VOL 9 | Issue 1 | Jan-June 2025

ISSN : 2581-6837

jims

JIMS JOURNAL OF LAW

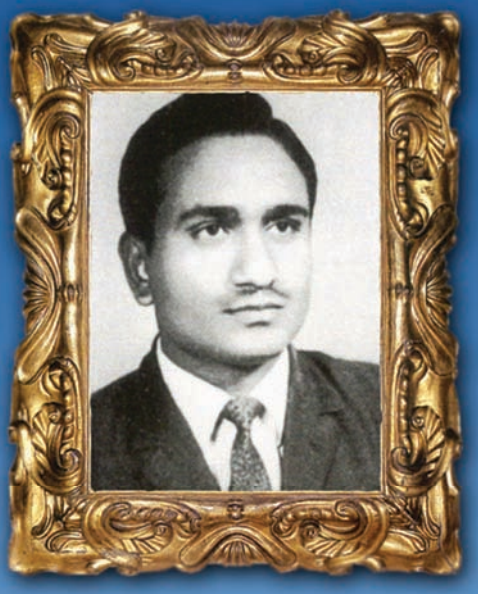
A Bi-Annual Peer Reviewed Journal

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

Copyright Reserve @ Publisher
Dr. Amit Gupta, Chairman, JIMS Group, **chairman@jagannath.org**

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

It gives me immense pleasure to present **Volume 9, Issue 1** of the JIMS Journal of Law, featuring thought-provoking papers that address some of the most pressing legal and policy challenges facing contemporary India. This issue brings together a diverse range of perspectives from academics, research scholars, and students, unified by a shared focus on financial crime, regulatory enforcement, socio-economic justice, and sustainable development.

The paper titled **Dark Web and Financial Cybercrime Ecosystems: Legal and Investigative Imperatives for India in a Borderless Digital Economy** explores the complex and often opaque world of digital crime, highlighting the urgent need for comprehensive legal frameworks and investigative strategies to address financial cybercrime in an increasingly interconnected global economy.

In **Role of Judiciary in Curbing Socio-Economic Offences and Ensuring Sustainable Development**, the author has delved into the critical role of the judiciary in balancing legal enforcement with the broader objectives of sustainable development. The paper reflects on the judiciary's potential as a transformative force in combating socio-economic crimes that hinder national progress.

Two papers in this issue examine the pivotal role of the Enforcement Directorate in India's fight against financial crimes.The article titled **The Role of Enforcement Directorate in Combating Financial Crimes in India** provides an in-depth institutional analysis, exploring both the strengths and limitations of the ED in the current regulatory landscape. Similarly, paper titled **An Examination of the Enforcement Directorate's Role in Addressing Financial Crime in India** critically assesses the agency's operational effectiveness and legal mandates from an academic standpoint.

In **Balancing Anti-Money Laundering Compliance and Financial Inclusion: Challenges at the Crossroads of Energy Access and Climate Finance,** the author brings attention to a pressing policy conundrum: how to reconcile strict financial compliance with the goals of inclusive finance and climate justice. The paper encourages a more nuanced approach to regulatory design in the age of sustainable development.

Concluding this issue is the 2G Spectrum **Scam Case** which revisits one of India's most high-profile corruption scandals. The case study offers valuable insights into the interplay between governance, public accountability, and institutional reform.

Each contribution in this volume reflects academic rigor, critical insight, and a commitment to addressing real-world legal challenges. I extend my heartfelt appreciation to all the authors for their valuable contributions and I hope this issue will serve as a meaningful resource for scholars, practitioners, policymakers, and students engaged in the evolving landscape of law and governance.

Sincerely,

Prof. (Dr.) Pallavi Gupta
Thanking You

Table of Contents

DARK WEB AND FINANCIAL CYBERCRIME ECOSYSTEMS: LEGAL AND INVESTIGATIVE IMPERATIVES FOR INDIA IN A BORDERLESS DIGITAL ECONOMY

Raghavendra S Kollurkar
Assistant Professor, University of Mumbai

ABSTRACT

The rise of the dark web as a marketplace for anonymised financial crime presents a significant challenge to India's cyber law enforcement architecture. This paper analyses the operational ecosystem of darknet-enabled crimes ranging from crypto laundering and carding to ransomware-as-a-service and assesses the legal and investigative incapacities in addressing them. It critiques India's fragmented legal response under the Information Technology Act, 2000, Bharatiya Nyaya Sanhita, 2023, and the Prevention of Money Laundering Act, 2002, while identifying the procedural and evidentiary gaps that hinder prosecutions. Drawing on case studies, official reports, and comparative insights from the US, EU, and Australia, the paper advocates for a unified legislative framework, blockchain-enabled forensics, and inter-agency coordination. It concludes with a call to construct a technologically literate rule of law capable of responding to transnational financial cybercrime within a constitutionally grounded framework.

Key words: *Dark Web, Financial Cybercrime, Crypto Laundering, Cyber Law Enforcement, Blockchain Forensics.*

Introduction: India at the Edge of the Dark Web Frontier

In the age of algorithmic finance and decentralised digital markets, the dark web has evolved into a potent enabler of transnational financial crime. Operating beneath the surface of indexed internet domains, the dark web accessed through anonymising networks such as Tor and Invisible Internet Project (I2P) provides an encrypted haven for illicit activities ranging from identity theft and crypto laundering to ransomware distribution and carding marketplaces[1]. While the global financial ecosystem undergoes digitisation at scale, India's expanding fintech sector and its demographic push toward digital payments have also rendered it increasingly vulnerable to these opaque, technologically advanced criminal networks[2].

The term *dark web* refers to a restricted portion of the deep web content not indexed by conventional search engines that can only be accessed via specialised software[3]. It is distinct from the *deep web*, which includes benign content such as academic databases and private cloud storage. In contrast, the dark web is intentionally concealed and anonymised, often leveraging layered encryption and privacy-enhancing cryptocurrencies like Monero, Zcash, or Tornado Cash to obfuscate identities and transactions[4]. The resulting *financial cybercrime ecosystem* comprises not merely individual offences, but a systemic, globally networked architecture of coordinated criminality that thrives on decentralisation, obfuscation, and technological sophistication[5].

In India, the proliferation of darknet-enabled financial crimes presents an urgent legal and enforcement challenge. Incidents of ransomware attacks targeting critical infrastructure, phishing kits tailored for Indian

---

[1] Europol, *Internet Organised Crime Threat Assessment* (2023).

[2] Reserve Bank of India, *Digital Payments Index* (2023).

[3] Turnbull I J, 'The Deep Web and the Darknet: A Primer for Law and Policy Makers' 12(1) *Journal of Cybersecurity Studies* 33 (2018).

[4] Financial Action Task Force (FATF), *Virtual Assets Red Flag Indicators* (2021).

[5] McGuire M, *Into the Web of Profit: Understanding the Growth of Darknet Markets* (University of Surrey, 2019).

banks, and the use of stolen credentials in dark web marketplaces have surged in recent years[6]. The National Crime Records Bureau (NCRB) reported a 45% rise in financial cybercrime cases between 2020 and 2022, many of which displayed patterns traceable to dark web sources[7]. Yet, India's legal and institutional response remains largely reactive and fragmented, lacking specialised frameworks to address the distinctive challenges posed by anonymity tools, distributed criminal networks, and blockchain-based laundering mechanisms[8].

This paper seeks to explore the following research questions:

1. What structural and normative gaps within India's existing legal framework hinder the effective investigation and prosecution of dark web–enabled financial crimes?

2. How do investigative constraints ranging from cross-jurisdictional challenges and evidentiary chain-of-custody issues to lack of technical forensic capacity complicate enforcement?

3. What comparative legal strategies have proven effective in other jurisdictions, and how can they inform a more coherent and resilient legal response in India?

This inquiry is grounded in a doctrinal-analytical methodology, examining Indian statutory frameworks such as the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, and the Prevention of Money Laundering Act, 2002. It integrates institutional practices of enforcement bodies such as CERT-In, FIU-IND, and the Enforcement Directorate, while drawing on comparative experiences from jurisdictions including the United States, European Union, and Australia. The analysis further incorporates criminological theories of deterrence, digital anonymity, and networked criminality to contextualise the unique legal challenges India faces at the intersection of cyberspace, financial regulation, and national security.

The structure of the paper progresses from mapping the operational mechanics of dark web financial crimes to analysing legal shortcomings and investigative constraints, culminating in a set of comparative insights and reform-oriented recommendations. In doing so, the paper positions India's legal regime at a critical inflection point between the rising tide of techno-criminal sophistication and the pressing need for a future-ready legal infrastructure.

Mapping the Dark Web Financial Crime Ecosystem

The dark web constitutes a specialised subset of cyberspace characterised by anonymised access protocols, decentralised hosting infrastructure, and encrypted communications. Unlike the surface web, which is indexed and publicly accessible, or the deep web, which comprises non-indexed but legal content such as databases or academic archives, the dark web is deliberately concealed. It is accessible only through anonymity networks such as The Onion Router (Tor) and Invisible Internet Project (I2P), which obfuscate user IP addresses by routing

[6] CERT-In, *Cyber Security Trends Report* (2023).

[7] National Crime Records Bureau (NCRB), *Crime in India 2022: Chapter XIII — Cyber Crimes*.

[8] Mehta P, 'Darknet, Crypto, and Criminal Law in India' 11(2) *Indian Journal of Law and Technology* 55 (2023).

traffic through multiple relays, thereby enabling both privacy-enhancing technologies and illicit marketplaces[9].

Darknet-based financial crime mirrors legitimate e-commerce platforms in sophistication featuring vendor reputation systems, escrow services, automated dispute mechanisms, and digital inventories. Cryptocurrencies like Bitcoin, Monero, and Zcash serve as the primary mediums of exchange, anonymising financial flows and significantly complicating forensic tracing efforts[10]. These platforms often rely on PGP encryption and decentralised storage mechanisms such as InterPlanetary File System (IPFS) to further obscure activity. The ecosystem supports a range of financially motivated crimes including carding (unauthorised use of stolen credit card data), SIM swap fraud (compromising mobile identities to bypass two-factor authentication), ransomware-as-a-service (RaaS), and laundering via tumblers, mixers, or decentralised exchanges[11]. These are not isolated actions, but part of a globalised and decentralised criminal economy that thrives on the collapse of jurisdictional boundaries and legal enforcement delays[12].

Anonymity and decentralisation are not merely technical affordances but structural features that confer resilience. Darknet actors operate in modular, often leaderless networks where cryptographic protocols and marketplace feedback systems replace legal accountability or contractual enforcement. Blockchain-based anonymity tools, smart contracts, and decentralised identity protocols enable trust less transactions, making infiltration and disruption by law enforcement exceptionally difficult[13]. This creates a criminal architecture that is scalable, adaptive, and remarkably persistent in the face of takedowns or legal actions[14].

Within India, there is growing empirical evidence of darknet-enabled financial criminality. The National Crime Records Bureau (NCRB) reported a 24.4% rise in financial cybercrime incidents in 2022, many involving fraudulent crypto investments, compromised bank credentials, and ransomware attacks with clear links to darknet forums[15]. Reports by the Indian Computer Emergency Response Team (CERT-In) highlight frequent targeting of Indian financial institutions through phishing kits and ransomware campaigns hosted on dark web servers[16]. Simultaneously, the Financial Intelligence Unit–India (FIU-IND) has observed a surge in suspicious transaction reports associated with crypto exchanges believed to be linked to dark web operations[17]. Yet, the institutional response has remained largely reactive. There is no mandatory obligation on private intermediaries to report fraud involving darknet links, and forensic investigation infrastructure remains underfunded and technically inadequate[18].

Compounding this is the inherently transnational character of dark web financial crimes. Offenders, victims, servers, payment platforms, and laundering nodes are dispersed across multiple jurisdictions, often beyond the

---

[9] Turnbull I J, 'The Deep Web and the Darknet: A Primer for Law and Policy Makers' 12(1) *Journal of Cybersecurity Studies* 33 (2018).

[10] McGuire M, *Into the Web of Profit: Understanding the Growth of Darknet Markets* (University of Surrey, 2019).

[11] Europol, *Internet Organised Crime Threat Assessment* (2023).

[12] United Nations Office on Drugs and Crime (UNODC), *Global Programme on Cybercrime: Annual Report* (2022).

[13] Financial Action Task Force (FATF), *Virtual Assets Red Flag Indicators* (2021).

[14] Hertig A, 'Monero and the Future of Anonymous Transactions' (2021) *CoinDesk Reports*.

[15] National Crime Records Bureau (NCRB), *Crime in India 2022: Chapter XIII — Cyber Crimes (2022)*.

[16] CERT-In, *Annual Report 2023*.

[17] Financial Intelligence Unit–India (FIU-IND), *AML-CFT Trends Report* (2023).

[18] Mehta P, 'Darknet, Crypto, and Criminal Law in India' 11(2) *Indian Journal of Law and Technology* 55 (2023).

reach of India's sovereign legal mandate. This fragmentation is further aggravated by the volatility of digital evidence logs that self-destruct, servers that route through anonymised relays, and encrypted wallets that evade attribution[19]. Legal processes such as mutual legal assistance treaties (MLATs) and Letters Rogatory are too slow to match the velocity of crypto-financial operations.

To analyse this evolving threat environment, network theory and economic criminology offer critical insight. The dark web functions as a scale-free network, where some nodes (such as marketplaces or escrow services) have many connections, while others remain isolated. This structure allows for redundancy and rapid regeneration, ensuring that even after high-profile shutdowns, the ecosystem persists and even mutates[20]. From the economic criminology perspective, darknet markets significantly reduce transaction costs and enforcement risks, offering rational incentives for participation. The relative ease of pseudonymity, combined with the global reach of crypto-assets and near-immediate execution of financial transactions, shifts the risk-reward calculus decisively in favour of offenders[21].

In sum, the dark web financial crime ecosystem is not merely a digital black market but a resilient, scalable, and transnationally-networked infrastructure. For Indian law enforcement and policymakers, the challenge is not only technological but institutional and normative demanding a reimagination of jurisdiction, evidence, and digital identity in the architecture of criminal law.

India's Legal Framework: Fragmented Norms in a Borderless Battlefield

India's legislative and enforcement framework remains fundamentally ill-equipped to counter the evolving threat posed by dark web–enabled financial crimes. The existing legal architecture, while robust in select domains, is marked by fragmented jurisdictional coverage, definitional ambiguity, and operational obsolescence when confronted with the technical sophistication of anonymised, transnational financial cybercrime ecosystems.

At the heart of India's cybercrime jurisprudence is the Information Technology Act, 2000 (IT Act), particularly Sections 66C and 66D, which criminalise identity theft and cheating by personation using computer resources, and Section 67B, which deals with online abuse involving children[22]. However, these provisions were drafted in an era when the threat landscape was limited to relatively primitive phishing or defacement attacks. The IT Act does not define or address anonymisation technologies, blockchain forensics, or the unique challenges of attributing conduct in decentralised digital ecosystems. Consequently, it fails to encompass the operational realities of ransomware-as-a-service, crypto laundering through mixers, or the use of privacy coins like Monero[23].

The recently enacted Bharatiya Nyaya Sanhita, 2023, introduces some degree of cybercrime recognition, notably in Section 336 (cyberterrorism) and Section 420 (cheating). While Section 336 offers a broader framing of digital

[19] Ghosh R, 'Evidence in the Age of Anonymity: Forensic Challenges in Darknet Investigations' 6 *NLUJ Law Review* 102 (2021).
[20] Barabási A, *Linked: How Everything Is Connected to Everything Else* (Penguin, 2002).
[21] Levi M, 'Economic Crime and the Dark Web: Rational Choice and Market Disruption' 35 *Crime, Law and Social Change* 233 (2019).
[22] *Information Technology Act, 2000*, ss 66C, 66D, 67B.
[23] Sinha D, 'The Limits of the IT Act in the Age of Blockchain Crime' 17(3) *NUJS Law Review* 201 (2022).

terror, its focus is national security, and it lacks specificity regarding financial crimes conducted through the dark web[24]. Section 420 continues the legacy of the Indian Penal Code's fraud-related provisions but remains insufficient to capture the technical nuance of algorithmic deception, spoofed identities, or synthetic financial instruments traded on darknet markets[25].

The Prevention of Money Laundering Act, 2002 (PMLA) provides a partial regulatory handle over financial cybercrime, especially crypto-laundering operations. The inclusion of virtual digital assets (VDAs) under the PMLA in 2023 was a pivotal step, bringing certain crypto transactions under suspicious transaction reporting requirements[26]. However, enforcement remains stunted by the absence of binding crypto exchange licensing standards, real-time blockchain forensics capabilities, and global cooperation frameworks. Given the anonymous nature of cross-border peer-to-peer wallets, most laundering activity via dark web–enabled ransomware still evades detection[27].

Admissibility of digital evidence often the most decisive factor in prosecuting dark web crimes is governed by the Indian Evidence Act, 1872, particularly Sections 65A and 65B. Although the Supreme Court's ruling in *Anvar v. Basheer* reinstated the requirement of a certificate under Section 65B(4), this provision often results in evidentiary exclusion due to procedural lapses[28]. Further, dark web crimes generate ephemeral evidence self-destructing links, encrypted logs, and decentralised ledgers necessitating urgent reform in the evidentiary framework to accommodate volatility and the chain of custody of digital artifacts[29].

Enforcement-related instruments such as the Reserve Bank of India's Guidelines on Digital Payments, KYC norms, and AML compliance frameworks attempt to bolster financial cybersecurity by regulating intermediaries. However, these are largely compliance-focused, not investigative in intent. Fintech platforms remain underregulated in their ability to detect and report crypto-based fraud that originates on the dark web. Despite mandatory KYC, wallet ownership obfuscation remains a persistent loophole[30].

The Digital Personal Data Protection Act, 2023 introduces a regime of data minimisation, consent-based sharing, and individual privacy safeguards. Paradoxically, while the DPDP Act enhances user privacy critical in democratic societies it also risks complicating darknet crime investigations by restricting real-time access to IP logs, metadata, or platform usage data by law enforcement[31]. The Act's ambiguity on carve-outs for state surveillance could lead to constitutional challenges under Articles 19 and 21, thereby creating additional procedural bottlenecks[32].

---

[24] *Bharatiya Nyaya Sanhita, 2023*, s 336.

[25] *Bharatiya Nyaya Sanhita, 2023*, s 420.

[26] Ministry of Finance, *Notification S.O. 1072(E)* (7 March 2023).

[27] Financial Action Task Force (FATF), *Updated Guidance for a Risk-Based Approach to Virtual Assets and VASPs* (2023).

[28] *Anvar P V v P K Basheer (2014) 10 SCC 473.*

[29] Mehta S, 'Dark Web Forensics and the Indian Evidence Act' 8(1) *NLUJ Law Review* 57 (2023).

[30] Reserve Bank of India, *Master Directions — Know Your Customer (KYC) Direction, 2016*.

[31] *Digital Personal Data Protection Act, 2023*, s 14.

[32] Singh R, 'Balancing Privacy and Investigation: The DPDP Act's Constitutional Implications' 36 *ILI Law Journal* 112 (2024).

A critical deficiency in India's legal framework is the complete absence of dedicated legislation on darknet activities or crypto-specific financial crime, leaving enforcement agencies to stretch ill-fitting statutes in innovative but ultimately inefficient ways. There is no legal definition of the dark web, no procedural manual for darknet forensics, and no statutory guidance for the investigation of pseudonymous crypto transactions. Mutual Legal Assistance Treaties (MLATs) are slow and rarely invoked for time-sensitive cyber operations. Moreover, India has not yet signed the Budapest Convention on Cybercrime, limiting its ability to cooperate internationally in darknet-linked financial investigations[33].

This techno-legal mismatch results in what may be termed enforcement paralysis a state wherein laws exist, but their application is structurally misaligned with the technological contours of the crime. Investigative agencies lack jurisdictional clarity, prosecutorial pathways are riddled with evidentiary hurdles, and regulators are forced to play catch-up with an adversary that thrives on code obfuscation, anonymity layers, and decentralised infrastructure.

Investigative Challenges in Practice: Between Law and the Dark Algorithm

While India's legislative framework provides a notional foundation for tackling darknet-driven financial crimes, investigative praxis remains stymied by technological evasiveness, evidentiary fragility, and institutional fragmentation. The dark web's operational opacity, layered anonymisation, and transnational architecture render conventional law enforcement methods ineffective, pushing Indian agencies into a domain where legal certainty is continually undermined by algorithmic evasion.

A central challenge is attribution, the foundational pillar of criminal culpability. Darknet actors mask their identities using Tor, I2P, privacy coins like Monero, and anonymising overlays such as VPN chains and cryptographic tumblers. These tools render IP-based tracking functionally obsolete, dismantling the conventional cause-effect linkage essential for establishing mens rea and actus reus[34]. Compounding this is the growing use of spoofed identities and deepfake avatars that further distort traceability, making it increasingly difficult to anchor digital activities to physical persons under the evidentiary standards prescribed in Section 61 of the Bharatiya Sakshya Adhiniyam, 2023 (BSA)[35].

Jurisdictional complexity aggravates the investigative impasse. The servers hosting illicit content or crypto-mining pools often reside in non-cooperative jurisdictions. Mutual Legal Assistance Treaties (MLATs), still the mainstay for cross-border electronic evidence, are notoriously inefficient and fail to match the temporal exigencies of cyber investigations[36]. India's reluctance to accede to the Budapest Convention on Cybercrime limits its access to faster digital evidence-sharing frameworks and leaves investigators isolated in global probes[37].

---

[33] Council of Europe, *Status of Budapest Convention Signatories* (2024).

[34] Jain R, 'Dark Web Attribution: Challenges and Innovations' (2023) 4 *JNLU Cyber Law Review* 112 (2023).

[35] *Bharatiya Sakshya Adhiniyam, 2023*, ss 61, 63.

[36] Ministry of Home Affairs, *Cybercrime Investigation Challenges in Transnational Contexts* MHA White Paper Series, Vol. III (2023).

[37] Council of Europe, *Budapest Convention on Cybercrime — Country Status* (2024).

Forensic deficiencies form a third, crippling constraint. A 2023 audit by the Ministry of Home Affairs found that only 11% of Indian police districts were equipped with digital forensic labs capable of handling blockchain forensics, darknet scraping, or crypto wallet analysis[38]. More critically, the Bharatiya Sakshya Adhiniyam, 2023 mandates strict compliance with electronic record authenticity and chain of custody under Sections 61 and 63, which require accurate metadata logging, secure storage, and digital signature verification for admissibility[39]. These are frequently compromised in real-world scenarios due to poor infrastructure, insufficient training, and lack of forensic continuity.

Case studies vividly illustrate this fragility. The GainBitcoin scam involved the laundering of over ₹20,000 crore through a series of pseudo-anonymous wallets layered across blockchain and dark web interfaces[40]. Despite Enforcement Directorate (ED) intervention, only partial asset recovery was achieved, and prosecutors failed to conclusively link the crypto assets to predicate offences due to evidentiary breakdowns. In 2023, ED seizures of digital wallets linked to ransomware gangs in Hyderabad and Mumbai stalled after suspects refused to divulge seed phrases, and forensic tools failed to decrypt wallet keys within a legally tenable timeline[41].

Another major limitation is inter-agency dissonance. Investigative functions are dispersed across police cyber cells, CERT-In, the FIU-IND, the RBI, and the Enforcement Directorate, each functioning under separate statutory mandates. This disaggregation leads to procedural inconsistencies, duplicated effort, and bureaucratic friction, particularly when dealing with evolving threats like ransomware-as-a-service or SIM swap fraud[42].

These systemic weaknesses can be theorised using the Digital Deterrence Framework, which posits that the low probability of detection and enforcement emboldens cybercriminals to scale operations without fear of legal consequence[43]. Similarly, the Cyber Forensics Capability Model underscores the necessity of real-time data acquisition, chain of custody, and cross-platform correlation elements severely lacking in India's investigative landscape.

Ultimately, the convergence of legal obsolescence, technological sophistication, and institutional disjointedness produces an investigative architecture that is reactive, uncoordinated, and increasingly outpaced by algorithmic criminality.

Comparative Legal Insights: What Can India Learn?

India's fragmented response to darknet-enabled financial cybercrime stands in sharp contrast to the proactive, ecosystemic strategies adopted by several jurisdictions. While India continues to rely on outdated techno-legal provisions and siloed institutional action, countries like the United States, members of the European Union, and

---

[38] Ministry of Home Affairs, *National Audit of Cyber Forensic Infrastructure*, Report No. 29 (2023).

[39] Basu D, 'Chain of Custody Under the BSA: Procedural Innovations and Evidentiary Hurdles' 12(1) *ILI Law Review* 98 (2024).

[40] Business Standard, 'GainBitcoin Scam: Crypto Kingpin Laundered ₹20,000 Crore' (2023).

[41] Enforcement Directorate, *Press Briefing on Cryptocurrency Seizures and Legal Follow-Up* (2023).

[42] Sharma V, 'Institutional Fragmentation in India's Cybercrime Response: A Structural Analysis' 18 *ILI Law Review* 88 (2024).

[43] Nye J S, 'Deterrence and Dissuasion in Cyberspace' 4(2) *International Security* 44 (2017).

Australia have embraced a more integrated model of regulation, enforcement, and intelligence co-production. These jurisdictions provide compelling templates for structural reform and legal innovation.

In the United States, enforcement against darknet financial crime has matured through operations like Disruptor (2020), which led to over 170 arrests across multiple jurisdictions and the seizure of 500 kilograms of drugs and USD 6.5 million in cash and cryptocurrency assets[44]. What distinguishes the U.S. approach is the tactical use of undercover cyber-operations, the embedding of digital assets task forces within the FBI, and the collaboration with blockchain analytics firms like Chainalysis and Elliptic[45]. The evidentiary admissibility of blockchain traces, upheld in decisions like *United States v. Sterlingov* (2022), has established jurisprudence that equates blockchain audit trails with forensic DNA subject to authenticity and reliability tests[46].

The European Union, through Europol's Joint Cybercrime Action Taskforce (J-CAT), demonstrates how multilateral coordination, coupled with policy uniformity, enables cross-border crime suppression. J-CAT's operational synergy among law enforcement, prosecutors, and intelligence agencies has disrupted over 30 major darknet operations since 2019[47]. Additionally, the General Data Protection Regulation (GDPR), while often seen as a privacy statute, contains nuanced carve-outs under Articles 23 and 89 that allow the processing of personal data for criminal investigation and archival purposes, ensuring compliance and prosecutorial latitude[48].

Australia provides lessons in legislative foresight. The Anti-Money Laundering and Counter-Terrorism Financing Act, 2006, was amended in 2018 to bring digital currency exchange providers under AML/CTF obligations, making KYC mandatory and traceability enforceable[49]. Australia's law enforcement agencies, including the Australian Federal Police (AFP) and AUSTRAC, have also pioneered proactive crypto-asset seizure mechanisms, securing judicial warrants to freeze assets even before formal charges are framed[50]. Their crypto-enabled asset recovery toolkit includes public-private cooperation with centralized exchanges, intelligence-sharing protocols, and pre-charge evidentiary preservation.

These international models reveal key lessons for India:

- Crypto-Specific Legislation: Unlike India's reliance on the PMLA and RBI circulars, these jurisdictions have clear statutory definitions, compliance mandates, and enforcement powers tailored to virtual assets.
- Joint Investigative Task Forces: India lacks a dedicated inter-agency mechanism like J-CAT. Institutional fragmentation continues to weaken real-time collaboration between CERT-In, FIU-IND, and state police units.

---

[44] United States Department of Justice, *Operation Disruptor: Global Darknet Takedown* (Press Release, 2020).

[45] Chainalysis, *Crypto Crime Report 2021: Darknet Markets and Ransomware* (2021).

[46] *United States v Sterlingov, Case No. 21-cr-00399 (District Court for the District of Columbia, 2022).*

[47] Europol, *J-CAT: Joint Cybercrime Action Taskforce Annual Report* (2023).

[48] General Data Protection Regulation (GDPR), arts 23, 89; Kuner C, 'Data Protection in the Context of Criminal Investigation' 16 *International Data Privacy Law* 205 (2020).

[49] AUSTRAC, *Regulation of Digital Currency Exchange Providers under AML/CTF Act* (2018).

[50] Australian Federal Police, *Proactive Cryptocurrency Seizure Framework* (2022).

- Evidentiary Chain Standardisation: The admissibility of blockchain evidence is facilitated abroad by uniform digital evidence protocols, chain-of-custody frameworks, and digital forensics capacity standards still evolving under the Bharatiya Sakshya Adhiniyam, 2023[51].
- Private Sector Intelligence Partnerships: Legal frameworks in the U.S. and Australia require crypto exchanges, ISPs, and hosting services to share threat intelligence and report suspicious transactions something India's current regulatory matrix only encourages, but does not mandate.

From an analytical perspective, these jurisdictions exhibit systemic coherence, not merely aggressive prosecution. They reflect the value of designing cybercrime frameworks that balance surveillance, privacy, evidentiary integrity, and transnational cooperation. A deterrent architecture is effective only when legal tools, institutional design, and investigative capacity converge seamlessly a strategic coherence India must urgently replicate.

Reimagining India's Legal and Investigative Paradigm

India's struggle to counter darknet-enabled financial crime is not simply a question of legal deficiency, but of systemic incoherence a mismatch between the scale of digital threat and the fragmented institutional and normative responses. While recent developments like the Digital Personal Data Protection Act, 2023 and Bharatiya Nyaya Sanhita, 2023 show legislative awakening, they do not address the unique, cross-sectoral challenges posed by the intersection of anonymity, crypto-economics, and algorithmic evasion. What India requires is not piecemeal reform but a paradigm shift toward a purpose-built legal and investigative architecture.

A. Toward a Comprehensive Digital Financial Crime Act

A dedicated Digital Financial Crime Act (DFCA) is essential to consolidate scattered provisions under the IT Act, PMLA, BNSS, and RBI circulars into a cohesive statute. The proposed DFCA should:

• Define and criminalize darknet-enabling conduct: marketplace hosting, crypto obfuscation (tumbling/mixing), and ransomware-as-a-service operations.
• Mandate Know-Your-Customer (KYC) and Suspicious Transaction Reporting (STR) compliance for Indian-hosted crypto platforms and VPN providers.
• Establish investigative protocols for lawful interception, blockchain forensics, and cross-border mutual legal assistance[52].
Such a law would move India from reactive enforcement to a preventive and adaptive framework, aligned with FATF's Recommendation 15 on virtual assets and their service providers[53].

[51] Singh R, 'Blockchain Evidence under the Bharatiya Sakshya Adhiniyam: A Forward-Looking Appraisal' 19(2) *ILI Law Review* 14 (2024) .
[52] Duggal P, *Cyber Law* (6th edn, LexisNexis) 217 (2023).
[53] Financial Action Task Force (FATF), *Guidance for a Risk-Based Approach to Virtual Assets and VASPs* (2021).

B. Capacity-Building Through Judicial and Forensic Reform

The Bharatiya Sakshya Adhiniyam, 2023 introduces structural change in the evidentiary regime, but it must be paired with capacity-building mechanisms:

• Judicial training modules on blockchain traceability, metadata authentication, and AI-generated deepfakes are critical to ensure consistent evidentiary appraisal.
• Courts must be equipped to handle chain-of-custody integrity in complex cases involving encrypted data and distributed storage systems[54].

These reforms align with the UNODC's Cybercrime Repository recommendations on judicial preparedness in developing nations[55].

C. Institutional Reforms: A Centralised Dark Web Crime Task Force

India's enforcement architecture is siloed, with the CBI, CERT-In, FIU-IND, MHA, and state cyber cells often working in disjointed silos. A Centralised Dark Web Crime Task Force, modelled on Europol's J-CAT, should be created under the Ministry of Home Affairs, with integrated blockchain intelligence, crypto-asset tracing, and cyber-forensic analytics divisions. This task force must:

• Operate with legal interoperability across state lines.
• Interface with foreign law enforcement through the Ministry of External Affairs for cross-border intelligence.
• Develop real-time alert systems for darknet financial crime indicators, leveraging partnerships with ISPs and crypto exchanges[56].

D. Doctrinal Updates to Core Legislation

Both the IT Act, 2000 and BNSS, 2023 remain technologically under-ambitious. Reforms must:

• Recognize anonymity infrastructure VPNs, onion routing, mixers as regulatory targets, without undermining legitimate privacy uses.
• Create offences for AI-enhanced scams, synthetic identity fraud, and deepfake-based financial deception, supported by minimum evidentiary thresholds and admissibility standards.
• Amend search and seizure provisions to allow on-chain evidence capture and remote forensic imaging, under judicial supervision.

These doctrinal shifts will harmonize India's legal system with emerging global standards, such as the Budapest

---

[54] Sharma R, 'Admissibility of Blockchain Evidence under BSA 2023' 8(1) *Journal of Digital Law and Policy* 112 (2024).
[55] United Nations Office on Drugs and Crime (UNODC), *Cybercrime Repository: Judicial Capacity Building* (2022).
[56] Singh A, 'Darknet Crime and Indian Enforcement Architecture' 18 *National Law School Journal* 145 (2023).

Convention on Cybercrime, which emphasizes dual criminality and evidence collection across jurisdictions[57].

E. Technological Integration: Blockchain for Asset Tracing and Surveillance

The future of enforcement lies in real-time intelligence. India must integrate blockchain analytics and digital forensics platforms such as Chainalysis Reactor or open-source tools like GraphSense into the standard toolkit of financial surveillance authorities. These platforms allow:

- On-chain visualization of fund flows.
- Risk-scoring of wallets and transactions.
- Integration with Suspicious Activity Reports (SARs) and foreign watchlists.

The Financial Intelligence Unit (FIU-IND) and Enforcement Directorate (ED) must be empowered to deploy such tools with statutory legitimacy, not mere operational discretion.

India's digital finance governance is at a crossroads. Mere augmentation of punitive statutes cannot substitute for institutional redesign, technological enablement, and normative reimagination. A systemic overhaul rooted in doctrinal innovation, investigative clarity, and global best practices is imperative to safeguard India's digital economy from the hidden algorithms of darknet crime.

Conclusion: Toward a Technologically Literate Rule of Law

India stands on the precipice of a new digital era where financial anonymity, algorithmic crime, and borderless economies are reshaping the landscape of criminal enterprise. The darknet is no longer a fringe zone; it has become a thriving parallel economy underpinned by crypto-assets, decentralised identity tools, and untraceable communication protocols. This evolution has outpaced the current legal, investigative, and institutional frameworks, rendering many of India's enforcement tools obsolete in both design and scope.

A. Reaffirming the Urgency of Legal Modernisation

The danger of regulatory inertia is no longer speculative. India's delayed response to financial cybercrime particularly in the context of the dark web and cryptocurrency laundering has resulted in enforcement paralysis, case backlogs, and underreporting[58]. As high-profile scams involving crypto assets and anonymous darknet vendors proliferate, the state's credibility and its capacity to uphold the rule of law face existential challenges. The Bharatiya Nyaya Sanhita, 2023 and the Digital Personal Data Protection Act, 2023, though progressive in tone, lack granularity to deal with the multifaceted nature of darknet-driven financial crime.

---

[57] Council of Europe, *Budapest Convention on Cybercrime: Explanatory Report* (2001).

[58] Singh R, 'Dark Web Threats and India's Legal Vacuum' (2024) 12 *Indian Journal of Cybersecurity Law* 92.

B. Anchoring Legal Coherence, Institutional Capacity, and Crypto-Literacy

A sustainable response must involve triangulation of three critical axes:

• Legal Coherence: A unified legislative framework such as a Digital Financial Crime Act would harmonise the fragmented ecosystem of the IT Act, PMLA, and BNSS, enabling targeted criminalisation of darknet-enabling conduct and crypto-based laundering[59].
• Institutional Capacity-Building: Cyber forensic labs, judicial academies, police training colleges, and financial intelligence units must be resourced and digitally literate, able to interpret blockchain trails, decrypt anonymised data, and maintain evidentiary integrity[60].
• Crypto-Literacy and Public-Private Intelligence Partnerships: Combating dark web financial crime also requires collaboration with virtual asset service providers (VASPs), ISPs, crypto exchanges, and financial institutions. The legal regime must encourage intelligence sharing while safeguarding individual rights under constitutional norms.

This tripartite framework is consistent with UNODC guidelines for digital crime prevention and reflects FATF's risk-based compliance approach to virtual assets[61].

C. Toward Normative Resilience: Future-Proofing Indian Cyber Law

Ultimately, India must reimagine the rule of law itself not as a static edifice, but as a technologically literate, future-proof architecture. The legal system must anticipate, rather than merely react to, emerging threats such as deepfake financial fraud, synthetic identity generation, automated ransomware, and DAO-based criminal organisations. Normative flexibility coupled with doctrinal precision must become the cornerstone of digital criminal justice.

A technologically literate rule of law does not abandon constitutionalism for convenience. Rather, it ensures that state sovereignty, individual rights, and financial integrity are preserved even in the murky corridors of the dark web. This is not merely a matter of enforcement it is a democratic imperative.

---

[59] Duggal P, *Cyber Law* (6th edn, LexisNexis 2023) 234.

[60] Sharma M, 'Chain of Custody and Blockchain Evidence under BSA, 2023' 19(2) *NALSAR Tech Law Review* 117 (2024).

[61] United Nations Office on Drugs and Crime (UNODC), *Guidelines on the Prevention of Digital Crime in Developing Countries* (2022); Financial Action Task Force (FATF), *Updated Guidance on Virtual Assets and VASPs* (2021).

ROLE OF JUDICIARY IN CURBING SOCIO-ECONOMIC OFFENCES AND ENSURING SUSTAINABLE DEVELOPMENT

Avni Kritika
Assistant Professor, Impact College of Law, Patna

ABSTRACT

In the context of sustainable development, the judiciary plays a vital role in addressing socio-economic offences such as corruption, tax evasion, money laundering, corporate fraud, and environmental violations. These offences not only erode public trust but also divert critical resources away from developmental priorities, impeding progress toward the Sustainable Development Goals (SDGs).

This paper examines the Indian judiciary's role in curbing such offences through landmark verdicts, legal interpretations, and the strategic use of Public Interest Litigations (PILs). It highlights the constitutional empowerment of courts under Articles 32 and 226, and the establishment of specialised courts for economic crimes. These judicial interventions have contributed significantly to enhancing accountability and governance.

However, challenges persist—including judicial delays, political interference, and limited expertise in complex financial matters. By analysing recent case law and institutional trends, the paper identifies structural and procedural gaps, proposing reforms aimed at improving judicial efficiency, independence, and capacity.

Ultimately, the study argues that a robust and proactive judiciary is essential not only for upholding the rule of law but also for fostering inclusive and sustainable national development.

Key words: *Socio-Economic Offences, Sustainable Development, Judicial Role Corruption, Governance.*

Introduction

"Sustainable development" means meeting present needs without compromising future generations[1]. Socio-economic offences – such as corruption, tax evasion, money-laundering, corporate fraud and environmental violations – target India's economic stability and social fabric[2]. These offenses misappropriate public resources, diminish faith in institutions, and obstruct developmental objectives, such as undermining Sustainable Development Goal 16 regarding transparent and responsible governance. In India, significant incidents such as the 2G spectrum scandal and widespread environmental contamination have underscored the peril these offenses present to prosperity. The Indian judiciary has assertively utilized its writ powers (under Articles 32 and 226), frequently through Public Interest Litigations (PILs), to ensure accountability and safeguard rights. The Hon'ble Supreme Court has construed Article 21 (the right to life) to encompass the right to a clean and healthy environment, rendering environmental protection justiciable. This paper examines how India's courts have utilized its constitutional authority to mitigate socio-economic offenses and promote sustainable development, while also acknowledging ongoing obstacles.

Constitutional Framework and Judicial Activism

The Constitution authorizes the Hon'ble Supreme Court and High Courts to issue writs for the enforcement of basic rights. Through the application of Articles 32 and 226, the superior judiciary has formulated novel judicial remedies by broadening standing and incorporating international norms. As Hon'ble Justice Hima Kohli has

[1] Report of the World Commission on Environment and Development- Our Common Future, United Nation, 1987

[2] Prathyusha, K. M., and T. Vaishali. "Laws to Prevent Socio-Economic Offences in India." *Indian Journal of Legal Review (IJLR)*, vol. 4, no. 4, 2024, APIS–3920–0001, ISSN 2583-2344. https://ijlr.iledu.in/wp-content/uploads/2024/12/V4I4107.pdf.

highlighted, courts "have played a pivotal role in interpreting Article 21 for redressal of environmental grievances," creating strategies that mix social justice with human rights. In effect, the courts have read ecological and socio-economic costs into the right to life. For example, a Constitution Bench decided that Article 21 empowers citizens to seek the writ jurisdiction directly for environmental concerns, calling the writ remedy a "powerful and expeditious tool" for such grievances. This judicial creative reach – visible in scores of PILs – has been important to pursuing pollution, corruption, and other public damage. Article 48A and Article 51A(g) explicitly advocate for environmental conservation. The judiciary has helped operationalize those mandates, treating infractions as concerns affecting fundamental rights.

Public Interest Litigation

Since the 1980s, PIL has become the major technique for enforcing socio-economic justice. The courts modified the usual *"locus standi"* requirements and permitted any public-spirited person or group to bring a writ petition on behalf of injured populations. As a result, several environmental and anti-corruption cases have been initiated by NGOs and citizens on a pro gratis basis. This activism has included suits to prevent indiscriminate mining, protect livelihoods of adivasis (e.g. *Banwasi Sewa Ashram v. U.P., AIR 1987 SC 374*), challenge illicit mining, and enforce disclosure of government schemes (e.g. under Right to Information Act). In essence, PIL has extended access to justice and empowered the judiciary to address policy gaps, frequently ahead of legislation, to defend sustainable development objectives.

Judicial Intervention in Environmental and Socio-Economic Offences in India

Indian courts – especially the Hon'ble Supreme Court and High Courts – have played an assertive role in policing environmental and socio-economic crimes, typically through Public Interest Litigations. Landmark verdicts have enforced environmental regulations, even against high□profile projects, and clamped down on corruption in telecom, finance and corporate sectors.

Environmental Offences: Judicial Responses

● **Mining and Natural Resources:** Courts have repeatedly struck at illegal mining and resource diversion. For example, in *Vanashakti v. Union of India*[3], a two-judge SC bench (Hon'ble Justices Oka & Bhuyan) struck down government "amnesty" schemes that legalized past mining/industrial projects without prior clearance. The Court held that ex-post facto environmental clearances violate the Environment (Protection) Act, 1986 and Article 21's guarantee of a "pollution-free environment"[4]. Similarly, in *Manohar Lal Sharma v. Principal Secretary*[5], the SC declared all coal block allocations since 1993 "illegal" for lacking any statutory basis[6]. Earlier cases *Common*

[3] Vanashakti v. Union of India 2025 SCC OnLine SC 1139

[4] Bhargava, Vanita, Nandita Chauhan, and Tijil Thakur. "Supreme Court Rules Against Ex-Post Facto Environment Clearance." *Lexology*, Khaitan & Co, 22 May 2025, https://www.lexology.com/library/detail.aspx?g=d47417c2-30c5-47e1-a686-ae61cb0523eb. Accessed 12 June 2025

[5] Manohar Lal Sharma v. Principal Secretary and Others (2014) 3 SCC 163

[6] Bhatia, Gautam. "Guest Post: The Supreme Court's 'Coalgate' Judgment – I." *Constitutional Law and Philosophy*, 29 Aug. 2014, indconlawphil.wordpress.com/2014/08/29/guest-post-the-supreme-courts-coalgate-judgment-i/. Accessed 14 June 2025.

Cause v. Union Of India[7] and *Alembic Pharmaceuticals v. Rohit Prajapati*[8] had likewise held retrospective clearances contrary to the EIA Notification (1994/2006) and fundamental environmental principles[9]. These rulings underscore that mining licenses or clearances must follow strict statutory procedure – e.g. public hearings and prior Environmental Clearance – and cannot be regularized after the fact.

● **Real Estate and Construction:** Courts have challenged unrestrained development that threatens ecosystems. In *Vanashakti*, the Hon'ble Supreme Court highlighted that housing, industrial and mining developers (including big PSUs and realty businesses) willfully broke EIA laws and cannot later claim an ownership in their illegality. The Court forbade further "grandfathering" of unlawful developments. Hon'ble High Courts have similarly ordered demolition of unauthorized projects on ecologically sensitive territory (such as Aravalli hills and floodplains). For instance, in April 2025 the Supreme Court stayed a Punjab–Haryana HC demolition drive targeting thousands of unauthorized homes in Gurugram, noting that homeowners had paid taxes and needed time to seek relief[10]. While that order was procedural, it indicates friction between development and environmental/zoning rules. In general, judges urge that "development cannot be at the cost of the environment", underscoring that real-estate ventures must satisfy environmental screens like other industries.

● **Industrial Pollution:** The Indian judiciary has pushed pollution control through PILs. In the 1980s–90s, Justice M.C. Mehta's petitions prompted the SC to impose absolute liability (for e.g. *the Oleum gas leak case*[11]), require closure of polluting companies (e.g. illegal tanneries, coke plants, etc.), and develop environmental guidelines. Notably, *Vellore Citizens Welfare Forum v. Union of India* (1996)[12] held the "polluter pays" and "sustainable development" principles integral to Article 21. In *Common Cause v. Union of India* (2017)[13], the SC provided directions for cleaning up the Bhopal gas catastrophe site. More recently, in 2020 the SC banned Tamil Nadu's Sterlite copper plant for chronic air and water violations. Across these cases, courts have applied the Environment (Protection) Act, 1986 (EPA) and sectoral statutes [The Air (Prevention and Control of Pollution) Act (1981), The Water (Prevention and Control of Pollution) Act (1974)] to restrain or sanction polluters. For example, the EPA's Section 3 - allowing the government to control the environment – was highlighted in *Vanashakti* as the very statute meant to give "effect" to the Article 21 right to clean environment.

● **Infrastructure and Development Projects:** Large projects (dams, highways, power plants) have also been subjected to judicial scrutiny. In *Narmada Bachao Andolan v. Union of India* (2000)[14], the SC weighed displacement and ecology against development, modifying rehabilitation conditions under Article 21. In *T.N. Godavarman Thirumulpad v. Union of India* (1996-onwards)[15], a series of orders protected forests from

---

7 Common Cause v. Union of India & Ors (2017) 9 SCC 499

8 Alembic Pharmaceuticals Ltd v. Rohit Prajapati (2020) 17 SCC 157

9 Goswami, Subhrajit. "Supreme Court Quashing Post-Facto Environmental Clearances Is a Timely Reminder That Long-Term Development Rests on Foresight — Not Shortcuts." Down To Earth, 19 May 2025, https://www.downtoearth.org.in/environment/supreme-court-quashing-post-facto-environmental-clearances-is-a-timely-reminder-that-long-term-development-rests-on-foresight-not-shortcuts. Accessed 10 June 2025.

10 Top Court Stays High Court Order to Demolish Illegal Constructions in Gurugram's DLF." NDTV, Indo-Asian News Service, 4 Apr. 2025, https://www.ndtv.com/india-news/supreme-court-stays-haryana-high-court-order-to-demolish-illegal-constructions-in-gurugram-dlf-8088825. Accessed 14 June 2025.

11 MC Mehta v. Union of India (1987) 1 SCC 395

12 Vellore Citizens Welfare Forum v. Union of India (1996) 5 SCC 647

13 Common Cause v. Union of India & Ors (2017) 9 SCC 499

14 Narmada Bachao Andolan v. Union of India (2000) 10 SCC 664

15 T.N. Godavarman Thirumulpad v. Union of India AIR 1997 SC 1228

encroachment during development. More recently, the SC (Green Benches) routinely hear PILs on railway and road projects harming rivers or forests. For instance, the Yamuna pollution case (*Go Green Earth Foundation v. Union of India, 2025*)[16] tackled industrial effluent in Delhi's river stretch (sourced via petitions). These interventions cite Article 21 and EPA, directing stronger safeguards (e.g. mandatory Environmental Clearances or risk mitigation) whenever projects impinge on the environment.

● **Statutory Frameworks and Interpretations:** Indian courts have rigorously examined environmental statutes. The EPA 1986, established to preserve Article 21, has been read stringently: *Vanashakti* determined the government cannot diminish EPA's EIA system by "fixing" infractions after the fact. The EIA Notification (2006) was judged unambiguously that no project can continue before clearance; ex post facto schemes contradict its simple words (as held in Common Cause and Alembic). Courts have also annulled government policies — knocking down the 2017-21 "amnesty" Notifications and SOPs under EPA and demanding punitive deposits for violators. Similarly, the Forest Conservation Act, 1980 and Coastal Regulation Zone restrictions have been enforced by courts to prohibit improper land-use changes. In essence, where statutory safeguards exist (EPA, Wildlife Protection Act, Forest Act, etc.), courts have often reinforced them rather than tolerate shortcuts that compromise environmental rights.

● **Telecom and Spectrum Scandals:** India's apex court has taken a hard line on major corruption cases. In the landmark case of *Centre for Public Interest Litigation v. Union of India* (2012)[17], arising from the 2G spectrum scam, a Constitution Bench cancelled 122 2G telecom licenses allotted in 2008 by then-Minister A. Raja. The Court (Singhvi & Ganguly, JJ) declared the first-come-first-served policy "unconstitutional and arbitrary"[18], and ordered that all future spectrum be auctioned. This verdict — in PILs by Subramanian Swamy and CPIL – highlighted transparency and equality in public resource allocation. (See Business Standard report: "SC cancels 122 telecom licences".) In sum, 2G jurisprudence underlines courts' propensity to throw down executive transactions tainted by corruption or favoritism.

● **Resource Allocation and Other Scams:** In *M.L. Sharma (Coalgate)* (2014), the SC concluded that absent a legislative auction procedure, past coal block allocations were unlawful. This "Coalgate" ruling (dismissed petitions declaring allocations unconstitutional) remanded the subject for future auction procedures. Other high-profile PILs include *Common Cause v. Union of India & Ors* (2001)[19] when the SC overturned discretionary permits for educational institutes; and *Niranjan Das Gupta v. C.B.I* (2013), revoking tainted permits. While not all corruption suits reach SC, these examples demonstrate courts applying Articles 14 and 32 to invalidate arbitrary allocations in telecom, coal, and other sectors.

● **Banking and Financial Frauds:** Private banking scams (e.g. Punjab National Bank/Nirav Modi case, Yes Bank) have generally been addressed by investigative authorities and tribunals. The SC's function has been to guarantee conformity with law in relevant processes. For example, in *Nirav Modi v. Enforcement Directorate* (2018) the Court took note of protracted pre-trial incarceration under the PMLA (2002) and reminded authorities

[16] Go Green Foundation v. Union of India Diary No. 94832024

[17] Centre for Public Interest Litigation v. Union of India (2012) 3 SCC 1

[18] "Supreme Court Cancels 122 Telecom Licences." Business Standard, 11 June 2025, https://www.business-standard.com/article/economy-policy/supreme-court-cancels-122-telecom-licences-112020300086_1.html. Accessed 10 June 2025.

[19] Common Cause v. Union of India Appeal (Civil) 3988-3939 of 2001

that accused must have speedy bail hearings – reflecting Article 21's personal liberty provision. In the Sahara-SEBI proceedings (2012), the Supreme Court maintained SEBI's competence to supervise unlisted deposit schemes, ordering Sahara to repay ₹24,000 crore collected from investors. (*Sahara India Real Estate Corp. Ltd. v. SEBI* affirmed SEBI's jurisdiction even over unregistered entities.) These verdicts bolstered legislative enforcement (Securities Laws, PMLA) and highlighted that huge financial firms are not beyond regulatory reach.

● **Corporate Misconduct and Markets:** The Satyam fraud (2009) led to CBI prosecutions, and in 2019 the trial court convicted R. Raju on corporate fraud charges. While the SC has not yet decided final appeals in Satyam, other cases have seen judicial probes. For example, insider trading and market manipulation cases (insider trading regs under SEBI Act) have been upheld by courts. More broadly, courts have enforced Article 21 rights (to a fair trial) even in economic violations, and reaffirmed the role of boards and auditors under the Companies Act. (E.g. SC in *SEBI v. Kanwal Rekhi* — maintaining market restrictions.

● **Money Laundering (PMLA):** The Prevention of Money Laundering Act (2002) is currently a vital tool against economic crime. Courts have construed PMLA severely but fairly. In *Navinchandra R. v. Union of India* (2015), the SC stated that PMLA processes must follow CrPC safeguards, and convicted offenders should be entitled for remission and bail like under other laws. Similarly, *Bharat J.C. Patel v. CBI* (2018) in the Nirav Modi situation underlined that PMLA is not an anti-terror law and the liberty of the accused must be balanced with investigation demands. In 2021, *Tukaram Omble v. Central Bureau of Investigation,* the Court banned long arbitrary detentions by CBI/ED and emphasized on speedy trial timeframes. Thus, while the ED pursues high-value money-laundering cases, courts have set constitutional constraints (Article 21 due process) on enforcement. (These principles complement the statutes – e.g. PMLA Sections 3, 45 – by mandating quick cognizance and bail for suspects.)

Constitutional Foundations and Public Interest Litigation

Across both environmental and economic cases, the Supreme Court has invoked basic rights and PIL jurisdiction to justify action. Crucially, Article 21 has been expansively read to cover environmental quality and public health. For instance, the Vanashakti judgment (2025) reiterates that "under Article 21… the right to live in a pollution-free environment is guaranteed," and even incorporates this requirement in the EPA itself. The Court stated that extensive air and water pollution infringe the right to life and health of all citizens. This constitutional responsibility – paired with Article 51A(g) (basic duty to safeguard the environment) – supports most eco-PILs. In prior decisions like *Subhash Kumar v. State of Bihar* (1991)[20] and *Vellore Citizens Welfare Forum v. Union of India* (1996), the SC initially acknowledged that "the right to life" encompasses enjoyment of natural resources and clean surroundings, laying the foundation for further rulings.

Similarly, PIL has been the tool for resolving socio-economic issues. The courts have loosened the locus-standi requirement to allow citizens and NGOs to suit on behalf of victims (see famous PILs: *Hussainara*

[20] Subhash Kumar v. State of Bihar 1991 AIR 420

Khatoon v. State of Bihar[21] – prisoners' rights; *Bandhua Mukti Morcha v. Union of India*[22] – bonded labour; MC Mehta series – environment). In corruption instances, public-spirited petitions (by Swamy, CPIL, NGOs) are often filed under Article 32 or 226 to enforce Articles 14 (equality) and Article 32 or Article 226 directly. For example, the 2G spectrum dispute was pursued as a series of PILs alleging infringement of equality and transparency rights. Through these constitutional authorities, judges have held the government and strong interests accountable when environmental or financial misdeeds affect citizens.

Finally, courts frequently cite the relevant statutes in their reasoning. Environmental orders routinely reference the Environment (Protection) Act, Air/Water Acts, Wildlife/Forest laws and the EIA Notification[23]. Anti-corruption rulings use the Prevention of Corruption Act (1988), Prevention of Money Laundering Act (2002) and Companies Act regulations. The trend has been to interpret these statutes purposively: for example, SC rulings have reduced the scope of "criminal misconduct" in the PC Act, and defined ED's responsibility under PMLA, therefore balancing enforcement with rights. Overall, the judiciary's environmental and white-collar jurisprudence rests significantly on constitutional rights (life, equality, transparency) and legislative conformity, as indicated by the various decisions noted above.

Specialized Courts and Institutional Reforms

Recognizing that white-collar offenses demand skill and speed, India's legislation provides for Special Courts. The Supreme Court endorsed this approach in In *Re: Special Courts Bill*[24] (1982), confirming that special courts are constitutional so long as their jurisdiction is reasonable. It remarked that Special Courts were constituted "to expedite the resolution of severe and complex cases" (particularly economic offences) and to protect judicial efficiency. Today, special PMLA courts, special CBI courts, and Economic Offences Courts are empaneled under various statutes (PMLA, FEMA, NIA, etc.) to focus on complicated financial cases.

In *In Re: Expeditious Trial of Section 138 NI Act Cases* (2022), the Supreme Court again pressed for more special courts, noting the alarming pendency (over 33 lakh cheque-bounce cases) and exhorting that **each state must constitute adequate NI-Act special courts** to resolve these fraud cases swiftly[25].

Legislative support has followed judicial calls: the Enforcement Directorate established PMLA courts, and the government frequently notifies new judgeships for economic offences. The 47th Law Commission (1972) had already advocated special courts for anti-corruption and economic offences, and current policy actions (e.g. fast-track courts for severe crimes, expanded ED staffing) reflect this. By diverting challenging cases to particularly trained judges and minimizing general court backlog, these systems aim to increase enforcement against socio-economic crimes.

---

[21] Hussainara Khatoon v. State of Bihar 1979 AIR 1369

[22] Bandhua Mukti Morcha v. Union of India & Ors AIR 1984 SCC 802

[23] Singh, Amita. "The Supreme Court on the Ex Post Facto Environment Impact Assessment?" SCC Online (SCC Times), 5 June 2025, https://www.scconline.com/blog/post/2025/06/05/the-supreme-court-on-the-ex-post-facto-environment-impact-assessment/. Accessed 4 June 2025

[24] Re: The Special Courts Bill 1978 v. Union of India AIR 1979 SC 478

[25] Mishra, Shivam. "Elevating Justice: The Imperative Role & Challenges of Special Courts in Economic Offences Prosecution." Mondaq, 3 Dec. 2024, www.mondaq.com/india/white-collar-crime-anti-corruption-fraud/1554938/elevating-justice-the-imperative-role-challenges-of-special-courts-in-economic-offences-prosecution. Accessed 4 June 2025.

Challenges to Judicial Enforcement

Despite its proactive jurisprudence, the judiciary faces persistent constraints:

- **Backlogs and Under-Staffing:** India has an acute shortage of judges. A 2025 Justice Report found only about 15 judges per million people (21,285 judges in total), far below the Law Commission's recommended 50 per million. High Court vacancies remain around 20–30%, and district courts have average caseloads of 2,200 cases per judge – with some high courts (e.g. Allahabad) seeing ~15,000 cases per judge[26]. Such overload means even eligible socio-economic cases can take years to reach a verdict, diluting deterrence. Undoubtedly, judicial delays are a major gap in curbing these offences.

- **Political and Executive Influence:** Courts have repeatedly warned about interference. For example, in 2013 Justice Lodha of the SC denounced the CBI as a "caged parrot" of the executive[27], highlighting how political pressure can stall investigations. More recently, the Court voiced concern over vindictive use of agencies between Centre and states, seeking a neutral mechanism. At times, even after a ruling limits interference (e.g. Vineet Narain), the legislature has reinserted protections (as in Section 17A of the PC Act, 2018). Such push-and-pull indicates that judicial statements alone are not always adequate – agency independence remains a battleground.

- **Limited Expertise and Technical Evidence**: Economic offenses often entail complicated financial tools, cyber traces, and global networks. Judges (educated in law) may lack domain competence, making them reliant on expert witnesses or forensic accountants. This can slow trials and lead to issues in fact-finding. For instance, tax evasion using cryptocurrency or complicated shell businesses typically outpaces the rate of legal reform. The judiciary has tried to bridge this by issuing practice directives (e.g. lab-intensive evidence in pollution cases) and by advocating capacity-building, but gaps remain.

- **Resource Constraints and Public Awareness:** The justice delivery system has inadequate resources — overcrowded courts, overworked police, and shortage of forensic labs. Moreover, ordinary folks may be uninformed of legal remedies like RTI or PIL. Without proactive enforcement, even strong judicial rulings (such cleanup directives or recovery schemes) require follow-through by authorities. The courts routinely enjoin governments or agencies to report progress, but structural obstacles (corrupt officials, administrative lethargy) might linger beyond the judiciary's reach.

Reforms and the Path Ahead

The courts themselves have suggested reforms to amplify judicial impact. Key recommendations include:

- **Expand Judicial Capacity:** Governments must clear judge vacancies and add new posts. The ET Report (2025) and Law Commission have urged raising judge strength dramatically. Special benches or fast-track divisions for corruption, money-laundering, and environmental cases can reduce delays. Technology-enabled courts (e-filing, video hearings) should be scaled up to handle economic cases more efficiently. As *Satender Antil*

[26] Only 15 Judges Per Million Population in the Country: 2025 India Justice Report." The Economic Times, 15 Apr. 2025, https://economictimes.indiatimes.com/news/india/only-15-judges-per-million-population-in-the-country-2025-india-justice-report/articleshow/120309565.cms?from=mdr. Accessed 14 June 2025.

[27] Colvin, Ross, and Satarupa Bhattacharjya. "A 'Caged Parrot' – Supreme Court Describes CBI." Reuters, 10 May 2013, https://www.reuters.com/article/world/a-caged-parrot-supreme-court-describes-cbi-idUSDEE94901X/. Accessed 14 June 2025.

directed, bail and trial procedures should be time-bound (e.g. setting fixed weeks for bail orders)[28], and higher courts should mandate such timelines.

- **Strengthen Agency Autonomy:** To ensure compliance with judicial demands, legal safeguards are essential. For example, establishing statutory independence to entities like the CVC, ED or CBI director (as courts have advised) inhibits executive influence. The collegium system (including the CJI in appointments panels) should be kept or enlarged for anti-corruption and regulatory offices, as recent SC judgments do. "Continuing mandamus" methods – where courts keep cases open pending implementation (used in many pollution cases) – can assure long-term oversight. Legislatures may also adopt a permanent, cross-party anti-corruption commission (as the courts originally suggested) to take the judiciary's proposals forward.

- **Enhance Expertise and Investigation:** Specialized training programs for judges and investigators are needed. Workshops by enforcement authorities, partnerships with accounting bodies, and development of forensic cells in courts (as done in some states) could help. Strengthening witness protection and plea-bargaining systems would increase cooperation. The judiciary's idea of a separate Bail Act (to simplify bail provisions) or revisions to streamline offences (to eliminate frivolous litigation) should also be examined.

- **Promote Transparency and Public Participation:** Courts have observed that citizen monitoring is vital. Expanding the reach of RTI, whistleblower protections, and legal aid (for undertrials in economic offense cases) complements judicial efforts. The SC has insisted on posting court orders (for example, compelling government websites to provide environmental compliance data) — these practices should continue. The success of PILs highlights the importance of public participation; enabling NGOs and citizen groups to monitor corruption and development projects can front-load problems before courts intervene.

Conclusion

In India's constitutional scheme, an independent judiciary is indispensable for sustainable development. By vigorously enforcing the rule of law, the courts have played a key role in guarding resources and rights against misuse by the powerful. From landmark anti-corruption judgments (insulating investigative agencies) to pioneering environmental orders (prioritizing clean air and public health) – the judiciary has linked good governance with development outcomes. As the Supreme Court observed, enforcement agencies' personnel "should not now lack the courage and independence to go about their task…even where those to be investigated are prominent and powerful persons"[29].

However, the task is far from complete. Significant adjustments are needed so that judicial mandates are transformed into reality on the ground. Strengthening the judiciary (via more judges and specialized courts), safeguarding agency autonomy, and providing technological support will intensify the courts' efforts. Ultimately, only a partnership of a vigilant judiciary, transparent institutions, and an informed population can ensure that India's growth is inclusive, equitable, and truly sustainable.

---

[28] LawBhoomi. "Satender Kumar Antil vs CBI." *LawBhoomi*, 28 Mar. 2025, lawbhoomi.com/satender-kumar-antil-vs-cbi/. Accessed 14 June 2025

[29] Anand, Utkarsh. "Past Orders Also Aimed at Institutional Reforms." Hindustan Times, 3 Mar. 2023, https://www.hindustantimes.com/india-news/past-orders-also-aimed-at-institutional-reforms-101677830492258.html. Accessed 14 June 2025.

THE ROLE OF ENFORCEMENT DIRECTORATE IN COMBATING FINANCIAL CRIMES IN INDIA

Abhay Kumar Pandey
Research Scholar, Atal Bihari Vajpayee School of Legal Studies,
CSJMU, Kanpur

Avinash Shandilya
Research Scholar, Department of Law, CMP Degree College,
University of Allahabad, Prayagraj

ABSTRACT

With a focus on money laundering, foreign exchange violations, and proceeds of crime, this article explores the Enforcement Directorate's (ED) changing role in India's fight against financial crimes. Since its founding, the ED, India's specialised financial investigation agency, has seen a major expansion in its mission, authority, and operational purview. Through the prism of significant cases and legislative developments, this paper examines the ED's legal framework, investigative procedures, difficulties, and efficacy. The conversation includes critical assessments of the Foreign Exchange Management Act (FEMA) and the Prevention of Money Laundering Act (PMLA), recent court rulings that impact the ED's operations, and the fine line between constitutional protections and the effectiveness of enforcement. This article offers insights into the ED's contributions to financial integrity by placing the agency's role within India's larger economic crime enforcement landscape and international compliance frameworks. It also identifies opportunities for institutional reform to improve the ED's efficacy while maintaining procedural fairness.

Key words: *Enforcement Directorate, Financial Crimes, Money Laundering, PMLA, FEMA.*

Introduction

India's economic security and the integrity of its governance are increasingly threatened by financial crimes. The complexity and scale of illicit financial flows have increased due to growing globalization, financial system digitization, and sophisticated criminal networks, making specialized enforcement mechanisms necessary[1]. First created in 1956 as an enforcement unit under the Department of Economic Affairs, the Enforcement Directorate (ED) has become India's top agency charged with looking into serious economic crimes and upholding two important laws: the Foreign Exchange Management Act of 1999 (FEMA) and the Prevention of Money Laundering Act of 2002 (PMLA)[2].

Over the years, the ED's mission has grown significantly, evolving from a small enforcement agency for foreign exchange regulations to a comprehensive financial intelligence and investigation organization with broad authority to search, seize, arrest, and attach assets[3].

This evolution is a reflection of how financial crimes are evolving in India and how their detrimental effects on regulatory frameworks, public trust in financial institutions, and national economic interests are becoming more widely acknowledged.

---

[1] Financial Action Task Force, "Money Laundering and Terrorist Financing Typologies 2020-21," FATF-GAFI, Paris, 2021.

[2] Ministry of Finance, Government of India, "Annual Report 2021-22," Department of Revenue, p.78.

[3] Directorate of Enforcement, "History and Evolution of ED," Official Website, Government of India, accessed March 2023.

The institutional framework, legislative underpinnings, investigative techniques, and enforcement results of the ED are all examined in this article. It assesses how well the ED detects, investigates, and prosecutes complex financial crimes by looking at landmark cases, legislative changes, and court rulings. It also tackles enduring issues like capacity limitations, legal disputes over procedural provisions, jurisdictional overlaps with other agencies, and the balancing.

The Financial Action Task Force (FATF) and other international initiatives have demonstrated India's commitment to international anti-money laundering standards, and as a result, the ED's role in demonstrating India's adherence to international best practices has gained increased significance[4]. This article explores the unique Indian challenges and methods for enforcing financial crime while placing the ED's operations within this larger global framework.

Historical Evolution and Institutional Framework

Origins and Development

The stringent foreign exchange control system in place in India after independence is where the Enforcement Directorate got its start. It was first created in 1956 as the Department of Economic Affairs "Enforcement Unit" with the sole responsibility of upholding the Foreign Exchange Regulation Act, 1947 (FERA), which placed extensive restrictions on foreign exchange transactions in order to preserve limited foreign reserves[5].

The implementation of a stricter FERA in 1973, which made foreign exchange violations illegal and gave the ED broad investigative powers, greatly increased the agency's capabilities[6]. The ED's primary focus shifted to forex violations and economic intelligence gathering during this time due to India's restrictive economic policies and worries about capital flight.

India's foreign exchange regime needed to be re-evaluated in light of the economic liberalization that occurred in the 1990s. As a result, the market-oriented Foreign Exchange Management Act, 1999 (FEMA) superseded FERA and decriminalized the majority of foreign exchange violations while keeping civil penalties in place[7]. Prior to the Prevention of Money Laundering Act, 2002 (PMLA), which significantly increased the ED's mandate to include complex financial crime investigation, this shift temporarily decreased the agency's enforcement vigor[8].

A turning point was reached in 2005 when the PMLA went into effect, making the ED India's main anti-money laundering enforcement agency with the authority to look into and prosecute crimes involving the proceeds of crime[9]. The PMLA was subsequently amended, especially in 2009, 2013, and 2019, to strengthen the ED's investigative and provisional attachment powers. This reflected India's commitment to fighting financial crimes

---

4 Financial Action Task Force, "Mutual Evaluation Report: India," FATF-GAFI, Paris, 2020.

5 Foreign Exchange Regulation Act, 1947 (Act No. 7 of 1947).

6 Foreign Exchange Regulation Act, 1973 (Act No. 46 of 1973).

7 Foreign Exchange Management Act, 1999 (Act No. 42 of 1999).

8 Prevention of Money Laundering Act, 2002 (Act No. 15 of 2003).

9 Ministry of Finance, "Notification S.O. 1031(E)," The Gazette of India, July 1, 2005.

in the face of mounting concerns about corruption, black money, and terrorist financing[10].

Organizational Structure

With its headquarters located in New Delhi and zonal offices spread throughout major cities, the Enforcement Directorate functions under the Department of Revenue, Ministry of Finance[11]. A Director, usually selected from the Indian Revenue Service or Indian Police Service, leads the organization. The Director is appointed by the Central Government. Additional Directors, Joint Directors, Deputy Directors, and Assistant Directors oversee operations across various regions and specialized units within the directorate's hierarchical structure[12].

The organizational structure of the ED is divided into multiple specialized wings:

1. Investigation Wing: Charged with carrying out search operations, examinations, and evidence gathering in accordance with PMLA and FEMA[13].
2. Adjudication Wing: Manages FEMA adjudication proceedings, where violations are identified and sanctions are applied using extrajudicial procedures[14].
3. Legal Wing: Oversees prosecution under the PMLA, speaks on behalf of the ED in court and before tribunals, and offers legal advice regarding investigative issues[15].
4. Intelligence Wing: Collects and evaluates financial intelligence, creates leads for investigations, and works with other intelligence organizations[16].
5. Technical Wing: Manages technical facets of financial investigations, electronic evidence analysis, and digital forensics[17].

While collaborating with other organizations within the economic intelligence framework, such as the Serious Fraud Investigation Office (SFIO), Directorate of Revenue Intelligence (DRI), Central Bureau of Investigation (CBI), and Financial Intelligence Unit-India (FIU-IND), the ED retains operational independence[18].

Legislative Framework and Powers

Prevention of Money Laundering Act (PMLA)

The PMLA serves as the main legislative mandate for the ED and the cornerstone of India's anti-money laundering system. The PMLA, which was passed in 2002 and put into effect in 2005, makes money laundering illegal. It is defined as "directly or indirectly attempting to indulge or knowingly assisting or knowingly being a party or actually involved in any process or activity connected with proceeds of crime and projecting it as

---

10 Prevention of Money Laundering (Amendment) Acts of 2009, 2013, and 2019.

11 Enforcement Directorate, "Organizational Structure," Official Website, Government of India.

12 Department of Revenue, "Administration Report 2020-21," Ministry of Finance, Government of India.

13 Enforcement Directorate, "Investigation Wing Manual," Internal Document, 2018.

14 Foreign Exchange Management Act, 1999, Sections 13-16.

15 Prevention of Money Laundering Act, 2002, Chapter VIII.

16 Ministry of Finance, "Economic Intelligence Council: Structure and Functions," Department of Revenue, 2020.

17 Enforcement Directorate, "Digital Forensics Unit Establishment Order," Internal Document, 2017.

18 Department of Revenue, "Inter-Agency Coordination Protocol," Ministry of Finance, Government of India, 2019.

untainted property[19]."[^20] The scope of the Act includes a broad range of "scheduled offenses" that are listed in its Schedule, such as terrorism, drug trafficking, counterfeiting, corruption, fraud, and other offenses under special laws[20]. The ED's jurisdiction is activated when proceeds from these specific crimes are generated, according to the predicate offense approach.

The ED has a wide range of authority under the PMLA, including:

1. Search and Seizure: The power to search a location and take items or documents thought to be related to money laundering[21].
2. Attachment and Confiscation: The authority to temporarily seize assets obtained through illegal activity for a maximum of 180 days (extendable), with the possibility of permanent seizure after conviction[22].
3. Arrest and Custody: The power to detain people for longer periods of time than is customary in criminal proceedings when there is a reasonable suspicion of money laundering[23].
4. Recording Statements: The authority to call witnesses, question them, record their statements, and demand the production of documents[24].
5. Special Courts: Under the PMLA, cases are tried in specially designated courts using altered evidence and procedural rules[25].

The scope of the PMLA has gradually been increased by significant amendments:
The 2009 amendments expanded predicate offenses and broadened the definition of money laundering[26].

- To combat cross-border money laundering, the 2013 amendments introduced the idea of "corresponding law."[27]
- The 2015 amendments increased attachment provisions and strengthened penalties[28].
- The 2019 amendments clarified a number of procedural issues and further enhanced the ED's investigative capabilities[29].
- The Supreme Court's historic ruling in Vijay Madanlal Choudhary v. Union of India (2022) strengthened the ED's legal position by upholding the majority of the PMLA's provisions, such as its strict bail requirements and the admissibility of Enforcement Case Information Reports (ECIR)[30].

---

19 Prevention of Money Laundering Act, 2002, Section 3.
20 Prevention of Money Laundering Act, 2002, Schedule (as amended up to 2023).
21 Prevention of Money Laundering Act, 2002, Section 17.
22 Prevention of Money Laundering Act, 2002, Sections 5 and 8.
23 Prevention of Money Laundering Act, 2002, Section 19.
24 Prevention of Money Laundering Act, 2002, Section 50.
25 Prevention of Money Laundering Act, 2002, Section 43.
26 Prevention of Money Laundering (Amendment) Act, 2009 (Act No. 21 of 2009).
27 Prevention of Money Laundering (Amendment) Act, 2013 (Act No. 2 of 2013).
28 Prevention of Money Laundering (Amendment) Act, 2015 (Act No. 2 of 2015).
29 Finance (No. 2) Act, 2019, Amendments to PMLA.
30 Vijay Madanlal Choudhary v. Union of India, 2022 SCC OnLine SC 929.

Foreign Exchange Management Act (FEMA)

FEMA offers the framework for regulating cross-border economic activity and foreign exchange transactions, while PMLA deals with the criminal aspects of money laundering. In 1999, FEMA replaced the strict FERA with a more lenient policy that imposed civil penalties for most infractions instead of criminal ones[31].

***1. The ED is authorized by FEMA to*:** Investigate Contraventions: Look into possible infractions of foreign exchange laws[32].

2. Search and Seizure: Search locations and confiscate cash, documents, or other items linked to FEMA violations[33].

***3. Adjudication*:** Start the adjudication process, in which the adjudicating authority finds violations and levies sanctions[34].

***4. Compounding*:** Use compounding procedures to settle some violations, requiring offenders to pay set sums without a formal adjudication[35].

***5. Civil Penalties*:** Apply severe financial sanctions of up to three times the sum of the

The scope of FEMA includes a broad range of operations, such as:

- Foreign exchange transactions and transfers;
- Currency import and export;
- Foreign investments made by Indian citizens abroad;
- Foreign investments made in India;
- Purchasing real estate overseas; and
- Opening branches and subsidiaries outside of India.

A partial return to the punitive approach under FERA was made possible by the 2015 amendments to FEMA, which were implemented through the Finance Act and introduced criminal liability for certain violations pertaining to cross-border transfers exceeding ₹1 crore[36].

Operational Mechanisms and Investigative Procedures

Investigation Initiation and Process

ED investigations usually start in one of several ways:

1. Source Information: Information about questionable transactions or activities obtained from public sources, regulatory agencies, or financial institutions[37].

---

[31] Foreign Exchange Management Act, 1999, Statement of Objects and Reasons.

[32] Foreign Exchange Management Act, 1999, Section 37.

[33] Foreign Exchange Management Act, 1999, Section 37A.

[34] Foreign Exchange Management Act, 1999, Section 13.

[35] Foreign Exchange Management Act, 1999, Section 15.

[36] Finance Act, 2015, Amendments to FEMA, Section 13.

[37] Enforcement Directorate, "Standard Operating Procedure: Investigation Initiation," Internal Document, 2019.

2. Information Sharing: Referrals made by other law enforcement organizations, especially the Income Tax Department, State Police, or CBI, when their investigations turn up evidence of possible money laundering[38].

3. FIU Reports: The Financial Intelligence Unit-India forwards Currency Transaction Reports (CTRs) or Suspicious Transaction Reports (STRs)[39].

4. Predicate Offenses: These are automatically triggered when primary enforcement agencies register cases pertaining to scheduled offenses under the PMLA[40].

These steps are commonly included in the investigative process:

Assessing the information at hand in order to create prima facie proof of offenses is known as preliminary inquiry[41].

• ECIR Registration: The Enforcement Case Information Report, which is comparable to a First Information Report (FIR), signifies the official start of an investigation under the PMLA[42].

• Gathering Evidence: By means of summonses, seizures, searches, and statements made in accordance with PMLA Section 50, which are admissible as evidence[43].

• Provisional Attachment: Using attachment orders to safeguard criminal proceeds and stop their disposal while an investigation is underway[44].

• Prosecution Complaint: submitting a formal complaint to the Special Court, which is comparable to a charge sheet in a typical criminal case[45].

Asset Tracing and Recovery Mechanisms

The ED's emphasis on locating, tracking down, and recovering the proceeds of crime is one of its unique operational characteristics. This includes:

1. Asset Identification: Identifying assets obtained through criminal activity, such as benami properties, shell corporations, and layered transactions, using financial intelligence[46].

2. Methods of Tracing: Using specific financial investigation methods such as digital forensics, fund flow analysis, bank account examination, and corporate structure mapping

- Global collaboration for cross-border resources[47]

---

38 Ministry of Finance, "Inter-Agency Coordination Protocol for Financial Crime Investigation," Department of Revenue, 2020.

39 Financial Intelligence Unit-India, "Annual Report 2021-22," Ministry of Finance, Government of India.

40 Prevention of Money Laundering Act, 2002, Section 3 read with Schedule.

41 Enforcement Directorate, "Investigation Manual," Internal Document, Chapter 3, 2021.

42 Vijay Madanlal Choudhary v. Union of India, 2022 SCC OnLine SC 929, Paras 182-190.

43 Prevention of Money Laundering Act, 2002, Section 50(3).

44 Prevention of Money Laundering Act, 2002, Section 5.

45 Prevention of Money Laundering Act, 2002, Section 44(1)(b).

46 Enforcement Directorate, "Asset Tracing Manual," Internal Document, 2020.

47 Financial Action Task Force, "Operational Issues - Financial Investigations Guidance," FATF-GAFI, Paris, 2020.

3. Attachment Mechanisms: Protecting identified assets with: o FEMA retention orders o Provisional attachment orders under Section 5 of PMLA

- Request letters for overseas asset restraining sent to foreign jurisdictions[48].

4. Confiscation Procedures: After a conviction under the PMLA, the Central Government will permanently seize the tainted assets[49].

5. Asset Recovery Units: Specialized groups that only work on tracking down and recovering criminal proceeds, especially in high-value cases[50].

The "follow the money" principle is embodied in the ED's asset recovery strategy, which aims to dismantle criminal enterprises' economic infrastructure by denying them access to illicit gains in addition to prosecuting offenders[51].

Major Enforcement Actions and Case Studies

The most notable instances of the ED's development show its growing operational reach and growing assertiveness in high-profile investigations:

Banking Fraud Cases

One of India's biggest banking scams, the Punjab National Bank-Nirav Modi Case (2018), involved about ₹13,000 crore that was obtained fraudulently through letters of undertaking. As a result of the ED's investigation, the primary accused was extradited and assets valued at over ₹2,400 crore were attached[52]. This case demonstrated the ED's proficiency in international coordination and cross-border investigations.

The ED looked into claims of fund diversions and kickbacks involving well-known banking executives and real estate firms in the Yes Bank-DHFL Case (2020). The ED's willingness to pursue delicate cases involving financial institutions was demonstrated by the attachment of assets valued at about ₹2,600 crore and the making of multiple high-profile arrests[53].

Political Corruption Cases

Several politicians and corporate executives were charged with money laundering as a result of the ED's investigations into the 2G Spectrum Case, which included attached properties worth over ₹223 crore. Even

---

48 Prevention of Money Laundering Act, 2002, Section 60.

49 Prevention of Money Laundering Act, 2002, Section 8(5).

50 Directorate of Enforcement, "Annual Action Plan 2022-23," Ministry of Finance, Government of India.

51 Financial Action Task Force, "Best Practices on Confiscation," FATF-GAFI, Paris, 2019.

52 Enforcement Directorate, "Press Release: PNB Fraud Case," February 15, 220.

53 Enforcement Directorate, "Press Release: Yes Bank-DHFL Case," March 18, 2021.

though the defendants were ultimately found not guilty, the case set significant precedents for the ED's ability to pursue proceeds of crime regardless of the results of the underlying offenses[54].

The allegations against prominent political figures in the National Herald Case serve as an example of the ED's growing engagement in politically delicate issues. The investigation's examination of intricate asset transfers and transactions between related businesses and trusts sparked intense legal and public discussion regarding the reach of money laundering laws[55].

Hawala and Terror Financing

Operation Hawala Trader (2015–17) focused on a large network engaged in illicit cross-border value transfers and foreign exchange transactions. Significant seizures and the discovery of methods for transferring money outside of official banking channels were the outcomes of the ED's coordinated efforts across several states[56].

The ED and the National Investigation Agency (NIA) have collaborated to target financial networks that support terrorist organizations in cases involving terror financing. Cases against Kashmiri separatist leaders are among the notable investigations in which the ED concentrated on locating funding trends and real estate purchases purportedly connected to the financing of terrorism[57].

Corporate Fraud and Economic Offences

The ED's role in combating widespread public financial fraud was made clear by the Saradha Chit Fund Scam investigation. In addition to pursuing money laundering charges against a number of powerful individuals suspected of participating in the Ponzi scheme that impacted thousands of investors, the agency seized assets valued at over ₹600 crore[58]. By designating Vijay Mallya as a "fugitive economic offender" under the Fugitive Economic Offenders Act of 2018, the ED achieved a major legal victory in the Vijay Mallya-Kingfisher Airlines Case. This established a significant precedent for dealing with cases involving high-value economic offenders who escape Indian jurisdiction by enabling the non-conviction based confiscation of assets valued at about ₹9,600 crore[59].

These cases demonstrate the ED's growing operational reach into a variety of financial crime categories and its growing readiness to conduct intricate investigations against both politically and economically

---

54 Directorate of Enforcement v. A. Raja and Others, Special Court CBI Case No. 1/2011.

55 Young Indian Private Limited v. Directorate of Enforcement, Delhi High Court, W.P.(C) 11315/2018.

56 Enforcement Directorate, "Annual Report Summary 2018-19," Ministry of Finance, Government of India.

57 National Investigation Agency v. Zahoor Ahmad Shah Watali, (2019) 5 SCC 1.

58 Enforcement Directorate, "Press Release: Saradha Chit Fund Case," October 2019.

59 Enforcement Directorate v. Vijay Mallya, Special Court, PMLA Case No. 564/2016.

Challenges and Criticisms

The ED continues to face a number of obstacles in spite of its expanded mandate:

Institutional and Operational Challenges

Capacity Restrictions: The ED is severely underfunded, with only 2,000 staff members managing thousands of complex cases across the country. This has an impact on the agency's capacity to carry out prompt investigations, especially in cases of technically intricate financial crimes that call for specialized knowledge[60].

Case Pendency: The ED has a significant backlog of cases, and investigations typically take years to complete. The conviction rate under PMLA as of 2022 was less than 0.5% of cases that were registered, which raises concerns about the efficacy of the prosecution and the efficiency of the investigation[61].

Jurisdictional Overlaps: The CBI, SFIO, and other state agencies are among the many agencies looking into economic offenses. This leads to coordination issues, investigative duplications, and sometimes competitive rather than cooperative methods[62].

The ED still faces difficulties in specialized areas like cryptocurrency investigations, cross-border financial intelligence, and advanced digital forensics, despite advancements. These areas are crucial for tackling new types of financial crime[63].

Legal and Constitutional Controversies

The ED's activities have sparked intense legal discussions about a number of controversial topics:

Arrest Powers and Bail Provisions: Strict bail requirements under Section 45 of the PMLA, which require judges to be convinced that the accused is innocent and unlikely to commit any crimes while out on bail, have drawn criticism for establishing a presumption of guilt that goes against basic criminal jurisprudence principles[64].

Statement Admissibility: In contrast to general evidence law rules governing custodial statements, Section 50 of the PMLA permits statements recorded by ED officers to be admitted in court. This has sparked worries about possible protections against coercion and self-incrimination[65].

The PMLA's expansive definition of "proceeds of crime" and money laundering has drawn criticism for possibly

---

60 Department of Personnel and Training, "Cadre Review of Enforcement Directorate," Government of India, 2021.

61 Ministry of Finance, "Response to Lok Sabha Unstarred Question No. 3989," August 8, 2022.

62 Parliamentary Standing Committee on Finance, "138th Report on Coordination Among Financial Sector Regulatory Agencies," Lok Sabha Secretariat, 2023.

63 NITI Aayog, "Report on Digital Financial Crime Prevention," Government of India, 2022.

64 Nikesh Tarachand Shah v. Union of India, (2018) 11 SCC 1.

65 P. Chidambaram v. Directorate of Enforcement, (2019) 9 SCC 24.

going too far, as it permits the attachment of almost any asset that is even remotely related to suspected criminal activity[66].

Reverse Burden of Proof: The PMLA challenges traditional criminal law principles by shifting the burden of proof to the accused due to its presumptions about the criminal origins of property and involvement in money laundering[67].

Allegations of Selective Enforcement

Allegations of political influence on the ED's case selection and investigative priorities have been made repeatedly. The timing of investigations against political figures, especially opposition leaders, during election seasons or significant political events is criticized for seeming patterns[68].

Significant differences in investigation patterns are revealed by statistical analysis, with some political entities appearing disproportionately in ED actions[69]. Supporters, however, argue that this is not political targeting but rather a legitimate focus on high-corruption sectors. In order to guarantee that the ED's investigations are not influenced by political factors, there are still demands for increased institutional autonomy, clear case selection standards, and more robust oversight procedures[70].

International Cooperation and Global Standards Compliance

India's FATF Commitments and Implementation

India has pledged to apply international standards in the fight against money laundering and terrorist financing since joining the Financial Action Task Force (FATF) in 2010. An essential implementing agency for these commitments is the ED[71].

Although India's AML/CFT framework has seen significant improvements, the most recent FATF Mutual Evaluation Report pointed out implementation gaps in beneficial ownership transparency, non-profit organization regulation, and prosecution effectiveness[72]. Legislative changes and procedural reforms are influenced by the frequent evaluation of the ED's operations in relation to these global standards.

Cross-Border Enforcement Mechanisms

The ED uses a number of international cooperation mechanisms, including:

India has signed Mutual Legal Assistance Treaties (MLATs) with more than 40 nations, which offer official frameworks for exchanging evidence, freezing assets, and assisting with extradition[73].

---

66 Vijay Madanlal Choudhary v. Union of India, 2022 SCC OnLine SC 929, Dissenting Opinion.

67 Prevention of Money Laundering Act, 2002, Section 24.

68 Association for Democratic Reforms, "Analysis of ED Case Registration Patterns 2014-2023," New Delhi, 2023.

69 Lok Sabha, "Unstarred Question No. 1920 on ED Investigations," Ministry of Finance Response, March 11, 2022.

70 Law Commission of India, "258th Report: Reforms in Economic Enforcement Agencies," Government of India, 2022.

71 Financial Action Task Force, "India: Membership Profile," FATF-GAFI, Paris.

72 Financial Action Task Force, "Mutual Evaluation Report: India," FATF-GAFI, Paris, 2020.

73 Ministry of External Affairs, "List of Treaties and Agreements: Mutual Legal Assistance," Government of India, 2023.

Cooperation between Financial Intelligence Units: The ED coordinates with international FIUs via the Egmont Group network to share financial intelligence on questionable transactions that have global implications[74].

Letters Rogatory: In jurisdictions without MLATs, the ED requests investigative support and evidence gathering through judicial Letters Rogatory[75].

Joint Investigation Teams: The ED occasionally takes part in coordinated investigations with foreign counterparts, especially when it comes to cases involving cross-border securities fraud, shell companies, and round-tripping of funds[76].

International cooperation still faces obstacles in spite of these mechanisms, such as differing standards for evidence, requirements for dual criminality, and political factors that influence extradition and asset recovery in high-profile cases[77].

Future Directions and Reform Perspectives

Technological Integration and Advanced Analytics

Future ED efficacy will be heavily reliant on technology adoption. Among the priority areas are:

Applications of Artificial Intelligence: Putting in place AI-based systems for risk assessment, pattern recognition, and transaction monitoring to more quickly spot questionable activity[78]. Blockchain analytics is the process of creating specialized tools to track cryptocurrency transactions and spot illegal uses of digital assets[79].

Integrated Databases: Establishing smooth channels for information exchange between different law enforcement and financial intelligence organizations to facilitate thorough financial crime analysis[80].

Predictive modeling is the process of using data analytics to spot new patterns in financial crime and more wisely distribute investigative resources[81].

Institutional Reforms and Capacity Enhancement

Current limitations could be addressed by a number of structural reforms:

Strengthening Autonomy: To protect the ED from possible executive influence, it should be granted statutory

---

74 Egmont Group, "Financial Intelligence Units of the World," Annual Report 2022.

75 Ministry of Home Affairs, "Guidelines for Indian Judicial Authorities for Issuing Letter Rogatory," Government of India, 2019.

76 International Criminal Police Organization, "Joint Investigation Teams: Best Practices," Interpol General Secretariat, Lyon, 2021

77 Enforcement Directorate, "International Cooperation Challenges Report," Internal Document, 2021.

78 NITI Aayog, "Artificial Intelligence in Financial Crime Detection," Government of India, 2022.

79 Department of Economic Affairs, "Report of the Committee on Virtual Currency Regulation," Ministry of Finance, 2022.

80 Ministry of Electronics and Information Technology, "National Digital Intelligence Strategy," Government of India, 2021.

81 National Crime Records Bureau, "Predictive Analytics in Financial Crime: Feasibility Study," Ministry of Home Affairs, 2022.

independence akin to that of the Central Bureau of Investigation[82].

Specialized Recruitment: Creating committed cadres with experience in financial investigations instead of depending mostly on deputations from other agencies[83].

Enhancement of Training: Creating cutting-edge courses in digital forensics, forensic accounting, and intricate financial crime investigation[84].

Performance Metrics: Implementing outcome-based assessment that goes beyond case registration or attachment values to include conviction rates and asset recovery effectiveness

Legislative and Procedural Refinements

The following areas could be the focus of future legislative development: Procedural safeguards: establishing more robust due process protections while preserving the efficacy of investigations, such as more equitable bail provisions and more precise attachment criteria. To speed up case resolution, the PMLA courts' network will be expanded to include judges with specialized training in financial crime jurisprudence.

Strengthening civil forfeiture provisions to handle circumstances where criminal prosecution might not be feasible because of diplomatic immunity, death, or flight is known as non-conviction-based confiscation.

Strengthening safeguards for financial crime informants in order to promote the reporting of intricate white-collar crimes is known as whistle-blower protection.

Conclusion

From being a restricted foreign exchange regulator, the Enforcement Directorate has developed into a key component of India's framework for combating financial crime. India's increasing awareness of the risks that money laundering, corruption, and illicit financial flows pose to economic stability and the integrity of governance is reflected in its enlarged mandate under the PMLA and FEMA.

The development of the ED is a microcosm of India's larger shift in combating intricate financial crimes, from straightforward regulatory strategies to advanced enforcement tools that focus on the financial aspects of illicit activity. This evolution keeps navigating conflicts between national enforcement priorities and international compliance standards, between institutional autonomy and accountability, and between enforcement imperatives and due process considerations.

The effectiveness of the ED will depend on its ability to adjust as financial crimes become more complex, transnational, and technologically enabled. This includes embracing technological innovation, enhancing

[82] Law Commission of India, "267th Report on Structural Independence of Economic Enforcement Agencies," Government of India, 2021.

[83] Department of Personnel and Training, "Specialized Cadre Creation Proposal for Financial Investigation Agencies," Government of India, 2022.

[84] National Institute of Financial Management, "Advanced Financial Crime Investigation Course Structure," Ministry of Finance, 2022.

institutional capabilities, and improving its legal framework to address new issues while upholding constitutional protections.

The ED's overall effectiveness is determined by its systemic influence on preventing financial crimes, recovering criminal proceeds, and bolstering public trust in financial integrity, not just by high-profile arrests or attention-grabbing attachment values. The delicate balance between strict enforcement and procedural justice that characterizes successful financial crime control in democracies must be continuously improved in order to achieve this balance.

AN EXAMINATION OF THE ENFORCEMENT DIRECTORATE'S ROLE IN ADDRESSING FINANCIAL CRIME IN INDIA

Tanveer Ahmad
LL.M. Student, School of law,
Pondicherry University.

ABSTRACT

Financial crime, including money laundering, fraud, and corruption, that causes significant threats to India's economic stability and governance. The Enforcement Directorate (ED), as the specialised investigative agency under the Department of Revenue, plays a pivotal role in combating these offenses through its enforcement of key legislations such as the Prevention of Money Laundering Act (PMLA, 2002), the Foreign Exchange Management Act (FEMA, 1999), and the Fugitive Economic Offenders Act (FEOA, 2018). This paper examines the ED's functions, legal framework, operational mechanisms, and effectiveness in addressing financial crimes while identifying challenges and proposing reforms for enhanced efficiency. The study describes the ED's investigative and prosecutorial powers, including asset attachment, cross-border cooperation, and high-profile cases such as the PNB scam (Nirav Modi), Vijay Mallya's extradition, and 2G spectrum fraud. Apart from this successes, the ED faces legal delays, political interference, technological gaps, and jurisdictional hurdles in prosecuting offenders and recovering illicit assets. A critical analysis of its conviction rate, recovery mechanisms, and global collaboration reveals both strengths and systemic weaknesses. Furthermore,this paper explores comparative models from international agencies like the FBI (U.S.) and NCA (UK) to suggest best practices for India. The Recommendations include strengthening legal frameworks, adopting advanced forensic tools, enhancing inter-agency coordination, and ensuring transparency to mitigate allegation of misuse. The research concludes that while the ED has been instrumental in deterring financial crime, structural reforms, technological modernization, and judicial efficiency are imperative to bolster its effectiveness. By addressing these challenges, the ED can better fulfill its mandate of safeguarding the India's financial integrity in an increasingly complex economic landscape.

Key words: *Enforcement Directorate (ED), Financial Crime, Money Laundering, PMLA, FEMA, Recovery, Economic Offenses.*

Introduction

FINANCIAL CRIME such as money laundering, corruption, fraud, and illicit fund flows pose a severe threat to India's economic security and governance. These offenses undermine financial system, distort markets, and erode public trust in institutions. In response, the Enforcement Directorate (ED) India's premier financial investigation agency has been tasked with enforcing key economic laws to combat such crimes. Established in 1956 under the Department of Revenue, the ED operates under stringent legal frameworks[1], including the Prevention of Money Laundering Act (PMLA, 2002)[2], the Foreign Exchange Management Act (FEMA, 1999)[3], and the Fugitive Economic Offenders Act (FEOA, 2018)[4].

The ED plays a multi-dimensional role investigating money laundering, regulating foreign exchange violations, and prosecuting high-profile economic offenders. Its power includes asset seizure, arrest, prosecution, and international cooperation to recover illicit wealth. Over the years, the agency has handled landmark cases such as the 2G Spectrum Scam, Punjab National Bank (PNB) fraud involving Nirav Modi and Mehul Choksi and the

[1] Mishra, Rini, "Economic Offenses: How Do the Laws Deal with Them?." *Jus Corpus LJ* 3 887 (2022).

[2] Prevention of Money Laundering Act, 2002, Act No. 15 of 2003.

[3] Foreign Exchange Management Act, 1999, Act No. 42 of 1999.

[4] Fugitive Economic Offenders Act, 2018, No. 17, Acts of Parliament, 2018.

extradition of Vijay Mallya. These cases describes the ED's critical function in deterring financial crimes and ensuring accountability[5].

Though, despite its successes, the ED faces significant challenges, including legal delays, political interference, limited resources, and evolving cyber-financial crime. The agency has also been criticized for alleged misuse of power and selective investigations, raising concern about transparency and fairness. Furthermore, the complexity of global financial networks makes tracking cross-border illicit funds a daunting task.

This research paper aims to analyze the ED's role, effectiveness, and limitations in combating financial crimes in India. It explores key function, major cases, legal frameworks, and operational hurdles while comparing India's approach with global best practices. The study also provides policy recommendation to strengthen the ED's capabilities, ensuring a more robust, efficient, and transparent financial crime enforcement mechanism.

By evaluating the ED's impact, this research contributes to the discourse on economic governance, anti-corruption measures and financial regulatory reforms in India. The findings will be relevant to policymakers, legal experts, and financial crimes researchers seeking to enhance India's defenses against economic offenses.

Overview of the Enforcement Directorate (ED)

The Enforcement Directorate (ED), established in 1956 under the Department of Revenue, Ministry of Finance, serves as India's primary agency for investigating and prosecuting financial crime[6]. Initially tasked with enforcing foreign exchange laws, its role expanded significantly with the enactment of key legislation like the Prevention of Money Laundering Act (PMLA, 2002)[7], the Foreign Exchange Management Act (FEMA, 1999)[8], and the Fugitive Economic Offenders Act (FEOA, 2018)[9]. The ED operates under a two-fold mandate: regulating foreign exchange violations under FEMA and combating money laundering and asset recovery under PMLA and FEOA. Structurally, the agency is headed by a Director and comprises Special Directors, Joint Director, and Deputy Directors across 10 zonal and 11 sub-zonal offices, ensuring nationwide jurisdiction. The ED collaborates closely with other law enforcement bodies, including the CBI, Income Tax Department, RBI, SEBI, and Interpol, forming a multi-agency approach to tackle complex financial crime[10]. Over the years, the ED has evolved into a powerful investigative body equipped with provisional attachment powers, arrest authority, and prosecution rights, making it a cornerstone of India's anti-financial crime framework.

The legal arsenal of the ED is both broad and severe, enabling it to tackle diverse financial offenses. Under PMLA, the agency targets money laundering by tracking proceeds of crimes, attaching properties, and prosecuting offenders, with punishments including imprisonment up to 7 years and unlimited fines[11]. FEMA,

---

5 Singh, Snehit and Amalendu Mishra, "Economic Crimes in India", Issue 2 *Int'l JL Mgmt. & Human* 2215 (2024).

6 Nainta, Rish Pal, *Banking system, frauds and legal control: Evolution, RBI, bank frauds, legal control, security measures, recent trends*, Deep and Deep Publications, (2005).

7 Prevention of Money Laundering Act, 2002, No. 15, Acts of Parliament, 2003.

8 Foreign Exchange Management Act, 1999, No. 42, Acts of Parliament, 1999.

9 Fugitive Economic Offenders Act, 2018, No. 17, Acts of Parliament, 2018.

10 Rider, Barry, *Introduction to A Research Agenda for Economic Crime and Development*, Edward Elgar Publishing (2023).

11 Kumar, Surender and Anjali Dixit, "Prevention of Money Laundering Act, 2002 (PMLA) Critical Review of Key Provisions."

replacing the older FERA (1973), focuses on foreign exchange violation, penalizing unauthorized cross-border transactions while promoting legitimate trade and investments[12]. The FEOA (2018)[13] empowers the ED to confiscate assets of fugitive like Vijay Mallya and Nirav Modi, who flee India to evade prosecution[14].

Moreover, the ED leverages international treaties and mutual legal assistance pacts (MLATs) to trace offshore assets and extradite offenders. The agency's investigative techniques include forensic audits, digital forensics, and data mining, adapting to modern challenges like cryptocurrency fraud and shell company networks. Despite its robust framework, the ED's effectiveness is sometimes hampered by legal delays, political scrutiny, and resource constraints, raising debates about its operational autonomy and accountability.

The ED's operational significance is evident in its handling of high-profile cases, which have shaped India's financial crime jurisprudence. Landmark investigations include the 2G Spectrum Scam (₹1.76 lakh crore loss)[15], the PNB Fraud (₹14,000 crore by Nirav Modi), and the Vijay Mallya extradition case, where the ED successfully secured the confiscation of assets worth ₹12,500 crore[16]. More recently, the agency has targeted hawala networks, crypto scams, and corruption cases involving politicians and bureaucrats. While the ED has secured notable convictions and asset recoveries, critics argue that its selective targeting and prolonged investigations undermine its credibility. The agency's global collaborations with bodies like the Financial Action Task Force (FATF) and Interpol enhance its cross-border reach, yet challenges like jurisdictional complexities and slow judicial processes persist[17]. As financial crimes grow in sophistication, the ED's role will remain pivotal, necessitating greater transparency, technological upgrades, and systemic reforms to strengthen India's economic defense mechanisms.

Investigative and Prosecutorial Powers

The Enforcement Directorate (ED) wields extensive investigative and prosecutorial authority under three primary legislations—the Prevention of Money Laundering Act (PMLA), the Foreign Exchange Management Act[18] (FEMA), and the Fugitive Economic Offenders Act (FEOA)[19]. Under PMLA, the ED's foremost responsibility is to investigate money laundering offenses, which involves tracing the "proceeds of crime derived from predicate offenses such as corruption, fraud, and narcotics trafficking. The agency has the power to conduct searches, seizer of evidences, and arrest individuals without a warrant in certain circumstances, ensuring swift action against suspects. One of its most potent tool is the provisional attachment of properties believed to be linked to money laundering, which can later be confirmed by the Adjudicating Authority and eventually confiscated by the central government.

---

[12] Singh, Nirajan Man, and P. Sandhya, "Hawala Financing: An Aid to Terrorism" *NALSAR Stud. L. Rev.* 4 108 (2008).

[13] Sestok, Alexandrea E., Richard O. Linkous, and Aaron T. Smith. "Toward a mechanistic understanding of Feo-mediated ferrous iron uptake" *Metallomics* 10, no. 7 887-898 (2018).

[14] Yadav, Rahul, and Munmun Kadam "Fugitive Economic Offenders Bill 2018: An Analysis" *Int'l JL Mgmt. & Human.* 1 165(2018).

[15] Gupta, Pooja, and Nainika Jain. "Signalling role of 2G scam investigation on stock market returns of select telecom companies in India" *International Journal of Public Sector Performance Management* 5, no. 3-4 370-383 (2019).

[16] Mishra, Rini, "Economic Offenses: How Do the Laws Deal with Them?" *Jus Corpus LJ* 3 887(2022).

[17] Kanki, Kanae and Alexander Resch, "Strengthening International Law Enforcement Cooperation: INTERPOL and Its Global Fight against Economic and Financial Crime" In *Corporate Criminal Liability and Sanctions*, 106-126 Routledge.

[18] Prevention of Money Laundering Act, 2002, No. 15, Acts of Parliament, 2003.

[19] Fugitive Economic Offenders Act, 2018, No. 17, Acts of Parliament, 2018.

The ED also files prosecution complain (equivalent to charge sheets) before the Special PMLA Courts, leading to trials that can result in imprisonment of up to seven years and hefty fines. Under FEMA, the ED regulates foreign exchange transaction to prevent violations such as illegal overseas investments, hawala transactions, and forex frauds. While FEMA is primarily a civil law with monetary penalties, repeated or severe violation can lead to criminal prosecution. The FEOA empowers the ED to target economic offender who flee India to evade prosecution, allowing for the confiscation of their domestic and international assets even in their absence, as seen in cases like Vijay Mallya and Nirav Modi[20].

Beyond domestic enforcement, the ED plays a crucial role in international cooperation to combat cross-border financial crime. It works closely with global agencies such as Interpol, the Financial Action Task Force (FATF), and foreign financial intelligence units (FIUs) to track illicit funds, extradite offenders, and facilitate asset repatriation. The agency has successfully utilized Mutual Legal Assistance Treaties (MLATs) and agreement with countries like the UK, UAE, and Switzerland to recover stolen wealth[21]. For instance, in the PNB fraud case, the ED collaborated with Hong Kong and Belgium to confiscate the assets linked to Nirav Modi[22]. Furthermore, the ED has adapted to emerging financial crime trends, including cryptocurrency frauds, digital payment scams, and the shell company networks, by employing advanced forensic accounting and blockchain analysis.

However, despite these powers, the ED faces challenges such as legal loopholes, delayed court proceeding, and jurisdictional conflicts, which sometimes hinder timely justice.

Asset Recovery and Deterrence Mechanism

One of the ED's most critical functions is asset recovery, which serves both as a penal measure and a deterrent against financial crimes. Under PMLA[23], the ED can attach and confiscate properties acquired through illicit mean, effectively stripping offenders of their ill-gotten wealth. Since 2005, the agency has attached more assets worth over ₹1.2 lakh crore, with a significant portion linked to high-profile cases such as the 2G scam, coal allocation scam, and bank frauds[24]. The confiscated assets are either liquidated to compensate victim or retained by the government, ensuring that crime does not pay. The FEOA[25] further strengthens this mechanism by allowing the ED to seize assets of fugitive who refuse to return to India, as seen in the Vijay Mallya case, where assets worth ₹12,500 crore were confiscated[26]. The ED also maintains a database of high-risk individual and entities, including politically exposed persons (PEPs), to monitor suspicious transactions and prevent future offenses.

The ED's role extends beyond enforcement to policy advocacy and systemic reform aimed at plugging gaps in India's financial regulatory framework. It regularly submits reports to the Finance Ministry and regulatory

---

[20] Agrawal, Kartik, “Critical analysis of economic offenders Act” Issue 1 *Indian JL & Legal Rsch* 4 (2022).

[21] Nessi, Giulio, "International cooperation to tackle transnational corruption: issues and trends in mutual legal assistance, extradition and asset recovery" (2015).

[22] Khalique, Fehmina, and Smriti Srivastava. “Nirav Modi: A Case Study on Banking Frauds and Corporate Governance” *Lloyd Business Review* 1-16 (2024).

[23] Prevention of Money Laundering Act, 2002, No. 15, Acts of Parliament, 2003.

[24] Vittal, N., *Ending Corruption?: How to Clean Up India*, Penguin UK (2012).

[25] Fugitive Economic Offenders Act, 2018, No. 17, Acts of Parliament, 2018 .

[26] Bhatt, Anannya, and Razit Sharma. “Review of Indian Extradition Law & Policy and the Impact of the Fugitive Economic Offender's Act 2018” Issue 4 *Int'l JL Mgmt. & Human,* 67 (2021).

bodies like RBI and SEBI, recommending sever compliance measures for banks, real estate sectors, and cryptocurrency exchanges. The agency also conducts awareness program for financial institutions and law enforcement agencies to improve detection and reporting of suspicious transactions. In spite of its successes, the ED faces criticism over delays in disposal of attached assets and allegations of political bias in certain cases. Nevertheless, its deterrent impact is undeniable, with high-profile conviction and asset seizures sending a strong message to potential offenders. Going forward, enhancing transparency, judicial efficiency, and inter-agency coordination will be crucial for the ED to maintain its effectiveness in India's fight against financial crime.

Major Cases Handled by the Enforcement Directorate (ED)

The Enforcement Directorate has been at the forefront of investigating some of India's most high-profile financial crime, setting important precedent in economic jurisprudence. These landmark cases demonstrate the agency's evolving capabilities in tackling complex money laundering scheme, banking frauds, and cross-border financial crimes while also revealing systemic challenges in India's financial governance.

High-Profile Banking and Corporate Frauds

The Punjab National Bank (PNB) scam (2018)[27] stands as one of the most audacious banking frauds in Indian history, involving diamond merchant Nirav Modi and Mehul Choksi who allegedly defrauded the bank of ₹14,000 crore through fraudulent Letters of Undertaking (LoUs). The ED's investigation revealed an intricate web of shell companies across multiple countries, leading to the seazer of assets worth ₹2,650 crore in India and abroad. The case emphasized critical gaps in India's banking oversight while showcasing the ED's ability to coordinate with international agencies, resulting in Modi's extradition from the UK. Likewise, the Vijay Mallya case marked India's first major success under the Fugitive Economic Offenders Act[28], with the ED securing orders for confiscation of assets worth ₹12,500 crore. The decade long investigation exposed how corporate debt could be siphoned abroad through complex financial engineering, ultimately leading to Mallya's extradition from Britain in 2022 a watershed moment for India's fight against economic offenders.

The Yes Bank-DHFL scam (2020[29]) uncovered a staggering ₹34,000 crore financial fraud involving collusion between bankers, corporates, and politician. The ED's probe revealed how Yes Bank's founder Rana Kapoor illegally diverted funds to DHFL in exchange for kickbacks, part of which were laundered through offshore entities and luxury real estate purchase. This case demonstrated the ED's growing sophistication in forensic accounting, as investigator traced money flows across 78 shell companies and multiple tax havens. Some other significant banking case involved the ICICI Bank Videocon loan fraud, where the ED established a quid pro quo between bank officials and corporate beneficiaries, attaching assets worth ₹1,300 crore.

---

[27] Gayathri, S., "A critical analysis of the Punjab National Bank scam and its implications" 119, no. 12 *International Journal of Pure and Applied Mathematics,* 14853-14866 (2018).

[28] Fugitive Economic Offenders Act, 2018, No. 17, Acts of Parliament, 2018.

[29] Standard Business, "What is the Yes Bank Crisis?" (2024).

These cases collectively exposed the vulnerabilities in India's corporate lending ecosystem while establishing the ED's role as a financial regulatory mechanism.

Political Corruption and Money Laundering Cases

The 2G spectrum allocation scam (2011) represented one of the ED's earliest major forays into political corruption cases with estimated losses of ₹1.76 lakh crore to the exchequer[30]. The agency's money trail investigation revealed how spectrum licenses were illegally allocated in exchange for kickbacks laundered through a maze of domestic and foreign entities. While the special court eventually acquitted all accused due to evidentiary challenges, the case significantly expanded the ED's understanding of political money laundering network. The Aircel-Maxis case involving former Finance Minister P. Chidambaram demonstrated how political influence could be monetized, with the ED attaching assets worth ₹1.16 crore and establishing foreign money imprints to Singapore and Malaysia[31].

Recently, the Delhi liquor policy case (2022-23) has emerged as a testing ground for the ED's capabilities in investigating political corruption[32]. The probe into alleged kickback in Delhi's excise policy has led to the arrest of several high-profile politicians and businessmen, with the ED claiming to have uncovered a ₹100 crore money laundering network. The Jharkhand mining scam case has similarly exposed how natural resource allocation is being exploited for money laundering, with the ED attaching assets worth ₹193 crore belonging to politicians and bureaucrats. These cases underscore the ED's expanding mandate in tackling the intersection of politics and financial crimes, though they have also attracted allegations of political partisanship that the agency continues to grapple with.

Emerging Financial Crimes and International Cases

The ED has increasingly focused on new age financial crimes, including cryptocurrency frauds and online scams. The Gain Bitcoin Ponzi scheme investigation revealed how ₹20,000 crore was laundered through cryptocurrency transaction and offshore entities, marking one of India's first major crypto-related money laundering cases[33]. The Chinese loan app cases have uncovered sophisticated digital hawala networks, with the ED freezing assets worth ₹1,000 crore linked to predatory lending apps operated through Chinese front[34]. These cases demonstrate the agency's efforts to keep pace with technological advancements in financial crimes.

On the international front, the AgustaWestland VVIP chopper scam saw the ED effectively tracing and attaching assets across multiple countries, including a luxury hotel in Dubai[35]. The Moshe Baqal money laundering case

---

30 Saeed, Saima, “Phantom journalism: Governing India's proxy media owners” In *Journalism, Democracy and Civil Society in India*, 61-77 (Routledge, 2018).

31 Bhatia, Jai, “Crime in the air: spectrum markets and the telecommunications sector in India” *The Wild East: Criminal Political Economies in South Asia* 140-167 (2019).

32 Jayachandran, Jesna, "Alcohol News: Analyzing Media Coverage of Alcohol and Public Health Challenges During COVID-19 Pandemic in India" *The Palgrave Handbook of Global Social Problems* 1-23(2023).

33 Agarwal Udit and Vinay Rishiwal, *et. at*., “Blockchain and crypto forensics: Investigating crypto frauds” 34, no. 2 *International Journal of Network Management* e2255(2024).

34 Hsu, Sara and Jianjun Li. *China's Fintech Explosion: Disruption, Innovation, and Survival*. Columbia University Press, (2019).

35 Matthew T., Dubai Property: an oasis for Nigeria's corrupt political elites, *Carnegie Endowment for International Peace* (2020).

involved coordination with six countries to uncover a ₹7,000 crore fraud resulting in the first-ever Interpol Red Notice against a sitting Indian legislator. The Sterling Biotech case exposed a ₹14,500 crore banking fraud with international dimensions, leading to the extradition of promoter from Albania[36]. These cases explain the ED's growing capability in global asset tracking and recovery, though they also reveal the challenges of navigating different legal systems and banking secrecy laws.

Each of these landmark cases has contributed to the evolution of India's financial crimes investigation framework, setting important legal precedents while exposing systemic vulnerabilities in banking, politics, and corporate governance. They demonstrate the ED's expanding technical capabilities but also underscore the need for judicial reform, better inter-agency coordination, and political will to ensure that high-profile investigations lead to convictions and meaningful asset recovery. As financial crimes grow more sophisticated, these cases provide crucial lesson for strengthening India's defenses against economic offenses.

Challenges Faced by the Enforcement Directorate

The Enforcement Directorate (ED) faces numerous challenges in its mission to combat financial crime, including legal and procedural hurdles such as prolonged judicial processes[37] and complex litigation strategies employed by high-profile offenders, which often delay justice and reduce the efficacy of investigations. Political interference and allegation of selective targeting have raised concerns about the agency's impartiality, undermining public trust and complicating sensitive cases involving influential figures. Resource constraints, including limited manpower and technological gaps, hinder the ED's ability to effectively investigate increasingly sophisticated financial crime, particularly in the digital realm involving cryptocurrencies, dark web transactions, and cross-border money laundering schemes. The agency struggles with international cooperation due to jurisdictional complexities, banking secrecy laws, and varying legal frameworks, making asset recovery and extradition processes time consuming and often unsuccessful. Moreover, the evolving nature of financial crimes demands continuous upskilling of personnel and adoption of advanced forensic tools, but bureaucratic delays in approvals and budget allocations slow down these necessary upgrades.

The lack of specialized courts for financial crime results in case backlogs, while the stringent burden of proof requirements under laws like PMLA[38] sometimes make convictions difficult to secure. Public perception issues, fueled by media trials and political narratives, additionally complicate the ED's operations, as does the growing trend of accused individuals fleeing the country before investigations conclude, exemplified by cases like Nirav Modi and Vijay Mallya[39]. These multifaceted challenges necessitate comprehensive reform, including greater autonomy, enhanced technological capabilities, faster judicial processes, and improved international collaboration to strengthen the ED's effectiveness in combating financial crimes while maintaining transparency and accountability in its operations.

---

[36] INAL, CRIM, CA SES, and XIILAW OFWAR 293 "IX. Production, Export, and Possession of Illegal Armaments".

[37] Richards, James R. *Transnational criminal organizations, cybercrime, and money laundering: a handbook for law enforcement officers, auditors, and financial investigators*. CRC press, 1998.

[38] Prevention of Money Laundering Act, 2002, No. 15, Acts of Parliament, *2003.*

[39] Kumar Narender. "Examining Money Laundering Practices through a Legal Perspective: Scrutiny under the ED's Oversight", 1 *International Journal for Public Policy, Law and Development*, 22-31 (2024).

Effectiveness & Criticisms of the Enforcement Directorate (ED)[40]

The Enforcement Directorate (ED) has emerged as a powerful agency in India's fight against financial crime, with notable successes in high-profile cases such as the PNB scam, Vijay Mallya extradition, and 2G spectrum case, where it recovered thousands of crores in attached assets and brought economic offenders to justice[41]. The agency's effectiveness is evident in its expanding conviction rate under PMLA[42] which rose from 54 cases in 2014 to over 1,100 cases by 2023, showcasing its growing investigative rigor. The ED's proactive asset attachment mechanism has frozen properties worth ₹1.2 lakh crore since 2005, disrupting money laundering networks and deterring future offense. Additionally, its international collaboration with agencies like Interpol and the Financial Action Task Force (FATF) have improved cross-border asset tracking, as seen in the Nirav Modi and Mehul Choksi cases, where overseas properties were identified and seized. The introduction of the Fugitive Economic Offenders Act (FEOA, 2018) further strengthened the ED's hand, enabling the confiscation of assets from absconding offenders like Vijay Mallya, sending a strong deterrent message to economic criminal.

Though, the ED has faced significant criticisms, particularly regarding political bias and selective targeting, with opposition parties and legal experts accusing the agency of being used as a tool for political vendettas rather than impartial enforcement. High-profile raids and arrest involving opposition leaders, such as in the Delhi liquor policy case and Jharkhand mining scam, have fueled allegations of government influence over investigations, eroding public trust in the agency's neutrality. Another major criticism is the low conviction rate relative to cases filed while the ED registers hundreds of PMLA cases annually, only a small fraction result in convictions due to delays in trials, weak evidence, and legal loopholes exploited by wealthy defendants. The agency has also been criticized for excessive delays in disposing of attached properties, leaving genuine businesses and third-party owner in financial limbo for years. Transparency remains a concern, as the ED operates with limited public accountability, and its findings are often disclosed only through media leaks rather than official report. Furthermore, the lack of specialized courts for financial crime leads to prolonged litigation, reducing the overall efficiency of enforcement actions.

Even with these criticisms, the ED remains a critical pillar in India's anti-money laundering framework, with its aggressive pursuit of high-value economic offenders setting important legal precedents. To enhance its credibility, reforms such as greater transparency in case selection, faster judicial disposal, and stricter oversight mechanisms are required. Balancing enforcement efficiency with fairness will be key to ensuring the ED maintains its role as an effective deterrent against financial crime while addressing concerns of political weaponization.

---

[40] Mohan, Dinesh and Rahul Goel, "What and How of Effective Police Enforcement" *Transport and Safety: Systems, Approaches, and Implementation* 85-103(2021).

[41] Bhargavi, Chittimalla. "A Comprehensive Study on Socio-Economic Implications with respect to Banking Scams and Frauds in India."

[42] Prevention of Money Laundering Act, 2002, No. 15, Acts of Parliament, 2003.

Comparative Analysis of the Enforcement Directorate (ED) with Global Financial Crime Agencies

The Enforcement Directorate (ED) operates within a unique framework that combines investigative, prosecutorial, and regulatory functions under law like PMLA[43], FEMA[44], and FEOA[45], giving it broader authority than many international counterparts. Unlike the US FinCEN, which primarily analyzes financial data[46], or the UK's National Crime Agency that coordinates between specialized units, the ED directly handles all stages of financial crimes cases from investigation to prosecution[47]. This centralized approach provides operational efficiency but also concentrates significant power within a single agency, raising concern about oversight and accountability. Compared to Australia's AUSTRAC, which leverages advanced AI for real-time transaction monitoring the ED still relies heavily on manual processes, highlighting a critical technological gap[48]. Where the ED stands out is in its aggressive asset attachment power under FEOA - a tool rarely available to agencies like the US DOJ or UK SFO in such expansive form[49]. Though, this strength is offset by India's slow judicial processes, with only 12 dedicated PMLA courts handling thousands of cases, resulting in conviction rate below 30%[50], far worse than the 90%+ settlement rate achieved by US agencies through plea bargains and deferred prosecution agreements[51]. The ED's international cooperation mechanisms also lag behind Western counterparts, particularly in asset recovery, wherever countries like Switzerland and the UAE have more efficient bilateral processes for freezing and repatriating illicit fund[52].

When examining structural independence, the ED faces greater political scrutiny than agencies like the FBI or UK NCA due to its direct reporting to the Finance Ministry unlike the relative autonomy enjoyed by many Western financial crimes units[53]. This has led to persistent allegation of selective enforcement that undermines public trust. The ED could benefit from adopting several global best practices implementing AUSTRAC-style AI-driven financial surveillance to detect complex money laundering patterns establishing specialized fast-track courts similar to the UK's Economic Crime Courts[54]; developing US-style deferred prosecution agreements to resolve cases efficiently[55]; and creating an independent oversight body modeled after the US Privacy and Civil Liberties Oversight Board to enhance accountability. The agency's asset recovery framework, while theoretically

---

43 Prevention of Money Laundering Act, 2002, No. 15, Acts of Parliament, 2003.

44 Fugitive Economic Offenders Act, 2018, No. 17, Acts of Parliament, 2018.

45 *Ibid.*

46 Goldberg, H. G. and T. E. Senator, “The FinCEN AI system: finding financial crimes in a large database of cash transactions.” In Agent technology: Foundations, applications, and markets, Berlin, Heidelberg: Springer Berlin Heidelberg 283-302 (1998).

47 Button, Mark. "Hiding behind the veil of action fraud: The police response to economic crime in England and Wales and evaluating the case for regionalization or a National Economic Crime Agency." 15, no. 3 *Policing: A Journal of Policy and Practice* 1758-1772 (2021).

48 Yamaguti Mondego, Domingos, “The Use of Artificial Intelligence to Enhance User Satisfaction in Cloud-Based Payment Systems in Australia” PhD diss., CQUniversity (2024).

49 Plaistowe, Sean. "Executive Obstruction and Encroachment: The Legacy of Executive Privilege in the Late 20th and Early 21st Century." Master's thesis, Simmons University (2021).

50 Chandran, Ganesh. "A Comparison of Punishment under the PMLA Act with the Japanese Legal System: Evaluating the Link between High Conviction Rates and Unfair Means of Prosecution." Issue 2 (7) *Int'l JL Mgmt. & Human,* 2843(2024).

51 Alexander, Cindy R. and Mark A. Cohen, "The evolution of corporate criminal settlements: An empirical perspective on non-prosection, deferred prosecution, and plea agreements" 52*Am. Crim. L. Rev.* 537(2015).

52 Lohaus Mathis, "Asset recovery and illicit financial flows from a developmental perspective: Concepts, scope, and potential" (2019).

53 Hughes, Craig, and David Hicks. "Financial Investigation and Financial Intelligence: A Critical Analysis." (2024).

54 Cook Dee, & Mandy Burton, *et. al*., "Evaluation of specialist domestic violence courts/fast track systems" (2004).

55 Davis Frederick T, “Judicial review of deferred prosecution agreements: A comparative study." 60 *Colum. J. Transnat'l L.* 751(2021).

robust, needs stronger international partnership and streamlined procedures to match the effectiveness of the US Kleptocracy Initiative or UK's unexplained wealth orders[56]. These comparative insights reveal that while the ED possesses unusually strong legal power, its operational effectiveness is hampered by technological limitations, judicial delays, and perception issues - challenges that global counterparts have addressed through institutional reforms, better resourcing, and balanced accountability mechanisms that India could adapt to strengthen its financial crime enforcement.

Recommendations for Strengthening the Enforcement Directorate (ED)

To enhance the ED's effectiveness in combating financial crimes, structural, technological, and procedural reform are urgently needed. First, the agency must modernize its investigative tools by integrating AI-driven analytics, blockchain forensics, and real-time transaction monitoring systems like to those used by Australia's AUSTRAC and the U.S. FinCEN[57]. This would significantly improve its ability to detect complex money laundering schemes, cryptocurrency fraud, and shell company networks. Second, specialized fast-track court should be established to handle PMLA[58]and FEOA[59] cases exclusively, reducing the current backlog and ensuring swifter justice. The ED should also adopt alternative dispute resolution mechanism like Deferred Prosecution Agreements (DPAs) and plea bargaining, which have proven successful in the U.S. and UK in resolving cases efficiently without prolonged trials. Third, international cooperation must be strengthened through pre-negotiated asset recovery treaties with key jurisdictions like Switzerland, UAE, and Singapore, enabling faster freezing and repatriation of illicit funds. Finally, to address concerns of political bias, an independent oversight body comprising retired judges, financial experts, and civil society representatives should be created to review high-profile cases and ensure impartiality.

Beyond operational upgrades, the ED requires institutional reforms to bolster its credibility and long-term effectiveness. Capacity-building program should be implemented to train investigators in digital forensics, forensic accounting, and cross-border financial crime trends, ensuring they remain ahead of evolving criminal tactics. The agency must also improve transparency and public trust by publishing annual enforcement reports with detailed case outcomes, asset recovery statistics, and redacted intelligence findings similar to the U.S. Treasury's public disclosures. Additionally, inter-agency coordination with the CBI, Income Tax Department, and RBI should be formalized through a dedicated financial crime task force, reducing jurisdictional conflicts and improving intelligence sharing. Legislative amendments to streamline the PMLA's[60] burden of proof requirement could prevent unnecessary delays, while a whistleblower protection program would encourage insider reporting of corporate fraud and corruption. By implementing these reforms, the ED can transition from a politically scrutinized enforcer to a globally respected, tech-savvy financial crime fighter balancing robust enforcement with fairness and efficiency.

---

[56] Heathershaw John and Tom Mayne, "Explaining suspicious wealth: legal enablers, transnational kleptocracy, and the failure of the UK's Unexplained Wealth Orders" 26 (2) *Journal of International Relations and Development* 301-323(2023).

[57] Alam, Syed Tanveer, “The convergence of artificial intelligence, blockchain and fintech in energy, oil and gas trading: Increasing efficiency, transparency and automations” (2024).

[58] Prevention of Money Laundering Act, 2002, No. 15, Acts of Parliament, 2003.

[59] *Fugitive Economic Offenders Act, 2018, No. 17, Acts of Parliament, 2018*

[60] *Ibid.*

Conclusion

The Enforcement Directorate (ED) has established itself as a cornerstone of India's financial crime enforcement framework playing a pivotal role in investigating high-profile cases of money laundering, bank frauds, and corruption. Through landmark actions like the Vijay Mallya extradition, Nirav Modi-PNB fraud case, and the 2G spectrum scam investigation, the ED has demonstrated its ability to tackle complex financial crimes and recover illicit assets. The agency's powers under PMLA, FEMA, and FEOA provide it with unique capabilities, including provisional assets attachment and the authority to pursue fugitive economic offenders. However, despite these successes, the ED faces significant challenges that undermine its effectiveness, including prolonged judicial processes, low conviction rate, and persistent allegations of political bias. These issues highlight the need for comprehensive reform to strengthen the agency's operational efficiency and restore public confidence in its impartiality.

The ED's current limitations stem from both structural and technological shortcoming. Unlike advanced financial crime units in countries like the U.S. and UK, the ED lacks cutting edge tools for real time transaction monitoring and forensic analysis of digital financial crimes. The agency's heavy reliance on manual investigation methods hampers its ability to keep pace with increasingly sophisticated money laundering techniques, particularly in cryptocurrency transactions and cross-border fund flows. Furthermore, the absence of specialized financial court and alternative dispute resolution mechanisms results in excessive delays, with cases often languishing for years without resolution. These systemic inefficiencies not only reduce the deterrent effect of enforcement actions but also allow economic offender to exploit legal loopholes and procedural delays to evade justice.

To transform the ED into a world-class financial crime fighting agency, India must implement a multi-pronged reform strategy. This should include establishing dedicated PMLA fast-track courts, adopting AI-driven financial surveillance systems, and creating an independent oversight mechanism to ensure transparency and accountability. Strengthening international cooperation through pre negotiated asset recovery treaties and enhancing inter agency coordination within India's financial regulatory ecosystem are equally critical. By addressing these challenges and implementing global best practices, the ED can evolve into a more efficient and respected institution capable of effectively combating 21st-century financial crimes while maintaining the delicate balance between enforcement power and democratic accountability. The coming years will be crucial in determining whether the ED can overcome its current limitation and fulfill its potential as a bulwark against economic offenses in India's rapidly evolving financial landscape.

BALANCING ANTI-MONEY LAUNDERING COMPLIANCE AND FINANCIAL INCLUSION: CHALLENGES AT THE CROSSROADS OF ENERGY ACCESS AND CLIMATE FINANCE

Tanvi Joshi
5th Year Student, BBA.LLB, Unitedworld School of Law,
Karnavati University

ABSTRACT

The paper analyses the complicated connection between anti-money laundering (AML) compliance and financial inclusion in developing countries, with a particular emphasis on the growing relevance of energy access and climate funding. While AML procedures seek to protect financial institutions, strict laws, notably KYC standards, frequently prevent low-income and marginalized communities from accessing formal financial services. This exclusion is particularly problematic in sectors such as clean energy, where digital payments provide access to solar power and energy subsidies. The paper examines international standards, such as FATF principles, and uses case studies from India and Kenya to demonstrate successful regulatory modifications. It also investigates the increased possibility of money laundering in climate-related financial flows like carbon markets and green bonds. The paper ends with recommendations for risk-based KYC, digital identification systems, and specialized AML frameworks to enhance financial inclusion while maintaining compliance, thereby supporting both energy equity and financial integrity.

Key words: *Anti-Money Laundering, Financial Inclusion, Risk-Based KYC, Energy Access, Climate Finance.*

Introduction

Anti-money laundering (AML) procedures are critical to ensuring the integrity of the global financial system. However, these approaches frequently pose hurdles to financial inclusion, especially in developing economies where a sizable segment of the population is unbanked or underbanked[1].

The issue statement is about balancing the need for AML compliance with encouraging financial access. Developing economies have the issue of developing comprehensive AML standards that do not inadvertently prohibit legitimate individuals and enterprises from using financial services[2].

The fundamental research issue in this study is: How can emerging economies strike an effective balance between anti-money laundering (AML) compliance and financial inclusion, particularly in the context of energy access and climate finance?

The paper tries to examine this equilibrium, with a particular emphasis on developing economies and the inclusion of underprivileged communities that rely on digital financial services for energy solutions like pay-as-you-go solar and subsidy-linked LPG distribution. Key objectives include analysing the legislative and regulatory frameworks that support AML measures, assessing their impact on financial inclusion in the energy and climate finance sectors, and proposing adaptive strategies such as risk-based KYC and technology-driven

[1] Financial Action Task Force, Revised Guidance on AML/CFT and Financial Inclusion (Mar. 2017), available at:https://www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Revisedguidanceonamlcftand financial inclusion.html.

[2] Financial Action Task Force, Public Consultation on Amendments to Recommendation 1, Immediate Needs Rating 1 & 10, and Immediate Needs Rating 15 (Oct. 24, 2023), available at: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/R1-INR1-INR10-INR15-Public-Consultation-Oct-24.html.

regulatory approaches to align AML compliance with inclusive and sustainable finance goals[3].

The scope of this paper:

A study of the FATF's recommendations and their implications for financial inclusion. Analysis of risk-based AML/CFT measures and their potential impact on underserved communities[4]. Explore simpler measures and proportionality principles in AML regulations[5]. This paper investigates the complex interplay between anti-money laundering (AML) compliance and financial inclusion in developing economies, with a specific focus on the emerging nexus of energy access and climate finance. Impact low-income populations' access to formal financial services, especially in contexts reliant on digital finance for energy solutions like pay-as-you-go solar and subsidy-linked LPG distribution.

The study analyzes the challenges posed by stringent customer due diligence (CDD) requirements and evaluates innovative risk-based approaches such as tailored KYC procedures, regulatory sandboxes, and public-private partnerships that can mitigate exclusion. Additionally, it addresses the rising concerns of money laundering risks in climate and energy finance, proposing context-sensitive AML measures that protect green investment flows without stifling financial inclusion.

By incorporating case studies from India and Kenya, this research aims to contribute to policy discourse on harmonizing financial integrity with inclusive energy access, advocating for flexible, technology-enabled, and sector-specific AML regulations that support sustainable development and equitable growth.

Overview of Anti-Money Laundering (AML) Measures

Anti-money laundering (AML) measures are essential components of financial crime prevention. They often include:

Customer Due Diligence (CDD) requires financial organizations to verify customers' identities and assess their risk profiles[6].

Suspicious Transaction Reporting (STR): Financial institutions must disclose transactions suspected of being associated with money laundering or terrorist financing[7].

Record Keeping: Keeping accurate records of client information and transactions for a lengthy period[8].

---

[3] Council of Europe, Financial Inclusion and Moneyval (2019), available at: ttps://www.coe.int/en/web/moneyval/implementation/financial-inclusion.

[4] Haseeb A. Ahmad et al., Analyzing the Role of Anti-Money Laundering Measures in Financial Inclusion and Financial System Stability: Evidence from Developing Economies, 11 Cogent Econ. & Fin. 1 (2023), available at: https://www.tandfonline.com/doi/full/10.1080/23322039.2023.2235821.

[5] Int'l Monetary Fund, Anti-Money Laundering and Combatting the Financing of Terrorism (AML/CFT), available at: https://www.imf.org/en/Topics/Financial-Integrity/amlcft (last visited Nov. 6, 2024).

[6] *Supra* note 6

[7] *Supra* note 7

[8] Paolo Mauro, Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) in Sub-Saharan Africa (IMF Working Paper No. 09/03, 2009), available at: https://www.imf.org/external/pubs/ft/dp/2009/afr0903.pdf.

International frameworks have an important influence on defining national anti-money laundering policies.

The Financial Action Task Force (FATF) is the leading global standard-setter for anti-money laundering and counter-terrorism measures. FATF Recommendations define international norms that governments are expected to follow. These standards have a global impact on national regulations, even those in developing economies[9].

National anti-money laundering laws and regulations in developing economies largely follow international norms.

Most nations have passed AML legislation based on FATF recommendations. These rules often require financial institutions to develop CDD protocols, keep transaction records, and report any questionable transactions[10]. Due to limited resources and infrastructure, developing economies may struggle to meet compliance requirements[11].

Financial institutions in these nations frequently face the following consequences:

Increased operational costs are related to adopting strong compliance systems. Strict KYC requirements may exclude underserved communities. Challenges in keeping correct records and efficiently reporting questionable transactions[12].

Developing economies face distinct hurdles when it comes to implementing anti-money laundering measures and boosting financial inclusion. They must reconcile the requirement for financial stability with the imperative to provide access to financial services for all segments of society[13].

Financial Inclusion in Developing Economies

Financial inclusion refers to attempts to make financial products and services available and affordable to all individuals and businesses, regardless of personal wealth or corporate size. Its significance goes beyond economic growth; it also contributes significantly to poverty reduction and overall financial empowerment[14].

The existing state of financial inclusion in developing economies poses numerous challenges:

In many rural and neglected communities, there is a dearth of physical banking facilities. Limited financial literacy: Potential customers frequently lack understanding of formal financial services. Regulatory barriers: Strict Know-Your-Customer (KYC) regulations may exclude vulnerable communities.

---

[9] *Supra* note *6*

[10] *Supra* note *6*

[11] *Supra* note *7*

[12] *Supra* note 8

[13] *Ibid.*

[14] Julia Kagan, Financial Inclusion, Investopedia (July 15, 2022), available at: https://www.investopedia.com/terms/f/financial-inclusion.asp.

According to the World Bank, around 1.7 billion adults globally were unbanked in 2021, with a large proportion residing in developing economies. This emphasizes the enormity of the dilemma confronting governments and financial institutions.

Key stakeholders in fostering financial inclusion are:

Governments play an important role in developing enabling policies and laws.

Financial Institutions: Banks and non-bank financial institutions provide numerous products and services[15].

Non-governmental organizations (NGOs) such as Grameen Bank have pioneered innovative financial inclusion initiatives[16]. International organizations such as the World Bank and IMF provide help and guidance[17]. Fintech companies are bridging gaps in financial access. Civil society advocates for policies that promote financial inclusion[18].

Taking on the difficulties of financial inclusion demands a multifaceted strategy. Policymakers should prioritize developing favourable regulatory regimes, while financial institutions should offer appropriate solutions for neglected markets. Technology continues to play an important role in increasing access to financial services, notably via digital platforms and agent banking models[19].

Finally, achieving universal financial inclusion remains a major problem for developing countries. However, the potential benefits in terms of economic growth, poverty reduction, and overall development make ongoing efforts to achieve this aim critical[20].

The Tension Between AML Measures and Financial Inclusion

AML policies can unintentionally impede financial inclusion in a variety of ways:

Stringent KYC (Know Your Customer) requirements: These can exclude disadvantaged populations who lack sufficient identifying documentation and financial histories. Expansion into underserved areas can be hindered by the high implementation and maintenance costs of complex transaction monitoring systems. Record-keeping requirements: Keeping detailed records for long periods can be difficult, especially in resource-constrained contexts[21].

---

[15] *Ibid*

[16] *The World Bank, Financial Inclusion Overview, available at: https://www.worldbank.org/en/topic/financialinclusion/overview (last visited Nov. 6, 2024).*

[17] *Ibid*

[18] Nitesh Chhaparia, Financial Inclusion, Anti-Money Laundering and Combating Financing of Terrorism, MPRA Paper No. 120213, Univ. of Munich (May 2023), available at: https://mpra.ub.uni-muenchen.de/120213/1/MPRA_paper_120213.pdf. available at:

[19] Md. Monirul Islam & Md. Selim Raihan, The Role of Financial Inclusion in Anti-Money Laundering in Developing Economies, 17 J. Risk Fin. Mgmt. 105 (2023), available at: https://www.mdpi.com/1911-8074/17/3/105.

[20] Simon Gray, Financial Inclusion and AML/CFT Policies in Emerging Economies, IMF Working Paper No. 20/157 (2020), available at: https://www.elibrary.imf.org/view/journals/001/2020/157/article-A001-en.xml.

[21] Consultative Grp. to Assist the Poor, Anti-Money Laundering Regulation and Financial Inclusion (Oct. 2020), available at: https://www.cgap.org/blog/anti-money-laundering-regulation-and-financial-inclusion.

These measures disproportionately affect the unbanked and underbanked:

Documentation issues: Many people lack birth certificates, passports, or other necessary identifying documents. Limitations in financial history: Applicants without prior banking links may struggle to meet verification requirements. Complexity barrier: Lack of simplified verification methods hinders access to formal financial systems[22].

High compliance costs for AML processes may hinder financial institutions from offering services to low-income or rural areas.

Implementing robust AML systems increases operating expenses. Hiring compliance officers and training staff can increase overhead costs. Sophisticated monitoring systems can be costly to purchase and maintain[23]. Compliance requirements can limit agent network reach. These challenges are reflected in statistics. According to CGAP, "about 1.7 billion adults worldwide remained unbanked in 2021,"[24], emphasizing the magnitude of the challenge for governments and financial institutions.

Recent developments aim to address the following issues:

The FATF has provided more specific guidelines on reconciling AML/CFT regulations with financial inclusion objectives. New record-keeping requirements offer greater flexibility, potentially reducing compliance burdens. The guidance allows for verifying client identity after establishing a business connection, rather than real-time verification.

However, the implementation of these adjustments remains critical. Countries must translate the FATF standards into realistic regulatory and supervisory frameworks. Proactive information sharing across the public and private sectors, as well as between countries, can assist in meeting the problems and opportunities presented by new standards[25].

Ultimately, striking a balance between AML compliance and financial inclusion would necessitate ongoing efforts from regulators, financial institutions, and technology vendors. The purpose is to protect against illicit money flows while maintaining access to fundamental financial services for all segments of society[26].

---

[22] World Bank, *Impact of the FATF Recommendations and Their Implementation on Financial Inclusion: Insights from Mutual Evaluations and National Risk Assessments (2022), available at:* https://documents1.worldbank.org/curated/en/597781637558061429/pdf/Impact-of-the-FATF-Recommendations-and-their-Implementation-on-Financial-Inclusion-Insights-from-Mutual-Evaluations-and-National-Risk-Assessments.pdf.

[23] RiskBusiness, *Governance and Risk in Banking for the Unbanked: Compliance Challenges of Financial Inclusion Initiatives* (Oct. 2023), *available at*: https://riskbusiness.com/blog/governance-and-risk-in-banking-for-the-unbanked-compliance-challenges-of-financial-inclusion-initiatives/.

[24] Oxfam, *Bank De-Risking: The Gaps in the World Bank's Defining Financial Inclusion (2015), available at*: https://www-cdn.oxfam.org/s3fs-public/file_attachments/rr-bank-de-risking-181115-en_0.pdf.

[25] Caitlin McGough, Assessing the Impact of AML Regulations on Financial Inclusion in Developing Economies, Duke J. of Econ. (2016), available at: https://sites.duke.edu/djepapers/files/2016/10/caitlinmcgough-dje.pdf.

[26] David Birch, I'm Anti the Anti-Money Laundering Rules, Forbes (May 3, 2021), available at: https://www.forbes.com/sites/davidbirch/2021/05/03/im-anti-the-anti-money-laundering--rules/.

Case Studies in Balancing AML and Financial Inclusion

Kenya's mobile banking revolution through M-Pesa illustrates a healthy balance between anti-money laundering measures and financial inclusion.

M-Pesa, introduced in 2007, used mobile phone networks to give financial services to millions of Kenyans, many of whom did not have traditional bank accounts. The platform implemented strong anti-money laundering controls while simplifying access to financial services[27].

Key success elements were:

Regulatory flexibility: The Central Bank of Kenya permitted new payment systems while ensuring control.

Safaricom and Vodafone formed a public-private collaboration to establish and operate M-Pesa.

Technological advancement: Mobile phones offered wider access to financial services[28].

In India, reduced KYC regulations for low-risk accounts show another successful approach:

India eased KYC requirements for opening small savings accounts in 2019. This initiative allowed banks to open basic savings accounts for some types of customers without requiring full KYC documentation[29].

The success aspects in this situation were: Regulatory changes: The Reserve Bank of India lowered KYC criteria for low-risk accounts. A gradual approach was used, with full KYC still necessary for higher-value accounts or services[30].

Balancing act: The adjustment ensured AML integrity while promoting financial inclusion[31].

Both situations demonstrate the significance of regulatory flexibility, public-private partnership, and technical innovation in combining anti-money laundering measures with financial inclusion objectives. These examples show that it is feasible to tighten AML frameworks while increasing access to financial services, particularly in developing economies.

---

[27] Shaktikanta Das, Role of Technology in AML Compliance, Bank for International Settlements (July 14, 2019), available at: https://www.bis.org/review/r190714a.htm

[28] Shaktikanta Das, Role of Technology in AML Compliance, Bank for International Settlements (July 14, 2019), available at: https://www.bis.org/review/r190714a.htm.

[29] Reserve Bank of India, Annual Report on AML/CFT Policies (2019), available at: https://rbi.org.in/Scripts/PublicationsView.aspx?url=/pub/bt/bullettin/bt2109/bt21_09_01.pdf.

[30] *Ibid*

[31] *Ibid*

Energy Access, Financial Inclusion, and the AML Challenge in Developing Economies

Access to sustainable energy is widely regarded as both a developmental imperative and a crucial promoter of financial inclusion in low-income and rural communities. As energy systems decentralize through mobile solutions and climate finance flows grow, a complicated interaction emerges between energy access, financial inclusion, and anti-money laundering (AML) compliance. In many emerging economies, this convergence affords both opportunities to advance development goals and obstacles posed by regulatory limits.

Energy access as a catalyst for financial inclusion.

Energy access is intimately related to financial inclusion. Off-grid energy solutions, notably Pay-As-You-Go (PAYG) solar models, use digital payment systems such as mobile money to collect small, recurring payments from customers. These systems, which are popular in East Africa, South Asia, and portions of Latin America, enable low-income people to purchase solar energy systems without making big upfront payments[32]. For example, in Kenya, M-KOPA has enabled over one million families to receive sustainable energy using mobile-based instalment plans linked to M-Pesa, a digital wallet platform regulated by the Central Bank of Kenya for anti-money laundering[33].

However, stringent anti-money laundering and Know Your Customer (KYC) regulations might make it difficult to participate in such energy-related financial services. Many rural consumers lack the proper identity needed to open mobile money accounts or obtain subsidies and credit. The Financial Action Task Force (FATF) recognizes this difficulty and suggests risk-based customer due diligence (CDD) for underprivileged communities[34]. However, national authorities frequently impose too strict rules that fail to reflect the low-risk nature of small-scale energy transactions.

AML Risks in Energy Financing and Climate Investment

On a macroeconomic level, the increased influx of climate financing and green energy investments creates new dangers to financial integrity. Developing countries are increasingly receiving funds from international climate mechanisms, carbon credit systems, and sovereign green bonds. These financial flows, while critical to achieving Sustainable Development Goal 7 on energy access, may be used for illegal financial activity in the absence of appropriate anti-money laundering controls[35].

Carbon markets, for example, are generally unregulated in many states. Fraudulent emission reporting and manipulation of carbon credit valuations have been observed, raising worries about money laundering via

---

[32] *Supra* note 21

[33] Gray, Simon. *Financial Inclusion and AML/CFT Policies in Emerging Economies,* IMF Working Paper No. 20/157 (2020), *available at:* https://www.elibrary.imf.org/view/journals/001/2020/157/article-A001-en.xml.

[34] Financial Action Task Force. *Revised Guidance on AML/CFT and Financial Inclusion* (Mar. 2017), *available at*: https://www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Revisedguidanceonamlcftandfinancialinclusion.html.

[35] Islam, Md. Monirul, & Md. Selim Raihan. *The Role of Financial Inclusion in Anti-Money Laundering in Developing Economies,* 17 J. Risk Fin. Mgmt. 105 (2023), *available at*: https://www.mdpi.com/1911-8074/17/3/105.

environmental finance[36]. Additionally, energy procurement contracts and concessional loans for infrastructure development sometimes lack transparency, particularly in shaky governance contexts. This has led calls for AML frameworks specific to the green energy and climate finance industries[37].

Country examples are Kenya and India.

Kenya's M-KOPA system demonstrates how mobile-enabled energy access can coexist with AML compliance if authorities take a flexible approach. The Central Bank of Kenya has approved the use of mobile money in low-value energy purchases while adhering to AML requirements such as suspicious transaction notification and agent due diligence. According to the IMF, Kenya's success stems from its risk-based use of KYC standards, which minimizes compliance burdens for low-risk, high-impact financial products[38].

In contrast, India's Direct Benefit Transfer (DBT) scheme demonstrates how rigid KYC requirements might impede energy access. The DBT plan requires consumers of LPG (liquefied petroleum gas) subsidies to have Aadhaar-linked bank accounts, which excludes many women, migrants, and rural residents who lack such documents[39]. Despite India's streamlined KYC rules for small savings accounts, full compliance remains a hurdle to getting energy subsidies and loans for clean cooking or rooftop solar installation.

Policy Recommendations: Aligning Energy Inclusion and AML Integrity

To balance AML enforcement with the need for energy access, the following initiatives should be prioritized:

Implement Tiered KYC in Energy Finance: The FATF's 2017 advice promotes simpler due diligence for low-risk transactions. Developing nations should establish tiered KYC regimes for energy-related mobile payments, permitting the use of alternate identification papers[40].

Create AML Frameworks for Climate Finance: As climate-linked funds expand, authorities must use sector-specific tools to monitor green investments and ensure accountability in carbon credit markets and energy infrastructure contracts[41].

Promote Interoperable Digital Identity Systems: By integrating national ID systems with mobile banking and energy platforms, compliance can be streamlined while also encouraging inclusiveness. Despite being

---

[36] Financial Action Task Force. International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: FATF Recommendations (June 2019), available at: https://www.fatf-gafi.org/en/publications/financialcrime/FATFRecommendations.html.

[37] World Bank. Impact of the FATF Recommendations and Their Implementation on Financial Inclusion (2022), available at: https://documents1.worldbank.org/curated/en/597781637558061429/pdf.

[38] Mauro, Paolo. Anti-Money Laundering and Combating the Financing of Terrorism in Sub-Saharan Africa, IMF Working Paper No. 09/03 (2009), available at: https://www.imf.org/external/pubs/ft/dp/2009/afr0903.pdf.

[39] IReserve Bank of India. Annual Report on AML/CFT Policies (2019), available at: https://rbi.org.in/Scripts/PublicationsView.aspx?url=/pub/bt/bullettin/bt2109/bt21_09_01.pdf.

[40] Financial Action Task Force. Revised Guidance on AML/CFT and Financial Inclusion (Mar. 2017), available at: https://www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Revisedguidanceonamlcftandfinancialinclusion.html.

[41] *Supra note* 7

problematic, India's Aadhaar scheme has enabled millions of people to get digital subsidies[42].

Leverage RegTech and FinTech: AML compliance technology like AI-based transaction monitoring and biometric verification can reduce operating costs while increasing transparency. Fintechs that provide PAYG energy can benefit from regulatory sandboxes, which allow for limited experimentation with supervisory monitoring[43].

Encourage public-private partnerships: Governments, financial authorities, energy corporations, and civil society must work together to create inclusive financial architectures that facilitate clean energy transitions. Joint data exchange and regulatory co-creation are critical.

Integrating energy access goals into financial inclusion and anti-money laundering agendas opens new opportunities for regulatory and policy innovation. Clean energy finance, digital utility payments, and climate-linked investments are all examples of financial activities that must be AML-compliant while being accessible to low-income populations. Developing economies must consequently adopt flexible, risk-sensitive ways that uphold AML rules without excluding vulnerable individuals from crucial services.

Countries may ensure that the shift to clean energy coincides with the transition to inclusive and secure financial ecosystems by bridging the AML-financial inclusion barrier through technology, collaboration, and sector-specific guidelines.

Recommendations for Balancing AML and Financial Inclusion

Implementing tiered KYC standards based on risk is a viable strategy to balance AML measures and financial inclusion.

Low-risk persons should go through streamlined KYC procedures, lowering obstacles to fundamental banking services. This methodology conforms with FATF principles, which suggest a risk-based approach to customer due diligence. Tiered KYC systems can recognize alternative ID documents typically used by underserved groups[44]. Capacity-building and financial literacy programs are critical. Educating communities on AML principles increases trust in formal banking institutions. These campaigns educate individuals on the significance of appropriate identification and transaction monitoring[45].

Regulatory sandboxes can drive innovation: Controlled environments enable the testing of novel financial products under looser AML regulations[46].

---

[42] Das, Shaktikanta. Role of Technology in AML Compliance, Bank for International Settlements (July 14, 2019), available at: https://www.bis.org/review/r190714a.htm.

[43] Chhaparia, Nitesh. Financial Inclusion, Anti-Money Laundering and Combating Financing of Terrorism, MPRA Paper No. 120213, Univ. of Munich (May 2023), available at: https://mpra.ub.uni-muenchen.de/120213/1/MPRA_paper_120213.pdf.

[44] World Bank, Digital Finance: Action 1 (2022), available at: https://digitalfinance.worldbank.org/action-1

[45] *Ibid*

[46] *Ibid*

This method allows fintech organizations to provide innovative solutions while being compliant[47].

Key success factors for these programs include regulatory flexibility, public-private cooperation, and harnessing technological breakthroughs[48]. By employing these techniques, emerging economies can strengthen anti-money laundering regimes while increasing access to financial services for underprivileged populations.

Conclusion

Major findings emphasize the complex relationship between anti-money laundering efforts and financial inclusion.

AML standards may mistakenly exclude vulnerable people who lack adequate documentation or financial history. High compliance costs deter financial institutions from serving low-income or rural communities. Maintaining a balance between AML compliance and financial access involves ongoing efforts from regulators, financial institutions, and technology suppliers[49].

Possible solutions include:

Implementing KYC standards based on risk level. Leveraging technology to improve AML compliance and financial access. Capacity-building and financial literacy programs can help promote compliance and trust in formal financial institutions. Using regulatory sandboxes to test innovative financial products under looser AML regulations[50].

Developing economies must protect their financial systems while providing access to disadvantaged populations. This necessitates new solutions that combine strong AML standards with flexible regulatory contexts and technological advances[51].

---

[47] iDenfy, AML and KYC Compliance for Fintech Companies (2023), available at: https://www.idenfy.com/blog/aml-kyc-fintech/.

[48] *Ibid*

[49] *Supra note* 21

[50] World Bank, *Digital Finance: Action 1* (2022),*available at*: https://digitalfinance.worldbank.org/action-1.

[51] *Supra note* 21

2 G SCAM CASE

Prakshaal Jain
Student, GIBS, Delhi.

ABSTRACT

The 2G spectrum case was one of India's biggest political and financial scandals, unravelling in 2008 when the government allocated telecom licenses at throwaway prices, bypassing competitive bidding. This arbitrary allocation allegedly caused a loss of ₹1.76 lakh crore to the public exchequer, as estimated by the CAG. The scandal implicated top politicians, including then Telecom Minister A. Raja, and corporate executives, sparking nationwide outrage and legal action. In 2011, the Supreme Court cancelled 122 licenses, calling the allocation unconstitutional. However, in a dramatic turn, all accused were acquitted in 2017 due to lack of evidence, leaving the public disillusioned about accountability in high-level corruption. The case became a symbol of systemic flaws in governance and regulatory oversight.

Key words: *2G spectrum scam, telecom license, A. Raja, CAG report, Supreme Court, corruption, political scandal, public exchequer, acquittal, governance failure.*

Introduction

The 2G spectrum allocation scandal (often called the "2G scam") erupted in India in 2010–2011 and centered on the controversial issuance of 122 (some reports say 123) second-generation (2G) mobile spectrum licenses in 2008. The then Telecom Minister, A. Raja, was accused of abusing his discretionary powers to grant these licences at artificially low prices and with irregular procedures. A detailed audit by the Comptroller and Auditor General (CAG) concluded that the spectrum was allotted on outdated 2001 price bases, resulting in a presumptive revenue loss of around ₹1.76 lakh crore. Public litigation followed, and in 2012 the Supreme Court of India, responding to petitions (notably *Centre for Public Interest Litigation* v. Union of India) invalidated the 122 licences as "totally arbitrary and unconstitutional".[1] After a lengthy trial, however, a special CBI court acquitted all accused in December 2017.[2] The 2G case thus spans dramatic twists – from political uproar and a landmark Supreme Court order to all-round acquittals – and remains highly consequential for India's legal, regulatory and political landscape. This paper provides a comprehensive account of the 2G spectrum [3] case, covering the facts of the alleged scam, the investigations by agencies (CAG, CBI, ED), the legal proceedings (including key case law and statutes), the political and public impact, and a critical analysis of the trial acquittal and its aftermath.

Detailed Overview of the 2G Spectrum Allocation Process and Allegations

Understanding the 2G scam requires some background on India's telecom licensing policy. In the late 1990s and 2000s, the government moved to liberalize telecommunications. Under the New Telecom Policy 1999, allocation of telecom spectrum licences for 2G services (basic mobile telephony) was typically done on a *first-*

---

[1] Pti and Ians, "2G Case: Some Relief for Chidambaram but No Comfort for Govt,", Hindustan Times, Feb. 04, 2012, available at: https://www.hindustantimes.com/delhi/2g-case-some-relief-for-chidambaram-but-no-co mfort-for-govt/story-EJ3LJiUEDDjopSXF0rrNpJ.html#google_vignette (last visited on June 4, 2025).

[2] Apurva Vishwanath, "Why Court Acquitted 2G Accused: 'First-Come, First-Served' Policy Was Not Clear,", *The Print*, Dec. 21, 2017, *available at*: https://theprint.in/report/court-acquitted-2g-accused-first-come-first-served-policy-not-cle ar/24181/ (last visited on June 4, 2025).

[3] *Ibid*

come, first-served (FCFS) basis, with companies paying a fixed licence fee. (By contrast, allocation of newer services like 3G/mobile broadband was moved to auctions.) In practice, this meant applicants who met entry criteria and paid fees received licences in order of application, without competitive bidding. This FCFS system had been in place since 2003 for Unified Access Service licences (which include voice and data).

In 2008, however, India's booming telecom sector saw a flood of new licence applications. By then, the number of new applications greatly exceeded available spectrum. The Department of Telecommunications (DoT) under Minister A. Raja (of the ruling UPA coalition) undertook a new round of 2G licence allocations in late 2007 and early 2008. Raja's Ministry framed the process as helping small firms by raising the foreign equity cap (to 74%) and promising spectrum at older, lower prices to spur competition. Critically, Raja's DoT set a new *"cut-off date"* for eligibility: on 10 January 2008, it announced that licences would be issued *a posteriori* to a cut-off of 25 September 2007. Applicants were then given only 45 minutes on that day to furnish performance bank guarantees, pay licence fees and complete paperwork. This sudden notice – 25 September as the cut-off and a very short window on 10 January – effectively excluded many earlier applicants and advantaged those who had been secretly tipped off.

Companies linked to particular business groups and politicians (notably connected to DMK leader M. Karunanidhi and other UPA allies) were able to meet these deadlines. By the evening of 10 January, 122 new licenses were issued to mobile operators for various "circles" (geographic areas).

Among the companies that obtained licences were several controversial new entrants and joint ventures: Uninor (Telenor/Unitech), Loop Telecom (Khaitan family), Sistema Shyam (Russia/Shyam group), Swan Telecom–Etisalat (DB Realty/Etisalat), S-Tel (Goyal), Videocon Telecom (Videocon Group), Tata Teleservices (CDMA services), and Idea Cellular (expansion of existing network), among others.[4] These allocations were made at the entry fee of ₹1,658 crore for a pan-India licence (roughly ₹2,000 crore for a pan-Indian 3G licence was charged in 2009), far below what the market seemed to bear. In fact, a 3G spectrum auction in 2010 (with fewer slots) fetched about ₹69,000 crore, whereas the entire 2G round yielded only about ₹9,000 crore. This striking disparity – and the opaque process – triggered immediate controversy.[5]

Key chronology: After the January 2008 allocations, industry insiders grew suspicious. An NGO petition (Centre for Public Interest Litigation) filed for a probe. The CAG audit was undertaken in 2009–2010. In May 2009, the media first reported an NGO complaint (Telco Watchdog) to the CVC. By October 2009, the CBI had started an inquiry. In May 2010, the NGO CPIL filed a petition in the Delhi High Court for CBI investigation. On 10 November 2010, CAG Vinod Rai unveiled the audit findings to Parliament, alleging a ₹1.76 lakh crore revenue loss due to the 2008 allocations.[6] (At that point Telecom Minister Raja resigned on 14 Nov 2010.) The Supreme Court took notice of the CAG report and, on 2 February 2012, cancelled the 122/123 licences, calling the 2008 procedure "totally arbitrary and unconstitutional".

---

[4] India Today Online, "SC Cancels All 123 2G Licences Issued by Raja", India Today, Feb. 02, 2012, available at: https://www.indiatoday.in/2g-scam/in-the-courts/story/sc-cancels-all-122-2g-licences-iss ued-by-raja-91688-2012-02-01 (last visited on June 4, 2025).

[5] *Ibid.*

[6] Express Web Desk, "G Case Verdict: CBI Court Acquits a Raja, Kanimozhi and All Other Accused", *The Indian Express*, Dec. 21, 2017, *available at*: https://indianexpress.com/article/india/2g-spectrum-scam-in-a-big-relief-to-a-raja-and-ka nimozhi-cbi-court-acquits-all-accused-4992453/ (last visited on June 4, 2025).

- October 2009: CBI registers a case on 2G allocation irregularities.[7]
- November 2010: CAG report to Parliament alleges ₹1.76 lakh crore loss due to underpricing. Telecom Minister Raja resigns.
- 2 Feb 2012: Supreme Court (Singhvi & Ganguly JJ.) quashes all 122 licences as "arbitrary" and orders auctions.
- Dec 21, 2017: Special CBI Court (Judge O.P. Saini) acquits A. Raja, Kanimozhi and all others in the case.[8]

These steps show the scope of the allegations: an audit by CAG (a constitutional body) highlighted procedural improprieties (e.g. ex-post announcing of cut-off, sidestepping ministries' advice), and Indian courts intervened. The saga engulfed much of 2010–2012, driving legal and political churn; it was widely deemed "India's biggest corruption scandal" at the time.[9]

Legal Proceedings: Investigations, Charges and Trial

The legal fallout of the 2G allegations involved multiple threads: public interest litigation, a Supreme Court verdict, criminal investigations and trials. The Supreme Court initially dealt with writ petitions (by CPIL and others) challenging the 2008 allocations. In February 2012 the Court cancelled the licences. Crucially, it mandated a special CBI court to try the criminal charges (rather than regular courts). Accordingly, the CBI and the Enforcement Directorate (ED) filed formal charges in 2011–2014.

On the prosecution side, the Central Bureau of Investigation (CBI) framed a sprawling chargesheet. The charges generally alleged criminal conspiracy (Section 120B, IPC) and corruption (Section 13 of the Prevention of Corruption Act, 1988) in shifting, in collusion with businessmen, the spectrum allotments in 2007–08. The case covered several figures: A. Raja (telecom minister), Kanimozhi Karunanidhi (DMK MP), DoT officials (like Sanjeev Chaturvedi), and corporate promoters (e.g. Kiran and IP Khaitan of Loop, Shahid Balwa of Swan/DB Realty). In October 2011 the CBI formally charged 17 accused under Sections 120B IPC and 13(2) read with 13(1)(d) of the PC Act. (Subsequently, in 2014 the ED filed a money-laundering case under the PMLA against Raja, Kanimozhi and others, based on the same facts.)

The trial in the Special CBI Court (Patiala House, Judge Saini) commenced in late 2011. The CBI's case included witness testimony and purported paper trails (phone logs, letters). For example, the prosecution alleged that Raja received unlawful gratification (reportedly ₹200 crore) to award licences to Swan Telecom, via companies that were later repaid with documents back-dated to conceal the trail. It was also argued that the 2008 allocations departed from standard procedure (earlier telecom policy) and had been orchestrated to favour certain firms. The CBI argued a loss figure (for sentencing purposes) in the tune of ₹30,984 crore. The defence, in turn, contended

---

[7] Amrita Ray, "2G Spectrum Scam Case: A Chronology of What is Known to Be India's Biggest Scam", Ndtv, Dec. 22, 2017, available at: https://www.ndtv.com/india-news/2g-spectrum-scam-case-a-chronology-of-what-is-know n-to-be-indias-biggest-scam-1790535 (last visited on June 4, 2025).

[8] *Supra* note 2

[9] Abhinav Sekhri, "India's 2G Spectrum Case: The Scam that Wasn't?", *The Print*, Mar. 02, 2018, *available at*: https://globalanticorruptionblog.com/2018/03/02/indias-2g-spectrum-case-the-scam-that-wasnt/#:~:text=allegations%2C%20 and%20in%20November%202010%2C,case%20of %20abusing%20executive%20power (last visited on June 4, 2025).

that the first-come-first-served rule was followed (albeit with a shifted cut-off) and that no direct evidence linked any bribe or quid-pro-quo to decision-making.[10]

Statutes and case laws: The accused were prosecuted under specific penal provisions. Section 120B IPC (criminal conspiracy) was invoked for alleged collusion in altering licence deadlines. Corruption charges fell under the Prevention of Corruption Act (s.13), especially s.13(1)(d)(public servant taking gratification other than legal remuneration) and s.13(2) (Criminal misconduct, wilful misuse of official position causing loss to government). The ED's PMLA case required that "proceeds of crime" exist from the predicate offence.

Notably, no statute mandated auctions for spectrum; this was a matter of policy.The Supreme Court later held that auctions are not the **sole** legal method of resource allocation, as long as the chosen process meets fairness/non-arbitrariness under Art.14. In this context, the defence cited the 2012 SC precedent (CPIL v. UOI)[11] which had struck down *Raja's procedure* as arbitrary, but argued that the standards for civil annulment (as in the SC judgement) are different from those for criminal conviction. They also invoked precedents (e.g. *Dr. Prem Das* v. *Union of India* or *Bhagwan Agro* v. *Union of India*) holding that administrative discretion need not follow auctions if reasons are valid, and that mere policy irregularities, without proof of dishonesty, are not criminal.

In short, **legal proceedings** spanned: the SC's 2012 constitutional decision cancelling licences, the trial-level criminal case (*CBI* v. *Raja et al*. and *ED* v. *Raja et al*.), and future appellate issues. The evidence was exhaustively examined over six years. On 21 December 2017, the **Special CBI Court rendered its judgement in three linked cases (CBI and ED vs. Raja & Ors.)**. It emphatically **acquitted all 19 accused** of every charge,[12] ruling that the prosecution had failed to prove guilt beyond reasonable doubt. According to news reports, the court noted there was "absolutely no hesitation" in exonerating them, and that the charge-sheets were based on "misreading" documents and unsubstantiated witness statements. This verdict concluded the trial-court phase. The CBI promptly indicated in 2018–2025 that it would appeal the acquittals. As of early 2025, CBI's appeal is **pending in the Delhi High Court**.

Political Implications and Public Impact

The 2G case had massive **political reverberations**. When the CAG report became public in late 2010, it caused an uproar: *communication* Minister A. Raja resigned, and the DMK (whose leaders Raja and Kanimozhi belonged to) was forced to exit the UPA coalition in 2013. The scandal fueled opposition attacks on the ruling Congress; it was widely cited by the BJP and others in the 2014 elections, allegedly contributing to UPA's defeat.

In Parliament and the press, 2G was portrayed as emblematic of systemic corruption. Parties traded charges: the BJP demanded stringent action and justice, while the Congress side (including DMK) decried a "political witch-hunt." For instance, BJP leader and key petitioner Subramanian Swamy repeatedly pressured for action. Immediately after the 2017 acquittal, Swamy demanded that the government "immediately file an appeal"

---

[10] *Ibid*

[11] *Centre For Public Interest Litigation v. Union of India on 18 August, 2020*

[12] Apurva Vishwanath, "India's 2G Spectrum Case: The Scam that Wasn't?", The Print, Dec. 21, 2017, available at:https://theprint.in/report/court-acquitted-2g-accused-first-come-first-served-policy-not-cle ar/24181/ (last visited on June 4, 2025).

against the verdict, and warned against celebrating prematurely (citing a similar reversal in the Jayalalithaa disproportionate assets case). DMK leaders, by contrast, hailed the outcome: Kanimozhi remarked that the acquittal "validat[ed] the rightfulness" of her actions.

Public reactions were mixed. Many citizens and analysts were shocked that the court did not convict anyone in what was thought to be a ₹1.76-lakh-crore scam. Media commentators described the acquittal as "unprecedented" or "stunning". Some saw it as proof that the 2G case had been overblown. (Notably, a later analysis argued that the Special Court felt the evidence was largely circumstantial and that "a huge scam was seen by everyone when there was none" – though formal reports of the verdict focused on evidentiary failings.) Civil society reaction included calls for legislative reform; critics noted that the case exposed gaps in India's anti-corruption laws. For example, legal experts pointed out that, under the Prevention of Corruption Act, mere administrative blunders do not suffice for conviction absent proof of dishonest intent. In political discourse, the case intensified scrutiny of public audit processes: Rajasthan CM Ashok Gehlot later noted that Vinod Rai had even "apologised in writing" to Congress leader Sanjay Nirupam for certain statements from the CAG report, reflecting that debate over the findings continued. [13]

A lasting impact of the scandal was policy change: following the CAG report and Supreme Court order, India adopted an **auction-based** regime for spectrum allocation (beginning in 2010–2012)[14] to promote transparency. Telecom policies were overhauled, and in practice, all subsequent spectrum, including 2G/3G/4G, has been auctioned. The case also influenced perceptions of accountability: it underscored tensions between judicial activism and prosecutorial thresholds. Though the licences were cancelled in court, many of the beneficiaries (e.g. Uninor/Telenor, Idea, Videocon) eventually received new spectrum or migrated to 3G/4G in later auctions; however, some foreign investors (like Telenor) reportedly threatened legal action for investor losses. In summary, the 2G saga deeply affected India's political narrative and reforms, even as its legal conclusion (acquittals) left contested questions.

Investigative Process and Findings

CAG Audit (2009–2010): The Comptroller and Auditor General's office conducted a *performance audit* of the 2007–08 spectrum allocations. Its report (tabulated in Parliament on 10 Nov 2010) was scathing. The CAG found that the Department of Telecom had advanced the licence cut-off date without transparency, ignored the advice of the Prime Minister and Law Ministry, and effectively violated its own procedures. It noted that the licences were issued at prices based on 2001 rates, which were far below current values. The CAG estimated the *"presumptive" revenue loss* to be about ₹1.76 lakh crore, calculated by benchmarking against contemporaneous 3G auctions. A press report quotes CAG head Vinod Rai saying the telecom ministry had "flouted every cannon of financial propriety" by issuing licences at 2001 prices. The report also audited corporate applicants: it highlighted that

---

[13] *Supra note* 11

[14] *Guru Acharya, "Case Study on the Supreme Court Ruling on the 2G Spectrum Scam", Ssrn, Dec. 27, 2018, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2048719#:~:text=The%20verdict%20took%20the%20telecom,The%20company%20had%20appealed%20to (last visited on June 4, 2025).*

companies like Swan Telecom (Etisalat) had hidden shareholding details, and that in CAG's view **85 of the 120 licences were "illegal"** due to these violations.[15]

CAG's process was later criticized by the accused: for instance, Sanjay Nirupam (a Congress MP implicated by Rai) sued for defamation. By 2022, Vinod Rai had even written an apology to Nirupam for some claims in the audit, indicating controversy over its methodology. Nonetheless, the CAG report was the catalyst for public outrage, parliamentary action, and the Supreme Court's orders. It named A. Raja personally as having altered the FCFS scheme and giving only a 45-minute window to 'favourites'. Footnotes in the report even reproduced Raja's own notes changing the policy.

CBI and ED Investigations (2009–2014): Parallel to the audit, the CBI (national fraud/anticorruption bureau) conducted a criminal probe. Initially, in late 2009 the CBI began an inquiry (based on complaints) into irregularities. On 8 Dec 2010, the Supreme Court ordered a specially notified CBI court to hear the case, and the CBI was asked to submit its investigation reports. In early 2011, the CBI formally arrested Raja (2 Feb 2011) and others began filing chargesheets.

The CBI's case rested on evidence it had collected: testimony of government officials, records of licence files, inter-office notes, and phone records. It alleged that Raja had "brushed aside" the previous system (FCFS) and granted licences to those who paid bribes. A sensational example in prosecution evidence was the claim that ₹200 crore of ill-gotten funds flowed from Swan Telecom's foreign investors (DB Realty/Etisalat) into Kalaignar TV (a channel owned by DMK's Karunanidhi, and linked to Raja). The CBI also charged that Raja and officials conspired from January 2008 onward to distort the allocation process. In April 2011 and Sept 2011, the CBI filed supplementary charge sheets adding more accused (e.g. K. Khaitan of Loop Telecom) to widen the net.[16]

In 2014, the **Enforcement Directorate (ED)** added a money-laundering angle. It registered a PMLA case, tracking alleged laundering of the bribe money through shell companies. The ED filed its charge sheet in April 2014 and framed PMLA charges by October 2014. These charges paralleled the CBI case, focusing on the same transactions (bill payments, backdated documents) but re-cast as laundering of "proceeds of crime."

Throughout these investigations, the accused maintained that whatever allocations happened were under legal authority and policy (indeed, at the time of allocation, Raja's ministry used a policy circular to justify the 45-minute notice). The CBI's central contention – that Raja *earned* illegal gratification – turned on proving quid pro quo, which the prosecution asserted but could not substantiate beyond doubt.

Acquittal and Its Consequences

On 21 December 2017, the Special CBI Court delivered its long-awaited verdict in ***CBI* v. *A. Raja and Ors.***[17] (covering the spectrum cases) and the related ED money-laundering cases. The court *acquitted* all accused of all charges. The judgement (spanning thousands of pages) observed that the prosecution had "miserably failed to prove any charge". Judge Saini's written observations were highly critical of the case presented: he noted that

---

[15] Government of India, "Compliance Audit on Accounts, Union Government(Civil)", *Government Report*, Mar. 18, 2011, *available at*: https://cag.gov.in/en/audit-report/details/3083 (last visited on June 4, 2025).

[16] Apurva Vishwanath, "Compliance Audit on Accounts, Union Government(Civil)", *The Print*, Dec. 21, 2017, *available at*: https://theprint.in/report/court-acquitted-2g-accused-first-come-first-served-policy-not-cle ar/24181/ (last visited on June 4, 2025).

[17] *Central Bureau of Investigation v A Raja & Ors on 22 March, 2024*

there was “no evidence on the record indicating any criminality” and that the charge sheet was largely built on “misreading, selective reading, non-reading and out of context reading of the official record”. He found that the prosecution's key witnesses had contradicted their earlier statements, and that there was no documentary proof of any money passing to Raja.[18]

Crucially, Judge Saini also held that the very *policy* under which the licences were issued was not a settled, mandatory rule. He agreed with the defence that the “first-come, first-served” criterion in telecom was never codified as a rigid law, and was in fact applied in Raja's case in a *different* manner. Thus, he could not find intent to defraud merely from shifting the cut-off date. The court explicitly stated that the FCFS policy was not “clear, definite, or explicit, and left room for misinterpretation,” so one cannot infer a criminal conspiracy from its implementation. On the ED's side, the court noted that since no crime (funds given) was proved, there were no “proceeds of crime” to be laundered, meaning the PMLA charges collapsed.[19]

In sum, the Special Court concluded that the government had been “cheated by a scam that never existed.” (In the words of commentary, it said “a huge scam was seen by everyone when there was none”.) The court's findings – that the prosecution's case was largely hypothetical and uncorroborated – led to the complete acquittal. Media reports quoted the judge as remarking that the chargesheet was “well choreographed” but unsubstantiated, and that it failed to demonstrate any *mens rea* (guilty intent) by the accused.[20]

Consequences: The acquittal had significant ramifications. The Union government immediately said it would appeal to the Delhi High Court. In fact, by early 2025 the CBI's appeal was listed for hearing. Political reactions were predictable: the DMK hailed it as vindication, while opponents decried it as a failure of the justice system. Some observers argued the verdict exposed flaws in India's anti-corruption regime – for instance, that the Prevention of Corruption Act (1988) required tighter proof of corrupt intent. There were also calls to improve audit methods, given that the CAG's presumptive loss figure had been largely rejected by the court.

The case prompted a wider public debate on the balance between presumption of innocence and prosecutorial zeal. Notably, key figures later revisited their earlier statements: in 2022, former CAG Vinod Rai apologized in writing to Congress leader Sanjay Nirupam over a claim in the 2G audit, suggesting acknowledgement of mistakes.

The **law and policy lessons** continue to be studied. The Supreme Court's separate 2012 ruling had emphasized equality under Article 14 and ordered auctions going forward. The trial judgement clarified that, in the absence of a clear statutory rule mandating auctions, policy deviations are not ipso facto crimes unless linked to personal gain. The case has thus underscored the need for transparent procedures (to avoid even the *appearance* of wrongdoing) and the difficulty of proving high-level corruption in criminal court.[21]

---

[18] *Supra* note 2

[19] *Ibid*

[20] *Supra* note 9

[21] Hindustan Times, “Some Relief for Chidambaram but No Comfort for Govt”, The Hindustan Times, Feb. 04, 2012, available at: https://www.hindustantimes.com/delhi/2g-case-some-relief-for-chidambaram-but-no-comfort-for-govt/story-EJ3LJiUEDDjopSXF0rrNpJ.html (last visited on June 4, 2025).

As of this writing (2025), the legal saga is not entirely closed: the CBI's high-court appeal remains pending.[22] But regardless of the final outcome, the 2G case has already become a landmark. It has influenced how India allocates critical resources, how it conducts public audits, and how aggressively it prosecutes suspected fraud. The case leaves a mixed legacy: an example of institutional vigilance on the one side, and of the legal system's rigor in enforcing evidentiary safeguards on the other.

[22] Economic Times, "Appeal Against Acquittal of a Raja, Others in 2G Case 'Ripe' for Hearing: CBI to Delhi HC Read More At: Https://Economictimes.indiatimes.com//News/India/Appeal-Against-Acquittal-Of-A-Raja- Others-In-2g-Case-Ripe-For-Hearing-Cbi-To-Delhi-Hc/Articleshow/118252689.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign =cppst", *Economic Times*, Feb. 14, 2025, *available at*: Appeal against acquittal of A Raja, others in 2G case 'ripe' for hearing: CBI to Delhi HC Read more at: https://economictimes.indiatimes.com/news/india/appeal-against-acquittal-of-a-raja-othe rs-in -2g-case-ripe-for-hearing-cbi-to-delhi hc/articleshow/118252689.cms?utm_ source=contentofinterest&utm_medium =text& utm_ campaign=cppst (last visited on June 4, 2025.

NOTES:

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