoT) technologies also introduces systemic risks. Each new access point makes it harder to catch cybercriminals and expands their attack surface. [14]The general lack of cybersecurity awareness in India is a significant contributor to cyber fraud. The majority of users are still not familiar with best practices like creating secure passwords, spotting phishing links, and spotting phoney emails or websites. Many first-time users of digital banking services, particularly those in rural and semi-urban areas, are vulnerable to social engineering attacks because financial literacy campaigns frequently do not include cyber hygiene training.

---

[11] Reserve Bank of India, *Vision Document for Payment Systems 2025*, RBI Publications.

[12] European Union Agency for Cybersecurity (ENISA), *Threat Landscape Report 2023*, p. 60.

[13] P. Chatterjee, "Cybersecurity Loopholes in India's Financial Sector," (2022) 7 *Journal of Financial Law and Policy* 41.

[14] World Bank, *Cybersecurity in Financial Sector: Trends and Risks*, 2022, available at: https://www.worldbank.org (last visited May 1, 2025).

The Information Technology Act of 2000, which serves as the current legal framework, is ill-prepared to handle new types of digital financial crimes like ransomware, cryptocurrency fraud, and phishing created by artificial intelligence. The Indian Penal Code, 1860, has provisions that deal with fraud and impersonation, but they are not specifically designed for offenses committed online. Furthermore, enforcement efforts are weakened by the absence of cyber-specialized courts, procedural delays, and investigating officers' lack of technical expertise. Additionally, India has limited its access to efficient cross-border cooperation mechanisms by refusing to sign the Budapest Convention on Cybercrime. This limits India's capacity to look into and bring charges against criminals overseas because the majority of digital financial crimes are transnational.

While end-to-end encryption, anonymizing browsers (like Tor), and cryptocurrencies provide users with privacy, they also prevent cybercriminals from being discovered. The emergence of unregulated cryptocurrency exchanges and decentralized finance (DeFi) has made it more difficult for authorities to track down the source and recipients of fraudulent transactions and allowed the laundering of illegal funds.

Law enforcement's access to data and suspects is further complicated by the fact that many of these platforms are housed in countries with loose or ambiguous regulatory frameworks. India's institutional response to the growing number of cyberfrauds is still disjointed and underfunded. The majority of state police forces lack the technical know-how, forensic equ ipment, or specialized training necessary to look into financial cybercrimes, even though some metro areas have set up cyber cells. This ultimately discourages victims from reporting offenses by causing delays in the filing of FIRs, gathering of evidence, and prosecution.

Additionally, financial institutions frequently treat cybersecurity as a compliance burden rather than a strategic imperative, demonstrating complacency. A lot of fintech startups don't have proper risk assessments, security audits, or emergency procedures in place. Millions of people have entered the digital economy as a result of the drive for financial inclusion, particularly through programs like Jan Dhan Yojana. However, this has unintentionally produced a sizable pool of susceptible users in the absence of commensurate advancements in digital education. Phishing schemes, OTP fraud, and fraudulent investment apps frequently target new digital users, especially those in economically disadvantaged areas.

Simultaneously, the increasing involvement of domestic actors in cybercrime syndicates has been associated with rising youth unemployment, particularly among tech-literate individuals.

Socio-Economic Impact of Digital Financial Crimes

Digital financial crimes have far-reaching effects on social cohesion and economic stability, making them more than just technical transgressions. Individuals, corporations, institutions, and even national economies are impacted by these crimes as they become more complex and widespread.

Economic Impact

The direct loss of money is the most obvious and quantifiable economic effect of digital financial crimes. Victims, who can be anyone from private citizens to large corporations, lose money as a result of fraudulent investments, ransomware demands, or illegal transactions. Financial frauds involving digital transactions have increased in

India, especially since the COVID-19 pandemic increased the use of digital payments[15]. The Reserve Bank of India's (RBI) 2023 Annual Report states that losses from digital payment frauds totaled almost ₹1,457 crore, a rise of more than 30 percent from the year before[16]. These losses are only the beginning, as many cases remain unreported because of concerns about one's reputation or a lack of trust in the legal system. Cybercrime frequently results in business disruption in addition to direct theft. Business operations can be stopped by ransomware attacks, data breaches, or fraudulent fund transfers, particularly for small and medium-sized businesses (SMEs) with weak cybersecurity defences. Loss of consumer trust, legal advice, and system restoration are all examples of recovery costs. Spending on fraud detection systems and cybersecurity infrastructure is on the rise, especially for financial institutions. Despite being essential, this takes money away from projects aimed at innovation and development. Smaller firms in the fintech sector are particularly burdened financially by the compliance expenses related to regulatory requirements for risk management.

The financial system's credibility is damaged by frequent cyberattacks. Fraud victims might be less likely to use digital platforms in the future, which would result in fewer transactions. Nearly 48% of Indian consumers polled for a 2022 Deloitte study said they would never use online banking again after being the victim of or witnessing a digital fraud incident. High exposure to cyber threats may also be viewed as a warning sign by investors, especially in start-ups and emerging fintech ventures. This discourages investment and hinders the expansion of financial models driven by innovation.

The cumulative effect of financial crimes, particularly those that remain unreported or unresolved, weakens economic systems on a macroeconomic level. Increased public spending on law enforcement and cyber infrastructure is required as a result of cybercrime, which also damages investor confidence and disrupts revenue flows. It also has an impact on cross-border investment appeal and international creditworthiness, especially in countries where there is a widespread belief that digital security is inadequate.

Social Impact

The foundation of any financial system is trust. This trust is undermined by digital financial crimes, especially when the offenders escape punishment or when money recovery is impossible. Victims frequently lose trust in the broader online banking and e-commerce ecosystem as well as in particular institutions[17]. This may hinder initiatives to advance digital financial inclusion, particularly in rural regions where there is already a lot of opposition to online banking. The goal of a cashless or less-cash society is thus hampered. High levels of psychological stress are frequently experienced by victims of cyber fraud. When legal action is postponed or rejected, the sense of violation caused by identity theft, data breaches, or financial loss is intensified. According to studies, victims of online financial crimes frequently express feelings of helplessness, shame, and anxiety, particularly when the fraud causes distress to their family or reputation[18].

People with low levels of digital literacy, such as the elderly, the impoverished in rural areas, and new users, are

---

[15] CERT-In, *Annual Report 2023*, Ministry of Electronics and IT, p. 47.

[16] Reserve Bank of India, *Annual Report 2023–24*, p. 103.

[17] A. Desai, *Digital Trust and the Rise of Online Crime*, Oxford University Press, 2023, p. 44.

[18] R. Mishra, "The Psychological Toll of Cyber Fraud," (2023) 18 *National Law School Review* 101.

disproportionately affected by digital financial crimes. Phishing, phony customer service calls, or fraudulent apps are used to manipulate a lot of people. This strengthens their exclusion from official financial systems and deters them from continuing to engage in the digital economy[19]. These groups often completely stop using digital platforms out of fear of being scammed. This contradicts the financial inclusion objectives of national initiatives such as Pradhan Mantri Jan Dhan Yojana and Digital India.

Affected people sometimes turn to naming and shaming suspected scammers on social media when legal action is either slow or non-existent. Misinformation, defamation, and even violent threats have resulted from this, which has weakened the rule of law and fuelled social unrest. Misinformation is further exacerbated by the ease with which fraudulent messages and apps proliferate on WhatsApp and other platforms, sometimes resulting in panic, mob behaviour, or even tensions within communities.

1.Legal and Regulatory Framework Governing Digital Financial Crimes in India

The effectiveness and sufficiency of current legal frameworks are called into question by digital financial crimes, particularly in countries like India where cyber law is still developing. India's legal system has not always kept up with the complexity and prevalence of digital financial crimes, despite the country's notable advancements in digitalization. The pertinent Indian statutory laws, regulatory frameworks, judicial decisions, and institutional arrangements are critically examined in this section, along with any shortcomings that prevent efficient enforcement.

- **Statutory Framework**

  i) Information technology Act, 2000 (IT Act)

The **Information Technology Act, 2000** remains India's principal legislation addressing cybercrimes. It provides legal recognition to electronic transactions and digital signatures, and criminalises unauthorised access, data breaches, and identity theft under Sections 43, 66, 66C, and 66D[20].

- **Section 66C** penalises identity theft and misuse of digital signatures or passwords.
- **Section 66D** criminalises cheating by impersonation through computer resources.
- **Section 43** outlines civil liabilities for unauthorised downloading, virus insertion, or data theft.

However, the Act does **not explicitly define "digital financial crimes"**, leaving a grey area in law. Many complex crimes involving cryptocurrencies, cross-border fraud, or AI-generated scams fall outside the Act's current scope[21].

---

[19] Ministry of Finance, *Financial Inclusion Status Report 2023*, Government of India.

[20] Information Technology Act, 2000, ss. 43, 66C, 66D.

[21] N. Singh, "Digital Crime and the Law: Challenges in the Indian Context," (2022) 14(1) *Journal of Law and Technology* 19.

ii) Indian Penal Code, 1860 (IPC)

While the IPC predates digital technology, certain provisions are invoked to prosecute cyber-financial crimes:

- **Section 420** (cheating and dishonestly inducing delivery of property)
- **Section 464** (forgery)
- **Section 468** (forgery for the purpose of cheating)
- **Section 471** (use of forged documents)

These provisions, though helpful, are not always technologically suited for digital evidence or nuanced financial cybercrimes. They rely on traditional concepts of mens rea, property, and physical harm, which may not align with cyber jurisprudence.

- ***Other Relevant Laws***

1) **The Prevention of Money Laundering Act, 2002 (PMLA):** Used in cases involving online money laundering or cryptocurrency fraud[22].

2) **The Banking Regulation Act, 1949 & RBI Circulars:** Empower the RBI to issue cybersecurity guidelines to banks and NBFCs.

3) **The Consumer Protection (E-Commerce) Rules, 2020:** Address unfair trade practices on digital financial platforms, but lack direct enforcement mechanisms.

- **Judicial Interpretation and Role of the Courts**

Digital financial crimes have been addressed piecemeal by the Indian judiciary. Courts have rarely offered systematic guidance for financial cybercrimes, instead concentrating on protecting the right to privacy, data protection, and criminal liability for fraud.

1) In **Shreya Singhal v. Union of India**, the Supreme Court struck down Section 66A of the IT Act as unconstitutional, citing free speech concerns. While this ruling protected civil liberties, it also removed a key provision that was frequently invoked—albeit sometimes misused—in digital crime cases[23].

2) In **State of Maharashtra v. Dr. Praful B. Desai**, the Court accepted electronic records as valid evidence under the Evidence Act, 1872, paving the way for digital proof in courtrooms[24].

However, the lack of specialized cybercrime courts leads to inconsistent adjudication and lengthy pendency. Judges and magistrates frequently lack specialized training, which causes delays in justice and incorrect interpretations.

---

[22] Prevention of Money Laundering Act, 2002, s. 3 read with Schedule A.

[23] *Shreya Singhal v. Union of India*, AIR 2015 SC 1523.

[24] *State of Maharashtra v. Dr. Praful B. Desai*, AIR 2003 SC 2053.

- **Role of Regulatory Institutions**

a) **Reserve Bank of India**

In order to secure India's digital financial architecture, the RBI is essential. It provides guidelines for customer redress, real-time alerts, and fraud detection. Among the noteworthy initiatives are: The 2016 Circular on Cyber Security Framework in Banks requires banks to implement real-time fraud monitoring systems and report breaches. The RBI Ombudsman Scheme (2021) offers consumers who are victims of fraudulent digital transactions a way to file grievances. The RBI's enforcement powers are constrained, though. It cannot impose criminal sanctions or investigate frauds independently; it must rely on law enforcement agencies.

b) **Indian Computer emergency response team (CERT-In)**

Under the Ministry of Electronics and IT, CERT-In is responsible for cybersecurity advisories, threat alerts, and incident monitoring. Despite being vital, it only plays a reactive role and has no prosecutorial authority. It frequently coordinates with law enforcement in a disjointed or delayed manner.

- **Enforcement and Investigation Challenges**

There are still a number of issues in spite of a fairly organized legal and regulatory environment:
Jurisdictional Ambiguity: Since digital financial crimes frequently occur across several states or countries, filing and enforcing FIRs can be challenging.
Lack of Technical Expertise: Many police departments lack the necessary tools to comprehend blockchain transactions or perform digital forensics.
Low Conviction Rates: Due to a lack of proof, subpar investigations, and protracted legal proceedings, the conviction rate in cybercrime cases is still less than 2%.
Law Reform Delay: Despite being discussed, the Digital India Act has not yet been put into effect, creating legislative gaps.

Conclusion

One of the most urgent issues facing legal systems, financial institutions, and individual users alike in an increasingly digitalized world is the emergence of digital financial crimes. These crimes, which range from sophisticated cryptocurrency scams to phishing and identity theft, are no longer isolated occurrences. They are borderless, systemic, and developing more quickly than the systems put in place to keep them in check.

This study has shown that the effects of digital financial crimes extend beyond monetary losses. They have a profound impact on society, undermining the promise of financial empowerment and digital inclusion, eroding public trust, and increasing the exclusion of marginalized communities. Because of the embarrassment, mental anguish, and complicated legal process that follow such crimes, people—especially those with low levels of digital literacy—frequently endure injustice in silence. These attacks cause operational disruptions, damage consumer trust, and necessitate ever-increasing resources for recovery and prevention for both governments and businesses.

This paper's recurrent theme is the disparity between legal readiness and technological advancement. The Information Technology Act of 2000 and a few other sections of the Indian Penal Code form the foundation of India's current legal system, which is antiquated and ill-prepared to handle the complexity and international scope of digital financial crimes. There is a justice void as a result of the lack of precise definitions, specialized cybercrime courts, or specific procedural codes for digital evidence; victims are frequently left without answers, and criminals evade punishment because of jurisdictional gaps and investigative slack. Although regulatory bodies such as the RBI and CERT-In have made admirable efforts to raise consumer awareness and cybersecurity, their mandates are not very broad. The absence of a single, centralized agency to enforce cyber financial crime leads to In light of this, multi-layered, multi-stakeholder reform is desperately needed. The first step in legal reform must be a thorough replacement of the IT Act with the proposed Digital India Act, making sure that it contains strong provisions for cross-border cooperation, digital fraud, and emerging technologies like blockchain, artificial intelligence, and financial scams made possible by deepfakes. Building judicial capacity is equally important; judges, magistrates, and investigators need to be continuously trained in forensic tools, digital evidence, and cyber jurisprudence.

India should think about establishing specialized cyber financial crime units in its courts, prosecution divisions, and legal aid organizations in addition to the police. Particularly for low-income victims who frequently suffer the most from these crimes, consumer grievance redressal procedures need to be made more easily accessible and time-bound. actors in the private sector—banks.

NOTES:

NOTES:

Printed, Published and owned by Amit Gupta. Printed at Shubham Enterprises, 129, DSIDC Sheds, Okhla Indl. Area, Phase-I, New Delhi - 110020.
Published at JIMS Engineering Management Technical Campus 48/4, Knowledge Park-III, Greater Noida. Editor: Amit Gupta