cyril amarchand mangaldas
ahead of the curve

Investigations and White Collar Crimes Enforcement Trends

A Cyril Amarchand Mangaldas Thought Leadership Publication

Handbook on Investigations and White Collar Crimes Enforcement Trends published by Cyril Amarchand Mangaldas.

This handbook has been updated till April 30, 2025.

A Thought Leadership Publication

We now present this handbook to enable readers to have an overview of the systems and legal rules and regulations that are essential for business operations in India.

Foreword

India is poised to shape the global economic narrative, reaffirming its position as the fastest-growing large economy in the coming years. As we witness this remarkable ascent, the evolution of Indian jurisprudence, especially in relation to white-collar crime demands our collective vigilance, expertise, and strategic foresight.

The surge in financial malfeasance has prompted regulators to respond with increased sophistication and agility. India's regulatory and enforcement framework has undergone a transformative journey, adapting to the complexities of corporate misconduct, financial fraud, and emerging threats. As I have emphasized before, "Artificial Intelligence is no longer a futuristic idea—it is here, deeply embedded in the way we live, work, and govern. India has an opportunity to take a leadership role in the development of ethical frameworks for policy and regulation of AI and digital technologies."

The rapid adoption of artificial intelligence (**AI**), the intensification of Environmental, Social, and Governance (**ESG**) regulations, and India's commitment to aligning with global financial crime standards reflect this evolving paradigm. Notably, the recent repeal of colonial-era criminal statutes- including the Indian Penal Code, the Code of Criminal Procedure, and the Indian Evidence Act and their replacement with modernized legal frameworks marks a defining moment in Indian law. The Bharatiya Nyaya Sanhita (**BNS**), the Bharatiya Nagarik Suraksha Sanhita (**BNSS**), and the Bharatiya Sakshya Adhiniyam (**BSA**) have been designed to address technology-driven crimes that were previously beyond the scope of traditional legal frameworks.

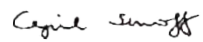
With these developments, we must also acknowledge the profound shifts within India's corporate governance landscape. India's exemplary commitment to financial crime compliance is evident in its elevated status within the Financial Action Task Force (**FATF**) framework. By securing a position among the top four G20 nations with the highest technical compliance, alongside the United Kingdom, France, and Italy, India has demonstrated its robust enforcement mechanisms. The strengthening of the Prevention of Money Laundering (**PML**) regulations has further reinforced coordination between financial intelligence units and law enforcement agencies, enhancing record-keeping practices and intensifying reporting obligations.

Global geopolitical dynamics have also reshaped legal frameworks, with trade laws, sanctions, and export controls emerging as pivotal instruments in international governance. These developments necessitate a recalibration of enforcement strategies to ensure resilience, inclusivity, and sustainability in legal policy. The legal profession must embrace this vision, leveraging technology while maintaining ethical integrity to navigate the challenges that lie ahead.

This book is a product of the Cyril Amarchand Thought Leadership Initiative, meticulously curated to provide insights into India's enforcement and investigative trends concerning white-collar crime. It examines the legal fundamentals and traces the direction of regulatory evolution, offering a roadmap for practitioners, policymakers, and stakeholders.

I extend my sincere appreciation to the contributors whose dedication and scholarly rigor have shaped this work. I trust that this volume will serve as a valuable resource, and I welcome your feedback as we continue to explore the complexities of India's legal and compliance landscape.

Thankyou,



Cyril S. Shroff
Managing Partner
Cyril Amarchand Mangaldas
cyril.shroff@cyrilshroff.com
May, 2025

Contents

Contents

Contents

A

Regulatory and Enforcement Trends in India & Investigation Best Practices

1. Statutory Developments

The Securities and Exchange Board of India (**SEBI**), on May 05, 2021, released a notification titled SEBI (Listing Obligations and Disclosure Requirements) (Second Amendment) Regulations, 2021, amending the provisions of SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 (**SEBI LODR**)[1]. The amendment was introduced to further strengthen the vigil mechanism, Risk Management Committee (**RMC**), secretarial audit, compliance requirements, and corporate governance systems, etc. One of the key amendments is the constitution of RMC for a larger number of listed entities (i.e., the top 500 to 1000 entities by market capitalisation)[2]. It oversees the risk management policy, global risk management framework, risk identification and mitigation, and sufficiency of risk management mechanisms. The board of directors of listed entities may direct the RMC to review and monitor the risk plan.[3]

Moreover, to prevent crimes in trading, the SEBI released a circular titled the Code of Conduct & Institutional mechanism for prevention of Fraud or Market Abuse, for all stock exchanges, clearing corporations and depositories (collectively called the Market Infrastructure Institutions (**MIIs**).[4] As per the circular, The MIIs have to formulate a code of conduct to regulate, monitor and report trading by designated persons and their immediate relatives. The administration will be overseen by a compliance officer.[5] Furthermore, MIIs are required to establish an institutional mechanism to preclude fraud or market abuse by the MIIs themselves, their designated persons and such immediate relatives, coupled with internal controls and whistle-blower policy.[6]

In 2025, the SEBI came out with certain guidelines that require MIIs to perform annual internal evaluations of their performance and the performance of their

[1] Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) (Second Amendment) Regulations, SEBI, (May 5, 2021), available at: SEBI | Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) (Second Amendment) Regulations, 2021
[2] *Id.*
[3] *Id.*
[4] Code of Conduct & Institutional mechanism for prevention of Fraud or Market Abuse, SEBI, (March 3, 2021), available at: SEBI | Code of Conduct & Institutional mechanism for prevention of Fraud or Market Abuse [2] *Id.*
[5] *Id.*
[6] *Id.*

statutory committees.[7] These evaluations, including both internal and independent external reviews, must adhere to specific guidelines, with internal reports submitted to the Governing Board within three months of each financial year's end. The guidelines also set weightage and minimum criteria for the independent external evaluation of the performance of Statutory Committees of MIIs.

On similar lines, the Central Vigilance Commission restructured the advisory board for banking and financial frauds (**Advisory Board**). Pursuant to this change, all public sector banks and financial institutions are required to redirect all issues of fraud, amounting to INR 50 crore, to the Advisory Board, before the commencement of any criminal investigation(s) or action under Section 17A of the Prevention of Corruption Act, 1988 (**PCA**).[8] Additionally, the Ministry of Personnel, Public Grievance and Pensions has issued Standard Operating Procedures in accordance with Section 17A of the PCA, requiring compulsory approval before any investigation against any alleged corrupt public servant is conducted.[9]

Moreover, the Standing Committee on Finance recommended that the Serious Fraud Investigation Office (**SFIO**) be armed with "*sufficient teeth*" to exclusively probe and prosecute cases relating to complex corporate frauds that affect the economy and stakeholders. The President of India also approved the extension of tenures of Central Bureau of Investigation (**CBI**) and the Directorate of Enforcement (**ED**) directors from two to five years.[10] Lastly, by an August 2021 notice, the SEBI empaneled 16 entities, including Binder Dijker Otte India, Ernst & Young and Deloitte Touche Tohmatsu India, to conduct forensic audits of listed companies.[11]

The National Financial Regulating Authority has issued a circular on June 26, 2023[12], to clarify that the statutory auditors are under a mandatory obligation to report fraud or suspected fraud if they observe suspicious activities, transactions or operating circumstances in a company that indicate "reasons to believe" that an offence of fraud is being or has been committed against the company by its officers or employees.

---

[7] Circular on '(1) Parameters for external evaluation of Performance of Statutory Committees of Market Infrastructure Institutions(MIIs);and (2) Mechanism for internal evaluation of Performance of MIIs and its Statutory Committees' published by the SEBI, (Jan 30, 2025), available at: SEBI | Parameters for external evaluation of Performance of Statutory Committees of Market Infrastructure Institutions (MIIs); and Mechanism for internal evaluation of Performance of MIIs and its Statutory Committees

[8] Prevention of Corruption Act, 1988, Section 17A

[9] Standard Operating Procedure for cases under Section 17A of the Prevention of Money Laundering Act, Ministry of Personal, Public Grievances and Pensions, (September 3, 2021), available at: SOP-Processing-under-Section-17A-of-Preservation-of-Corruption-Act3pX4G.pdf

[10] Sandeep Phukan, *CBI, ED chiefs can now have five-year terms*, THE HINDU (November 14, 2021), available at: CBI, ED chiefs can now have five-year terms - The Hindu

[11] *SEBI Empanels 16 Entities to Conduct Forensic Audit*, ECONOMIC TIMES (August 24, 2021), available at: Sebi empanels 16 entities to conduct forensic audit - The Economic Times

[12] Statutory Auditors' responsibilities in relation to Fraud in a Company published by National Financial Regulatory Authority (June 26, 2023), available at: NFRA circular on Statutory Auditors' responsibilities in relation to Fraud in a Company | National Financial Reporting Authority | India

Furthermore, on July 15, 2024, the Reserve Bank of India issued the Master Direction on Fraud Risk Management in Banks, superseding the directions issued in 2016.[13] It aims to provide a robust framework that will enable early detection, and timely reporting of fraud in regulated entities. Notably, the framework on early warning signs and red flagging of accounts have been strengthened for timely detection, which will include reporting to various law enforcement agencies and supervisors.

2. Recent Judicial Decisions

a. Anti-Corruption:

The Hon'ble Supreme Court in its landmark decision of *Neeraj Dutta v. State (Govt of NCT Delhi)*,[14] settled the debate on whether the demand and acceptance of illegal gratification by a public servant can be proved by circumstantial evidence when direct evidence is unavailable due to the death of the complainant or his or her failure to support the prosecution case. In the *Neeraj Dutta case*, the Constitution Bench held that if evidence shows a demand, payment, or acceptance of a bribe, and the fundamental circumstances are proven, then a legal presumption arises that the bribe was illicit, unless it is successfully challenged. Accordingly, then this presumption, under Section 20 of PCA, holds and it implies that the bribe was given as a "motivation or reward" for official actions or inaction. In this particular case, circumstantial evidence was used to establish the grant of illegal gratification.

In 2025, the Hon'ble Supreme Court in *Dileepbhai Nanubhai Sanghani v. State of Gujarat*[15], while referring to *Neeraj Dutta*, clarified and set clear limits on corruption prosecutions, stating that simple policy violations or administrative errors leading to financial losses are not enough. Bribery evidence is essential for PCA charges. The court reiterated that policy mistakes, without personal financial gain, cannot be criminalised. Additionally, the legal presumption of corruption under Section 20 of the PCA is only valid if proof of demanding and receiving an undue advantage exists.

Moreover, in *Arvind Kejriwal v. CBI*,[16] when the issue concerning grant of bail in PCA-related offence involving a state chief minister arose, the Hon'ble Supreme Court granted regular bail to Mr. Kejriwal, subject to conditions tied to the initial ED case relating to the Delhi Liquor Excise Policy 2021–22 that was framed to

[13] Master Directions on Fraud Risk Management in Commercial Banks (including Regional Rural Banks) and All India Financial Institutions, RBI (Jul 15, 2024), available at: Reserve Bank of India - Master Directions
[14] *Neeraj Dutta v. State (Govt, of NCT, Delhi)*, Criminal Appeal 1592 of 2022
[15] *Dileepbhai Nanubhai Sanghani v. State of Gujarat*, 2025 INSC 280
[16] *Arvind Kejriwal v. CBI*, 2024 SCC OnLine SC 2550

financially benefit his party's election campaign in Goa. The Court recognised the conflict between the PCA's two-year trial target and the reality of complex corruption and money laundering cases, which often exceed that time frame. While upholding the right to a speedy trial under Article 21, the Court emphasised that prolonged pre-trial detention, even in serious cases, is unacceptable. This highlights the ongoing efforts of the Judiciary to balance the demands of justice with individual liberty. Section 17A of PCA stipulates a mandatory requirement wherein police officers are legally required to get permission from the competent authority before investigating any alleged crime by a public servant. This is only necessary when the alleged crime is connected to decisions or recommendations made by the public servant while performing their official duties. The provision was incorporated by an amendment with effect from July 26, 2018.

In *Nara Chandrababu Naidu v State of Andhra Pradesh*,[17] the Hon'ble Supreme Court delivered a split verdict regarding the applicability of Section 17A to inquiries initiated after the provision was incorporated into the PCA. Although the Supreme Court confirmed the prospective nature of Section 17A, there's no consensus on its exact implementation. The point of contention is whether the requirement for prior approval applies when an investigation starts or when the alleged crime happened. This crucial issue remains unresolved by the Supreme Court, and High Courts across the country have issued varying opinions on how Section 17A should be applied.

[17] *Nara Chandrababu Naidu v. State of Andhra Pradesh*, 2024, SCC OnLine SC 47

Furthermore, in a ruling against former Chief Minister Siddaramaiah, the Karnataka High Court upheld the Governor's authority to grant sanction for corruption investigations under Section 17A of the PCA. The court clarified that complainants can directly petition the Governor for this approval and that, in special circumstances, the Governor can act independently of the Council of Ministers. The court also made a distinction between the pre-investigation approval under Section 17A and the post-investigation prosecution sanction required by the Bharatiya Nagarik Suraksha Sanhita, 2023 (**BNSS**) and Section 19 of the PCA[18].

b. Anti-Money Laundering

In the landmark case of V*ijay Madanlal Choudhary and Ors. v. Union of India and Ors*,[19] the Hon'ble Supreme Court upheld the constitutionality of several sections of the Prevention of Money Laundering Act, 2002 (**PMLA**), including Sections 5, 17, 8(4), and 50. The three-judge bench of the Hon'ble Supreme Court held that the ED could provisionally attach property or conduct searches under Sections 5 and 17 without a prior complaint or report concerning a predicate offence, as long as reasons were recorded in writing that the accused possessed "proceeds of crime."

The Hon'ble Supreme Court also upheld Section 50, allowing the ED to summon and record statements during investigations, stating that it did not violate Articles 20(3) and 21 of the Constitution since such summons were not for prosecution. However, if statements were recorded post-arrest, the protection under Article 20(3) against testimonial compulsion would apply. The Court emphasised adequate safeguards in the PMLA, including the potential prosecution of vexatious ED actions under Section 62, ensuring fairness and transparency in investigations. Additionally, under Section 50, the ED can summon and compel an accused to make admissible statements under penal threats.

The law laid down by the Hon'ble Supreme Court in *Vijay Madanlal* has been propounded by various other judgments of the apex court, most notably in *Pankaj Bansal v. Union of India*.[20] The Pankaj Bansal judgment addressed the safeguards available under the PMLA against an arrest made by the ED, and directed the ED to provide the arrested person with "written grounds of arrest" while exercising its powers to arrest under Section 19 of the Act. Under the PMLA, Section 19 empowers authorised officials of ED to arrest persons based on the material in their possession, providing a reasonable basis to suspect that an individual has

[18] *Shri Siddaramaiah v. State of Karnataka and Others,* WP No 22356 of 2024
[19] *Vijay Madanlal Choudhary and Others v. Union of India and Others,* Special Leave Petition (Criminal) No. 4634 OF 2014
[20] *Pankaj Bansal vs. Union of India,* 2023 SCC Online SC 1200

committed an offence punishable under the law. The Hon'ble Supreme Court examined whether the arrest and detention of the appellants under the PMLA complied with the due process standards as the appellants had alleged procedural irregularities and violation of their rights and pleaded that their arrest and remand orders be set aside. While addressing the issue of the appellants' arrest on the basis of allegations against related entities and associated public servants, the court opined that in the absence of a written justification for the arrest, mere non-cooperation of a witness in response to the summons issued under Section 50 of the PMLA would not be enough to render them liable to ED arrest. The court upheld the principle of liberty and due process, and directed that the appellants, if not required to appear in any other case, be released immediately. The court ruled that it was of utmost importance to uphold an individual's fundamental rights and ensure ways to safeguard such rights. The judgment highlights the court's cognizance in acknowledging grave flaws in the actions of the authorities, leading to such unlawful detention. The Division Bench of Hon'ble Supreme Court, through its judgment, declared that the ED's arrest of the appellants was illegal, emphasising that a suspect's refusal to answer questions is not sufficient grounds for arrest under Section 19 of the PMLA. The court reinforced the constitutional rights of the appellants, under Article 22(1), to be informed of the grounds of arrest. It further explained that the ED's power to arrest under Section 19 of the PMLA is limited to situations where they have "reasons to believe" the suspect has committed a PMLA offence.

To ensure the protection of both the accused's rights and the integrity of the legal process, the Supreme Court ruled that grounds of arrest must be communicated in writing. This requirement aims to eliminate ambiguity and guarantees compliance, thus ensuring that constitutional and statutory protections are in place. The court also provided a mechanism to redact such information from the written grounds and furnish the edited copy of the grounds of arrest to the detained person to safeguard the sanctity of the investigation. The principle set forth in *Pankaj Bansal* has been upheld by a subsequent ruling in *Prabir Purkayastha v. State*.[21]

c. Criminal Procedure

The Hon'ble Supreme Court in the latest judgement of *G.C. Manjunath & Others v. Seetaram*[22], discussed the extents of statutory protection granted to public servants, under Section 197 of the Code of Criminal Procedure (**CrPC**). Section 197 of

[21] *Prabir Purkayastha v. State*, 2024 INSC 414
[22] *G.C. Manjunath v. Seetaram*, 2025 SCC Online SC 718

the CrPC ensures that public servants are protected from being prosecuted for acts alleged committed in an effort to discharge their official duties by requiring prior sanction from competent authority. The case involved police officers who were accused of having acted in excess of their official duties which included assault and wrongful confinement of the complainant. A private complaint was lodged against the police officers as a result of which the trial court issued summons against them. Aggrieved, the police officers approached the High Court, seeking to get the summoning order, issued by the trial court, against them, quashed. The High Court dismissed the application which led the police officers to approach the Supreme Court in appeal. The Apex Court set aside the High Court order justifying the summons issued against the appellants and laid emphasis on the fact that even for excessive acts which includes custodial torture during investigations will fall under the ambit of protection if there is a 'reasonable nexus' for the acts committed. It was essential to determine if the actions were connected to the duty assigned and not if they were lawful.

The Hon'ble Supreme Court addressed the scrutiny of sanctions issued under PCA in *State of Punjab v. Hari Kesh*,[23] which originated from a First Information Report (**FIR**) being registered against a public servant for offences under Sections 7[24] and 13(2)[25] of the PCA. The case involved corruption charges against a public servant wherein he had used his official position to secure personal gains. Initially, the Nagar Council i.e., the competent authority, denied sanction, but it was later granted by an Executive Officer of the Nagar Council, who was not authorised to grant such sanction, in the absence of any new evidence. The accused challenged this second sanction in the Punjab & Haryana High Court, citing previous Supreme Court rulings in *Manoranjan Prasad Choudhary v. State of Bihar*[26] and *State of H.P. v. Nishant Sareen*.[27]. The Hon'ble High Court set aside the impugned Sanction Order and the proceedings arising therefrom, even when the trial had already commenced, and the prosecution had examined seven witnesses.

Upon appeal to the Hon'ble Supreme Court, it reinstated the proceedings before the Special Court in Sangrur, and dealt with the question of law as to whether a High Court can halt an already commenced corruption trial midway, wherein the prosecution had already presented its case. The Apex Court also looked into whether the impugned sanction order was in alignment with Section 19 of the PCA. It was held that the validity of the sanction order should be assessed as part of the trial, as it is an evidentiary issue. The Hon'ble Supreme Court opined that

[23] *State of Punjab v. Hari Kesh*, 2025 SCC OnLine SC 49
[24] Prevention of Corruption Act, 1988, Section 7
[25] Prevention of Corruption Act, 1988, Section 13(2)
[26] *Manoranjan Prasad Choudhary v. State of Bihar,* (2002) 10 SCC 688
[27] *State of H.P. v. Nishant Sareen,* (2010) 14 SCC 527

invalidating the sanction order without proving a "failure of justice" would breach Section 19(3) of the PCA, and such order can only be set aside if it is shown that an irregularity in the sanction order leads to a failure of justice. In this case, however, the High Court neither observed nor demonstrated how the sanction order resulted in a failure of justice. Therefore, the impugned sanction order was reinstated by the Court and the proceedings that had been initiated as a result of it.

In *State of Punjab v. Partap Singh Verka*,[28] the Hon'ble Supreme Court dealt with a situation wherein during the pendency of trial, the Special Court summoned a doctor, who was a public servant, after the prosecution filed an application to add him as an accused to the case, based on the complainant's testimony alleging that the doctor had demanded and received a bribe. While upholding the decision passed by the High Court of Punjab & Haryana setting aside the order issuing summons, the Supreme Court held that courts cannot take cognizance of offences under the PCA against a public servant, even under Section 319 of the CrPC, without first fulfilling the mandatory requirements of Section 19 of the PCA as the entire procedure becomes legally flawed and invalid. The Hon'ble Supreme Court opined that the language of Section 19(1) of the PCA clarifies that obtaining prior sanction from the appropriate Government is a mandatory prerequisite, which ought to be followed before filing the application under Section 319 of the CrPC.

In *G. Krishnegowda v. Karnataka*,[29] the Hon'ble Karnataka High Court held that offences under the PCA can be invoked against both the public servant and against a person who by virtue of his office discharges public duty. The Hon'ble Karnataka High Court dismissed a petition to quash an FIR filed under the PCA against the petitioner, who was a project manager in a society registered under the Karnataka Societies Registration Act, 1960.

The Hon'ble Delhi High Court in *Ravina and Associates Pvt. Ltd. v. CBI*,[30] held that while imposing fines under the PCA, courts must provide due consideration to the value of the property obtained through the crime committed. The Hon'ble Court decided on whether the whole of the frozen amount should be considered as proceeds of crime and be liable for confiscation upon conviction. It held that any amount attached under criminal proceedings like the PCA can be confiscated only up to the extent of amount that is actually involved in the criminal proceeding.

In *CBI v. Thommandru Hannah Vijayalakshmi*,[31] the Hon'ble Supreme Court held that the CBI need not conduct preliminary enquiry before filing FIRs in corruption

[28] *State of Punjab v. Partap Singh Verka* 2024 SCC OnLine SC 1659
[29] *G. Krishnegowda v. Karnataka* Crl.P.No.2801 of 2021
[30] *Ravina and Associates Pvt. Ltd. v. CBI*, 2021 SCC OnLine Del 4249
[31] *CBI v. Thommandru Hannah Vijayalakshmi*, 2021 SCC OnLine SC 923

cases. This appeal came from a Telangana High Court order, which quashed an FIR in a disproportionate asset case, where it held that the CBI should have conducted a preliminary enquiry before it registered an FIR, as required by the Central Bureau of Investigation (Crime) Manual of 2005. The Hon'ble Supreme Court set aside the Telangana High Court's judgement and held that the FIR will not be vitiated just because the CBI did not conduct preliminary enquiry. The accused cannot seek a preliminary enquiry as a right.

3. Investigations

Investigation is a process that involves examination, search, study, or inquiry into the fundamentals of various factors to arrive at an understanding of the facts unknown, to be able to establish the veracity of the issue. Investigations can be bifurcated into internal and external. Internal investigation by a company usually begins upon receiving a complaint either from its employees or an outsider. The objective is to ascertain whether any alleged violation of the law, rules, regulations, or internal company policy has occurred. Often times, accountancy and legal firms are engaged to prepare comprehensive reports on these investigations. Internal investigations permit the company to clean up its affairs, redeem its image, show its dedication towards compliance, and protect it from any governmental repercussions.[32]

When governmental agencies probe such breaches of the law and to unearth cases of bribery, money laundering, corruption, fraud, etc., it is termed as external investigation. External investigations tend to bring the company under the radar of such agencies that enact stringent measures against them. Raids are conducted by investigative bodies such as the CBI, the ED, the SFIO, etc., which play a crucial role in exposing scandals.

4. Best Practices in Internal Investigations

Generally, no one method is followed for carrying out internal investigations. The companies are provided the leeway to choose practices that are best suited to their organisational structure. Despite the freedom to adopt any system as it deems fit and proper, often times, companies have universally agreed upon certain best practices. Across the board, these practices are both accepted and implemented for the smooth conduct of internal investigations.

[32] Bruce E Yannett and David Sarratt, *Beginning an Internal Investigation: The US Perspective*, GLOBAL INVESTIGATION REVIEW (January 4, 2023), available at: 20190125_beginning_an_internal_investigation_us_perspective_chapters.pdf

a. Role of the External Counsel

External counsels play a crucial role in investigations as they demonstrate specialised expertise, having knowledge of substantive legal issues and essential business procedures of the company. They are likely to be more objective. They also appear to be more objective to third parties and the government. This is necessary to maintain the integrity of the investigation.[33] During an investigation, external counsels may assist in various aspects like reconstructing the sequence of past events that led to the alleged wrongdoing, collecting and reviewing documents, preparing an investigation plan, conducting interviews, and presenting the findings of the investigation in the form of an investigation report. They are involved in managing the interests of board members and employees, while fulfilling and balancing their duties towards the client company. Moreover, to preserve information confidentiality, communicated between the company and the legal counsel, client-attorney privilege is important. India has taken a stringent stance on privileged professional communication between clients and attorneys, which is protected by virtue of Sections 132 to 134 of the Bharatiya Sakshya Adhiniyam, 2023 (previously enumerated in Sections 126 to 129 of the Indian Evidence Act, 1872)[34]. However, this protection does not extend to in-house counsels.

Therefore, an inside counsel must not be engaged in investigations since parts or whole of the process may be exempt from attorney-client privilege and work product protection.[35] Further, they may not be equipped with requisite skills of research and document review. Lastly, the independence and objectivity of an inside counsel may be compromised if the subjects are his or her superiors or colleagues. However, an inside counsel provides the necessary company knowledge and can act as a link between the external counsel and the company.[36]

b. Point of Contact

As a general standard for ensuring smooth functioning, a company employee, who acts as a neutral point of contact for the entirety of the investigation, is present in the room during the interviews or investigative proceedings. For ensuring smooth functioning, the presence of a neutral point of contact is essential. This person

---

[33] Miller & Chevalier, *How Can Outside Counsel Sidestep Ethical Pitfalls in Internal Investigations of Antitrust Wrongdoing?, CORPORATE COMPLIANCE INSIGHTS (June 8, 2022)*, available at: How Can Outside Counsel Sidestep Ethical Pitfalls in Internal Investigations of Antitrust Wrongdoing? | Miller & Chevalier

[34] Bharatiya Sakshya Adhiniyam, 2023, Section 132; Bharatiya Sakshya Adhiniyam, 2023, Section 133; Bharatiya Sakshya Adhiniyam, 2023, Section 134

[35] Payel Chatterjee and Sahil Kanuga, *Internal investigations: There is no escaping anymore!*, INTERNATIONAL BAR ASSOCIATION (September 1, 2022), available at: Internal investigations: There is no escaping anymore! | International Bar Association ·CBI v. Thommandru Hannah Vijayalakshmi, 2021 SCC OnLine SC 923

[36] *Id.*

undertakes various fundamental tasks such as maintaining the confidentiality of ongoing investigations, engaging and coordinating with the counsels, sharing documents and relevant information, and informing the independent director as well as the concerned management of the progress of the investigation. The point of contact is briefed about the developments in the investigations and is present mainly to take any critical business decisions arising out of the investigation process. Such a person should not be implicated for his or her conduct during the course of the investigation.[37]

c. Disclosures

There are a variety of laws that a corporate entity must comply with. These include the provisions relating to internal controls and audits in the Companies Act, 2013 (**Companies Act**), and the SEBI LODR, among others. Under the Companies Act, though companies are not expressly required to report bribery, fraud and corruption, but if a fraud (discovered) exceeds a set monetary threshold, then auditors of the company are required to notify the central government of the fraud.[38] Moreover, any fraud committed by the company or on the company must be disclosed in the auditor's report as per the Companies (Auditor's Report) Order, 2020.[39] Similarly, the SEBI LODR, requires listed companies to disclose to stock exchanges, the initiation of any forensic audit, the name of the entity initiating the audit, the reasons for the same and the final forensic audit report.[40] Furthermore, a person may also be punished for failing to report the commission of certain offences by another entity or the intention to do so under the BNSS.[41]

[37] *Guide to Conducting Workplace Investigations*, CORPORATE COMPLIANCE (2008), available at: Workplace Investigations Guide | PDF | Witness | Regulatory Compliance.
[38] Companies Act 2013, Section 143(12)
[39] Companies (Auditor's Report) Order, 2020, available at: Orders_25022020.pdf
[40] Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) (Third Amendment) Regulations, SEBI, (October 8, 2020), available at: SEBI | Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) (Third Amendment) Regulations, 2020
[41] Bharatiya Nagarik Suraksha Sanhita, 2023, Section 33

However, it must also be noted that an internal investigation and its findings are matters of confidentiality and, therefore, the overall process must be conducted with discretion. The fact of an internal investigation may be communicated to the employees under the directions of the company. Moreover, the interviewees should also be issued Upjohn Warnings before the commencement of the interviews. This notice informs a company's employee that the attorney, whether in-house or outside counsel, represents only the company and not the individual employee. Pursuant to this, the company has the option to forego the aforementioned privilege and give the interviewee's information to any governmental body, law enforcement agency, or third party.[42]

d. Collection and Retention of Information

Information such as the companies' financial statement, business records, observations of statutory audit, employees' personal data, etc., is collected and retained for a successful investigation. A review of all these documents is crucial and may be stored across multiple locations in such formats as emails, text messages, network devices (physical devices that permit the computer hardware to communicate and interact with one another), internet backup tapes and so on.[43] However, collection of information involves data privacy concerns. Data privacy comes under the purview of the Information Technology Act, 2000 (**IT Act**). In addition, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data and Information) Rules, 2011, which currently regulates the transmission of personal data, will be repealed by the Digital Personal Data Protection Act (**DPDP Act**) which was enacted in August 11, 2023. Under the DPDP Act, the data principals can request summary report detailing the processing method applied to their personal data. However, this excludes data shared with authorised entities for lawful purposes like crime prevention or investigation.

Broadly, the companies are required to: (i) ensure that there is legitimate reason to collect and use sensitive personal data or information; (ii) provide adequate privacy notice to the affected employees; (iii) obtain prior consent from the affected employees'; and (iv) maintain reasonable measures to protect the security

[41] Bharatiya Nagarik Suraksha Sanhita, 2023, Section 33
[42] Sherbir Panag, Tanya Gaunguly & Lavanyaa Chopra, *The Practitioner's Guide to Global Investigations: India*, GLOBAL INVESTIGATIONS REVIEW, (February 8, 2021), available at: 21_04_19_Global_Investigations_Review.pdf
[43] Robert Keeling, Chapter 18 – Corporate Internal Investigations, in THE GENERAL COUNSEL'S GUIDE TO GOVERNMENT INVESTIGATIONS, (2nd ed., 2018)

and confidentiality of such data.[44] Violation of the prescribed security practices and procedures is punishable under Sections 43A and 72A of the IT Act.[45]

e. Interviewing Witnesses

Witnesses may be segregated into the following three categories:

i. Implicated Witnesses

Implicated witnesses are responsible for civil or criminal liability under both *respondeat superior* as well as personal liability. When interviewing, the counsel must clearly state that he represents the organisation and not the employee. Confidentiality of the information provided must be maintained by both the employee and the organisation. However, the organisation might waive attorney-client privilege and disclose the information obtained if it becomes necessary.

ii. Implementing Witnesses

Liability can arise due to *respondeat superior*, where a violative act has been committed under the direction of a superior, without personal liability. The witness is typically not hostile to the organisation. The counsel should nevertheless inform the witness that the purpose of the interview is to form legal advice for the organisation.

iii. Mere Witness Employee

They expose the company to no liability at all and have merely heard about the breach or the investigation. They are primarily interviewed to know the subject matter of the investigation.

f. Whistleblowing Mechanisms

A whistleblowing system is for identifying and fighting maladministration. It is the foundation of successful risk management. Potential whistle-blowers can inform of such maladministration through a fully internal system, without exposing the company to unwanted disrepute.[46]

Employee feedback is an effective way of detecting compliance violations. Information of potential threats that are safely and anonymously communicated

[44] Srijoy Das, Siddharth Seshan and Disha Mohanty, *India-A Guide to Conducting Internal Investigations in India*, GLOBAL INVESTIGATIONS REVIEW, (March 4, 2016), India - A Guide To Conducting Internal Investigations In India - Global Investigations Review

[45] Information Technology Act, 2001, Section 43A, Information Technology Act, 2001, Section 72A

[46] Moritz Hozman, *What is a whistleblowing system?* (FAQ), INTEGRITY LINE (Oct. 24, 2022), available at: FAQ: What Is a Whistleblowing System?

help reduce financial damage to companies caused by compliance issues. This is confirmed by the study "Whistleblowing Report 2019" where more than half of the feedback received *via* internal whistleblowing systems uncovered compliance-related abuses and misconduct.[47]

Although telephone hotlines exist, they neither ensure nor guarantee complete anonymity. Digital software like whistleblowing mechanisms offer complete anonymity and security to the whistle-blower and help maintain the internal track of communication with the company.[48]

g. ESG Investigations

In this day and age, Environmental, Social and Governance (**ESG**) investigations are of paramount importance. It has both internal and external triggers like mergers and acquisitions, whistleblowing, audit reports, etc.

The ESG investigations requires a comprehensive focus on both hard and soft law frameworks. Hard law has substantially evolved in response to the growing ESG considerations. Soft law and other frameworks, such as the guidelines by Organisation for Economic Co-operation and Development and the United Nations Environment Programme for multinational enterprises,[49] plays an important role

[47] Christian Hauser, Nadine Hergovits and Helene Blumer, *Whistleblowing Report 2019*, EQS (2019), available at: WhistleblowingReport2019_EN-002.pdf.
[48] *Id.*
[49] *A legal framework for the integration of environmental, social and governance issues into institutional investment*, UNITED NATIONS ENVIRONMENT PROGRAMME (October 2005), available at: A legal framework for the integration of environmental, social and governance issues into institutional investment : October 2005

in ESG practices adopted by companies. Other frameworks include contractual commitments, voluntary public commitments and industry's own standards and targets. Engagement with special risk consultants and Non-Government Organisation experts and reports, crisis and media strategy are of absolute relevance. In 2012, the SEBI made it mandatory for the top 100 listed companies by market capitalisation to include the Business Responsibility Report as part of their annual report so that they could describe the initiatives taken from an ESG perspective.[50] Enhanced mandatory sustainability reporting came into effect in April 2022 (for large listed companies). Disclosures are required to be made as per the National Guidelines for Responsible Business Conduct.

In 2023, the SEBI introduced new regulations to enhance ESG reporting for the top 1,000 listed companies, focusing on the Business Responsibility and Sustainability Report format.[51] This format requires disclosure of key performance indicators across nine ESG areas, including environmental footprints, employee well-being, and diversity. The SEBI also introduced a phased approach to require "reasonable assurance" of these disclosures, ensuring the accuracy and reliability of the ESG disclosures.

When lawyers in India conduct investigations into ESG matters, they must carefully navigate a dynamic and multifaceted regulatory environment that includes statutory obligations, disclosure mandates, and mechanisms for enforcement. The following outlines a methodical approach suited to India's present circumstances, which lawyers could implement to comply with all ESG guidelines and laws:

- Carry out comprehensive research into relevant ESG-related laws, rules, and guidelines, covering the Companies Act, SEBI standards, environmental legislation, and specific ESG requirements in particular sectors. It is also important to clarify the extent of directors' responsibilities and what must be disclosed under these regulations.[52]
- Examine the company's ESG-related disclosures, including its BRSR reports, sustainability documentation, and any official announcements concerning ESG matters. Assess whether these disclosures meet regulatory standards and accurately represent the company's real-world practices.[53]

[50] Securities and Exchange Board of India Notification, (September 2, 2015), available at: SEBI | Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015 [Last amended on October 23, 2023]
[51] Circular on 'BRSR Core – Framework for Assurance and ESG disclosures for value chain' published by SEBI, (July 12, 2023), available at: SEBI | BRSR Core - Framework for assurance and ESG disclosures for value chain
[52] Christine Cuthbert *et al.*, *Is Your Business Aligned with India's ESG Wave?*, Baker McKenzie (October 15, 2024), available at: Is Your Business Aligned with India's ESG Wave? | Insight | Baker McKenzie
[53] *Indian Legal Regime for ESG*, S&R Associates (June 14, 2022), available at: Indian Legal Regime for ESG – Legal Developments

- Assess the company's governance frameworks, including the board's supervision of ESG issues and the internal mechanisms for managing ESG risks. Determine whether these governance structures are in line with legal requirements and recognised best practices.[54]
- Assess the company's adherence to relevant environmental rules, labor statutes, and human rights guidelines along with its engagement in social responsibility programs. Identify deficiencies or vulnerabilities that could expose the organisation to legal consequences or harm its reputation.[55]
- Analyse whether any ESG-related decisions or omissions could constitute breaches of directors' duties or regulatory violations. Consider the possibility of shareholder actions or regulatory enforcement based on ESG failures.[56]

5. Way Forward

The scope of white-collar crimes is expanding with the increasing use of technology. Accordingly, there have been parallel developments in the trends and modifications in law to combat these issues. A forward-looking approach would be to view internal investigations favourably since they ensure a balance between disclosures and reporting. Fraudulent activities and misconduct are brought to the attention of the authorities before they can escalate. Artificial intelligence and predictive analysis are emerging trends that can be potentially used to assist in investigations. Forensic data analytics can play a role in monitoring, investigating and decrementing frauds, non-compliance, and misconduct. To nab offenders, professionals are likely to develop and implement mechanisms that prioritise governance, compliance, ethics, industry standards, and greater cooperation with the agencies. Further incorporation of best industry practices into the Indian setup would help overcome the loopholes in the existing framework.

[54] The role of the legal department in shaping the ESG strategy, Wolters Kluwer, available at: The role of the legal department in shaping the ESG strategy | Wolters Kluwer
[55] Umakanth Varottil, *The Legal and Regulatory Impetus towards ESG in India: Developments and Challenges*, NUS Law (January 2023), available at: 03_UmakanthVarottil.pdf
[56] *Id.*

B

Emerging Powers of Investigating Agencies in India

1. Introduction

The process of investigation of offences, often involving multitude of steps such as collection and examination of evidence, recording of witness statement, etc., is one of the foremost and critical functions of law enforcement. According to Section 2(l) of the Bharatiya Nagarik Suraksha Sanhita, 2023 (**BNSS**) (previously, Section 2(h) of the Code of the Criminal Procedure, 1973 (**CrPC**)), investigation comprises any proceeding carried out by the police or any magistrate-authorised official (other than a magistrate), such as visiting the crime scene, making arrests, etc., required for collecting evidences. To determine if any legal violations have taken place, the government and other relevant authorities employ the investigative apparatus to detect such infractions. The BNSS has introduced procedural reforms, including enhanced reliance on digital evidence, electronic summons, and video conferencing for witness statements, aimed at streamlining investigations.

Law enforcement agencies conduct investigations on matters ranging from corruption, bank frauds and money laundering to murders, forgery, terrorism and riots. Besides state and local level law enforcement, India has specialised investigating agencies like the Directorate of Enforcement, the Central Bureau of Investigation, the Serious Fraud Investigation Office, the Directorate of Revenue Intelligence, the Income Tax Department and the Competition Commission of India. These investigating agencies have the power to conduct search and seizure, arrest, summon, and document production under various laws that are briefly discussed in this Chapter.

2. Directorate of Enforcement (ED)

The ED is a multi-disciplinary organisation mandated with the investigation of offences related to money laundering and violations of foreign exchange laws.[1] The

[1] *Directorate of Enforcement*, GOVERNMENT OF INDIA (2023), available at: https://enforcementdirectorate.gov.in/

agency was established as an "Enforcement Unit" in 1956 within the Department of Economic Affairs of the Ministry of Finance, and subsequently in 1957, it was renamed as "Directorate of Enforcement". The ED primarily deals with the implementation of Foreign Exchange Management Act, 1999 (**FEMA**), and the Prevention of Money Laundering Act, 2002 (**PMLA**), which has undergone significant amendments in recent years. These amendments have strengthened the ED's investigative powers to cover not only third-party property attachments and corporate liabilities, but also enabled juridical expansion to include cases involving digital assets and financial intermediaries, thereby increasing its role in combating illicit financial flows. The principal powers of ED include looking into allegations of money laundering, conducting search and seizure of properties, undertaking investigative actions ancillary to its objective such as attachment of properties and assets, and prosecution of money laundering and related illegal activities. The agency has led some of the renowned investigations in recent years, including the INX Media case, the alleged scam in West Bengal school recruitment, the National Herald case,[2] and the BRD Group case.[3] Additionally, the ED has intensified its scrutiny over cryptocurrency transactions, offshore investments, and politically exposed persons (**PEPs**), reflecting global enforcement trends and Financial Action Task Force (**FATF**) recommendations.

Under FEMA, the Central Government has authorised the ED to investigate any person or company suspected of transgressing the law or rules and regulations made pursuant to FEMA. Recent amendments have broadened the ED's authority over cross-border transactions, shell entities, and beneficial ownership structures. Under Section 13 of FEMA, the ED examines violations and has the authority to compound offences committed by an accused.[4] Section 37 of FEMA gives the Director and Assistant Director of the ED the authority to investigate any violation and contravention of FEMA,[5] and these officers while investigating under the said section have the same powers as those granted to Income Tax authorities under the Income Tax Act, 1961 (**ITA**).[6] Therefore, regarding discovery, inspection, evidence collection and production thereof, examination, issuing commissions, etc., the ED has the same powers as a Civil Court under the Code of Civil Procedure, 1908 (**CPC**).[7] The ED's authority to conduct search and seizure, and also summon under Section 37(3) of FEMA has been upheld by the Hon'ble Delhi High Court in *Suman Sehgal v. Union of India*.[8]

[2] *Id.*
[3] ED *files charge sheet against BRD Group, its chairman and 5 others*, ZEE BUSINESS (November 23 2022), available at: ED files chargesheet against BRD Group, its chairman and 5 others | Zee Business
[4] Foreign Exchange Management Act, 1999, Section 13
[5] Foreign Exchange Management Act, 1999, Section 37
[6] Foreign Exchange Management Act, 1999, Section 37(3)
[7] Income Tax Act, 1961, Section 131
[8] 2006 SCC OnLine Del 429

Under the PMLA, the ED is responsible for investigating and attaching assets acquired through the proceeds of crime and subsequently institute necessary steps to confiscate such proceeds.[9] These steps are conducted in response to the proceeds of crime obtained from the Scheduled Offenses mentioned under the PMLA. Additionally, the ED is empowered to undertake steps to recover the proceeds of crime held outside India. Section 5 and 8(4) of the PMLA empowers the ED with wide discretionary powers to attach the property of the accused.[10] The ED also assists foreign law enforcement agencies in undertaking investigations into money laundering and evidence collection.

Section 17 of the PMLA empowers the ED to enter, search and seize the suspected property without judicial permission.[11] The ED has the authority to undertake search and seizure against any individual based on information in the officer's possession and by establishing in writing the exact reasons to suspect that money-laundering has occurred. The powers of search and seizure under Section 17 of PMLA *inter alia* include: (a) entering and searching any building, place, vessel, vehicle or aircraft where the ED has reasons to suspect that relevant records or proceeds of crime are kept; (b) breaking open the lock of any door, box, locker, safe almirah or other receptacle where the keys thereof are not available; (c) seizing any record or property found as a result of such search; (d) make an inventory of such properties; and (e) examine on oath any person who is found to be in possession or control of any record or property. Although Section 17 grants substantial powers to the ED, it also incorporates a mechanism for judicial oversight. The Adjudicating Authority, as defined under the PMLA, must review the circumstances surrounding the seizure, ensuring that due process is followed.

[9] *Directorate of Enforcement, GOVERNMENT OF INDIA (2023)*, available at: https://enforcementdirectorate.gov.in/
[10] Prevention of Money Laundering Act, 2002, Section 5, 8(4)
[11] Prevention of Money Laundering Act, 2002, Section 17

The ED is also empowered to arrest any person for offences punishable under the PMLA; and the manner in which the arrest can be affected is postulated under Section 19 of the Act.[12] Moreover, under Section 50of PMLA, the ED has the same power as a Civil Court under CPC such as discovery, inspection, evidence production, issuing summons, examining witnesses, and issuing commissions.[13] The Hon'ble Supreme Court in *Vijay Madanlal Choudhary v. Union of India*,[14] upheld ED's wide powers to make arrest, carry out search and seizure operations and issue summons to any person as constitutional and noted that these provisions do not suffer from the vice of arbitrariness. However, the Hon'ble Supreme Court has agreed to review certain aspects of its decision, including concerns over not providing a copy of Enforcement Case Information Report i.e., the ECIR, to the accused and placing the burden on the accused to demonstrate their innocence to secure bail, effectively reversing the standard burden of proof.

The case of *Arvind Kejriwal v. Directorate of Enforcement*[15] examines the validity of arrest by the ED for alleged corruption and money laundering in the Delhi Liquor Policy scam of 2022. The ED contended that Kejriwal was the "kingpin" of the scam, accusing him of colluding to favour certain private entities. Mr. Kejriwal challenged the legality of his arrest, arguing that the ED lacked sufficient material and that his arrest, a week into the Model Code of Conduct, suggested a political motive. The Division Bench of the Hon'ble Supreme Court held that arrests under the PMLA are subject to judicial scrutiny to ensure the conditions for arrest under Section 19 of the PMLA are met. While the court found that the ED had presented sufficient "reasons to believe" that Mr. Kejriwal was guilty, particularly regarding the alleged use of proceeds of crime in the Goa elections, it referred the question of whether the necessity and justification for arrest constitute a distinct ground for challenge to a larger bench. Therefore, Mr. Kejriwal was granted interim bail until the validity of his arrest was determined by the larger bench with certain conditions imposed, including restrictions on visiting the Chief Minister's office, signing official files, commenting on the case, and interacting with witnesses. Notably, Mr. Kejriwal was later arrested by the CBI in connection with the same excise policy case, despite the interim bail.

Furthermore, The Hon'ble Supreme Court had also granted bail to the erstwhile Deputy Chief Minister of Delhi, Mr. Manish Sisodia, who was arrested by the CBI in February 2023, and by the ED in March 2023, for his alleged involvement in the Delhi liquor policy scam. The bail petitions of Mr. Sisodia were initially rejected by

[12] Prevention of Money Laundering Act, 2002, Section 19
[13] Prevention of Money Laundering Act, 2002, Section 50
[14] *Vijay Madanlal Choudhary v. Union of India*, 2022 SCC OnLine SC 929
[15] *Arvind Kejriwal v. Directorate of Enforcement*, Criminal Appeal 2493 of 2024

the Hon'ble Delhi High Court, and subsequently by the Hon'ble Supreme Court on October 30, 2023. However, the Hon'ble Supreme Court stressed upon the prolonged incarceration and the importance of the right to a speedy trial, opining that the trial must be concluded within six to eight months. As the trial did not commence even after a significant period, Mr. Sisodia filed further bail applications that were concurrently rejected by the Trial Court and the Hon'ble Delhi High Court.

Ultimately, on August 09, 2024, the Division Bench of the Hon'ble Supreme Court in *Manish Sisodia v. Directorate of Enforcement*[16] granted bail to Mr. Sisodia, explicitly stating that the continued incarceration of around seventeen months without the trial having begun, deprived him of his right to a speedy trial with evidence running into 69,000 pages and 493 witnesses still pending examination, the Hon'ble Supreme Court cited the excessive delay in the trial's start as the main justification for granting bail.

The Hon'ble Supreme Court also dismissed the argument that Mr. Sisodia himself caused delays by filing numerous applications for documents, noting that only a limited number of applications were filed, and the accused has a right to inspect relevant documents for a fair trial. The directions for his release on bail included furnishing bail bonds, surrendering his passport, reporting to the Investigating Officer regularly, and not attempting to influence witnesses or tamper with evidence.

3. Central Bureau of Investigation (CBI)

The CBI is the premier police investigative agency in India, which was set up by the Government of India by a resolution dated April 01, 1963.[17] Additionally, it is the nodal police organisation that undertakes inquiries on behalf of Interpol Member nations. The legal powers of CBI are derived from the Delhi Special Police Establishment Act, 1946 (**DSPE Act**). Under the DSPE Act, the CBI is authorised to only investigate offences in Union Territories,[18] however, the Central Government can extend the agency's jurisdiction to other areas, including States and Railways.[19] As per Section 6 of the DSPE Act, the CBI cannot initiate investigations in a State without the concerned State Government's consent. Over the years, several State Governments have withdrawn their general consent, requiring the CBI to seek approval on a case-by-case basis.[20] The Hon'ble Supreme Court has upheld the right of States to withhold consent, significantly impacting CBI's ability to investigate crimes outside

[16] *Manish Sisodia v Directorate of Enforcement*, SLP (Crl) 8781 of 2024
[17] Central Bureau of Investigation, GOVERNMENT OF INDIA (2023), available at: Central Bureau of Investigation
[18] Delhi Special Police Establishment Act, 1946, Section 2
[19] Delhi Special Police Establishment Act, 1946, Section 5
[20] Delhi Special Police Establishment Act, 1946, Section 6

Union Territories. As per Section 2(2) of the DSPE Act, the CBI has all the powers, duties, privileges, and liabilities that police officers have in connection with the investigation of offences committed.

The Hon'ble Supreme Court in *State of West Bengal v. Union of India*[22] ruled that the suit filed by the State of West Bengal contesting the CBI's registration of *suo moto* cases within its territory following the withdrawal of the State's consent under Section 6 of the DSPE Act, 1946[23] was maintainable. The West Bengal government requested the Hon'ble Supreme Court to declare the CBI's action as unconstitutional and sought to restrain the agency from registering and/or investigating cases in the state without prior consent. The Division Bench of the Hon'ble Supreme Court held the suit to be maintainable, emphasising that when considering preliminary objections, only the averments in the plaint are to be examined to determine if a cause of action exists. The Apex Court noted West Bengal's argument that Entry 80, List I of the Constitution of India ensures the Union does not encroach upon the state's jurisdiction without its permission, and thus the CBI's actions, drawing power from the DSPE Act, violated constitutional provisions and the DSPE Act itself.

The Hon'ble Supreme Court further highlighted that Section 6 of the DSPE Act necessitates the State's consent for extending CBI jurisdiction as a component of federalism. Furthermore, the Apex Court underscored that the establishment, exercise

[21] Delhi Special Police Establishment Act, 1946, Section 2(2)
[22] *State of West Bengal v. Union of India*, 2024 SCC Online SC 1684
[23] Delhi Special Police Establishment Act, 1946, Section 6

of powers, extension of jurisdiction, and superintendence of the DSPE Act all vest with the Central Government. While acknowledging the CBI's independent authority in investigating specific cases, the court affirmed that the administrative control and superintendence of the DSPE Act lie with the Union.

The procedure for conducting investigations by the CBI is majorly governed by the procedural law i.e., the BNSS. Additionally, detailed guidelines on CBI investigation is provided in the CBI (Crime) Manual, Government of India (2005).[24] The CBI's power to arrest is derived from Section 35 of BNSS (previously, Section 41 of CrPC), pursuant to which the CBI may arrest an individual, for any cognizable offence notified under Section 3 of the DSPE Act, against whom a reasonable suspicion exists of being involved in a crime, without any arrest warrant issued by a competent court.[25]

As per Section 94 of BNSS (previously, Section 91 of CrPC), if the Investigating Officer (i.e., the CBI) considers the procurement of any particular document or thing as absolutely necessary for the purpose of an investigation, it may issue a written order to the person who might have possession of such document.[26] If the document cannot be procured through such means for any legitimate reason, then documents can be procured through the process of search and seizure.

Under Section 96 of BNSS (previously, Section 93 of CrPC), the CBI has the power to conduct searches after obtaining warrants for the search, whereas under Section 185 of BNSS (previously, Section 165 of CrPC), the CBI has the power to conduct search without the issuance of a warrant.[27] Section 185 of BNSS provides that if the document(s) or thing(s) required for investigation is likely to be found at a place and the Investigating Officer has reason to believe that such document or thing cannot otherwise be obtained without undue delay, such officer may, after recording in writing the grounds for his belief and specifying in such writing so far as possible the document(s) or thing(s) for which search is to be made, conduct a search of a place or dwelling for such document or thing.[28] Copies of any record made under Section 185(1) or 185(3) shall forthwith be sent to the nearest Magistrate or Special Judge empowered to take cognizance of the offence.[29]

Section 106 of BNSS (previously, Section 102 of CrPC) provides power to the CBI to seize any property, which may be alleged, or suspected to have been stolen, or which may be found under circumstances that create suspicion of the commission of any offence.[30] The Investigating Officer, who seizes any such property, is required to report

[24] Central Bureau of Investigation (Crime) Manual, (2005)
[25] Bharatiya Nagarik Suraksha Sanhita, 2023, Section 35
[26] Bharatiya Nagarik Suraksha Sanhita, 2023, Section 94
[27] Bharatiya Nagarik Suraksha Sanhita, 2023, Section 185
[28] Bharatiya Nagarik Suraksha Sanhita, 2023, Section 185
[29] Bharatiya Nagarik Suraksha Sanhita, 2023, Section 185(5)
[30] Bharatiya Nagarik Suraksha Sanhita, 2023, Section 106

the seizure to the Magistrate having jurisdiction.[31] Moreover, the CBI may, by order, require any person to appear before it.[32] The CBI is also empowered to interrogate witnesses (orally) under Section 180 and 181 of the BNSS (previously, Section 161 and 162 of the CrPC), respectively.[33]

4. Serious Fraud Investigation Office (SFIO)

The SFIO is a multi-disciplinary organisation under the Ministry of Corporate Affairs, comprising experts in the field of accountancy, forensic auditing, law, information technology, investigation, company law, capital markets and taxation. It is tasked with the detection, investigation and prosecution of white-collar crimes.[34] The concept of establishing such a body was first given by the Naresh Chandra Committee in 2002, which recommended the creation of a "Corporate Serious Fraud Office" to track down corporate fraud and oversee prosecutions under various economic legislations. In response to this recommendation, the SFIO was established in July 2003. Subsequently, the SFIO was granted statutory force through Section 211 of the Companies Act, 2013 ("Companies Act"), pursuant to which the Government of India established SFIO by way of Notification No. S.O.2005(E), dated July 21, 2005.[35]

Under Section 212 of the Companies Act, the SFIO is assigned to investigate into the affairs of the company when the Government deems such investigation is necessary. The government opinion to undertake such an investigation in based on the following grounds:

a. on receipt of a report of the Registrar or inspector under Section 208 of the Companies Act;

b. on intimation of a special resolution passed by a company that its affairs are required to be investigated;

c. in public interest; or

d. on request from any department of the Central Government or State Government.[36]

The SFIO has the sole power to undertake investigations allotted to it under the Companies Act, barring other Central or State Government agencies authorised to investigate such cases, and if any such investigation has already been initiated, it shall not be continued, and the concerned agency shall transfer the pertinent

[31] Bharatiya Nagarik Suraksha Sanhita, 2023, Section 106(3)
[32] Bharatiya Nagarik Suraksha Sanhita, 2023, Section 179
[33] Bharatiya Nagarik Suraksha Sanhita, 2023, Section 180; Bharatiya Nagarik Suraksha Sanhita, 2023, Section 181
[34] Serious Fraud Investigation Office, GOVERNMENT OF INDIA (2023), available at: Serious Fraud Investigation Office
[35] Serious Fraud Investigation Office, GOVERNMENT OF INDIA (2023), available at: https://sfio.gov.in/en/
[36] *Id*; Companies Act, 2013, Section 212

documents and records to the SFIO.[37] The SFIO conducts the investigation in the manner and procedure provided under Chapter XIV of the Companies Act.[38] The Investigating Officer, to whom the Director of SFIO assigns the task of investigating the affairs of the company, shall have the powers of an Inspector under Section 217.[39] The Investigating Officer may, with prior approval of the Central Government, also conduct investigations into the conduct of related companies, if the officer considers the results of such investigation relevant to the investigation of the affairs of the company for which he is appointed.[40] The company under investigation along with its officers and employees, who are or have been in employment of the company, shall be responsible for providing all information, explanation, documents and assistance to the Investigating Officer as he may require for the conduct of the investigation.[41]

Section 212(8) of the Companies Act, read with the Companies (Arrests in Connection with Investigation by Serious Fraud Investigation Office) Rules, 2017, confers the SFIO with the power to arrest if it has reasons to believe that the person is guilty of any offence punishable under the Sections referred to in Section 212(6).[42] Such reasons should be recorded in writing by the Investigating Officer.[43] Provisions in relation to arrest under the BNSS applies mutatis mutandis to arrests made by the SFIO.[44] Moreover, if the Investigating Officer has reasons to believe that the books and papers of, or relating to, any company or other body corporate or managing director or manager of such company are likely to be destroyed, mutilated, altered, falsified or secreted, he may seize the books and papers as he considers necessary for the purposes of his investigation.[45] The Central Government may prosecute a person based on the SFIO report that has found the person guilty of criminal offence.[46]

5. Income Tax Authorities

The ITA is an act to levy, administrate, collect & recover Income-tax in India. It came into force on April 01, 1962.[47] For the proper implementation of the ITA and to monitor the ethical operation of the Income Tax Department, the government has established many Income Tax Authorities. Income Tax Authorities exercise their powers and perform their functions to keep a check on harassment of assesses, tax-evasion, and prevent unnecessary discrimination while collection of tax.

[37] Companies Act, 2013, Section 212(2)
[38] Companies Act, 2013, Section 212(3)
[39] Companies Act, 2013, Section 212(4)
[40] Companies Act, 2013, Section 219
[41] Companies Act, 2013, Section 212(5)
[42] Companies Act, 2013, Section 212(8)
[43] *Id.*
[44] Companies (Arrests in Connection with Investigation by Serious Fraud Investigation Office) Rules, 2017, Rule 9
[45] Companies Act, 2013, Section 220(1)
[46] Companies Act, 2013, Section 224
[47] *Income Tax Department, History of Taxation Pre- 1922*, GOVERNMENT OF INDIA (2023), available at: History of Direct Taxation

The government constituted various Income Tax Authorities, which are: (1) The Central Board of Direct Taxes (**CBDT**) constituted under the Central Boards of Revenue Act, 1963; (2) Principal Chief Commissioners of Income-tax or Chief Commissioners of Income-tax; (3) Directors of Income-tax or Commissioners of Income-tax or Commissioners of Income-tax (Appeals); (4) Additional Directors of Income-tax or Additional Commissioners of Income-tax or Additional Commissioners of Income-tax (Appeals); (5) Joint Directors of Income-tax or Joint Commissioners of Income-tax; (6) Deputy Directors of Income-tax or Deputy Commissioners of Income-tax or Deputy Commissioners of Income-tax (Appeals); (7) Assistant Directors of Income-tax or Assistant Commissioners of Income-tax; (8) Income-tax Officers; (9) Tax Recovery Officers; and (10) Inspectors of Income-tax.[48]

Income Tax Authority officers have the same powers as a Civil Court under CPC for investigations regarding discovery, evidence production, summons, and issuing commissions.[49] These authorities may also impound and retain in its custody, for such a period as it deems fit, any books of account or other documents after recording the reasons for doing so. In case the period of retention exceeds fifteen days, then the said authorities must obtain approval of the Commissioner.[50] The Union Budget 2023 introduced a significant amendment, extending the time limit for retaining books and documents seized during a search from fifteen days to thirty days, provided the reasons are duly recorded and approved.

Section 132 of the ITA empowers certain authorities to carry out search and seizure. These authorities may enter and search any building or place where they have reasons to believe relevant books of account or other documents, money, bullion, jewellery or other valuables are kept, and examine them.[51] They have the permission to break open locks of doors, boxes, lockers, safes, almirahs or other receptacles if keys thereof are not available during search.[52] The authorities also have the power to seize these things or place marks of identification thereon or make extracts or copies therefrom.[53] The authorised officer may, during the course of the search or seizure, examine on oath any person who is found to be in possession of the valuables mentioned above.[54] The Union Budget 2023 introduced a new provision allowing the authorised officer to requisition digital data directly from cloud storage services, enabling access to encrypted financial records for effective tax enforcement.

[48] Income Tax Act, 1961, Section 116
[49] Income Tax Act, 1961, Section 131(1)
[50] Income Tax Act, 1961, Section 131(3)
[51] Income Tax Act, 1961, Section 132
[52] *Id.*
[53] *Id.*
[54] Income Tax Act, 1961, Section 132(4)

6. Competition Commission of India (CCI)

The Competition Act, 2002 (**Competition Act**) is based on the philosophy of modern competition laws. The Competition Act forbids anti-competitive agreements, corporate abuse of dominant positions and regulates combinations (acquisition, acquiring of control and M&A) that have or are likely to have a materially negative impact on competition in India.[55] The Central Government has established the CCI with effect from October 14, 2003, for the purposes of achieving the objectives of the Competition Act.[56] The CCI is entrusted with the responsibility of eliminating practices having adverse impact on competition, fostering and maintaining competition, safeguarding the interests of consumers and ensuring trade freedom in the Indian market.[57]

The Director General (**DG**) acts as the investigative arm of the CCI and assists in investigating anti-competitive business practices of enterprises. The Competition (Amendment) Act, 2023 introduced key changes, including a deal value threshold for merger notifications i.e., INR 2,000 crore, an expanded definition of "control" to include material influence, a framework for settlements and commitments, and penalties based on global turnover.

Any person aggrieved by an enterprise's anti-competitive actions may submit information to the CCI and request an investigation.[58] If the CCI finds a prima facie case based on the submitted information, it can, basis the authority bestowed on it under Section 26(1) of the Competition Act, direct the DG to conduct an investigation

[55] *Competition Commission of India*, GOVERNMENT OF INDIA (2023), available at: Competition Commission of India, Government of India
[56] *Id.*
[57] *Id.*
[58] Competition Act, 2002, Section 19

into the same.[59] The DG is then required to submit a report of his findings within such period as may be specified by the CCI.[60] The DG has all the powers as are conferred upon the CCI under Section 36(2) of the Competition Act i.e., the DG has been given the same power as a Civil Court under CPC to perform such acts as discovery and production of evidence, summons, examining on oath, receiving evidence on affidavit, and issuing commissions.[61] Furthermore, Section 41(3) of the Competition Act states that the DG has powers equivalent to that of an Inspector as given under Section 240A of the Companies Act, 1956,[62] which empowers the DG to carry out search and seizure with the authorisation of the Magistrate.[63] Recent CCI investigations have targeted alleged anti-competitive practices in e-commerce, fast-delivery platforms, and digital markets, with notable fines imposed on Meta over WhatsApp's data-sharing policy and regulatory conditions placed on the Disney-Reliance merger to address competition concerns.

The Hon'ble Supreme Court in *Excel Crop Care Ltd. v. Competition Commission of India*,[64] has clarified that the purpose behind a DG investigation is to look into anti-competitive activities and as part of that goal, the DG must take into consideration all relevant facts and evidence. The Hon'ble Supreme Court stated that if, during the course of an investigation, other related facts pertaining to the case are brought to light, the DG would be well within its powers to bring them to the forefront in its report. However, the starting point of the inquiry would be the allegations, which are contained in the information.

7. Customs Officers

Customs Duty is a duty or tax charged on goods imported into India or exported outside India. The fundamental law for levy and collection of customs duties in India is the Customs Act, 1962 (**Customs Act**). It was formulated to prevent the illegal import and export of goods. Customs officers are empowered to exercise various powers specifically relating to collection of custom duties and prevention of smuggling for the enforcement of Customs Act.[65]

Under Section 100 of the Customs Act, a customs officer has the authority to search any individual entering or leaving India if there is a reasonable belief that the

[59] Competition Act, 2002, Section 26(1)
[60] Competition Act, 2002, Section 26(3)6
[61] Competition Act, 2002, Section 41(2), 36(2)
[62] Competition Act, 2002, Section 41(3)
[63] Companies Act, 1956, Section 240A
[64] *Excel Crop Care Ltd. v. Competition Commission of India*, (2017) 8 SCC 47
[65] Customs Act, 1962, Section 5

individual has concealed facts about himself and possesses goods or any related documents liable for confiscation.[66] If any goods liable to confiscation is secreted inside the body of the suspected person, the customs officer may detain such person and promptly produce him before the nearest magistrate.[67] In cases involving gold, diamonds, manufacture of gold and diamonds, watches, etc., the customs officer, having been empowered by general or special order, may search any suspected person.[68] They also have the power to summon individuals to give evidence and produce documents.[69] Such empowered customs officer has the power to arrest any person in India or within Indian customs water if there are reasons to believe that the person has committed certain offences punishable under the Customs Act.[70] Every person arrested shall, without unnecessary delay, be taken to a magistrate.[71] Additionally, the customs officer, on authorisation from the required authority, may search premises suspected of hiding goods liable to be confiscated, or any documents or things which will be useful for any proceeding under the Customs Act.[72] The power of customs officers related to seizure of goods, documents and things is derived from Section 110 of the Customs Act, pursuant to which he is empowered to seize any goods believed to be liable for confiscation under the Customs Act.[73]

8. Conclusion

India has used the above stated investigating agencies over the years to fight fraud, corruption, money-laundering, scams, and other problems, to safeguard the nation's safety and integrity. However, often the powers of these agencies are limited and restricted due to factors such as politics, bureaucracy, frequent challenges to the powers of the investigating agencies under various Acts, etc., that lead to inefficient working and getting embroiled in external corruption. On the other hand, expansion of the scope of such powers with no checks and balances in place results in conferring unfettered powers to the investigation agencies, which can go against public interest. Therefore, neither of these extreme scenarios are desirable; instead, India needs a balance in the investigating agencies' powers to enable better functioning, unbiased investigation and the advancement of national welfare without favouring any individual or institution in particular.

[66] Customs Act, 1962, Section 100
[67] Customs Act, 1962, Section 103(1)
[68] Customs Act, 1962, Section 101
[69] Customs Act, 1962, Section 108
[70] Customs Act, 1962, Section 104(1)
[71] Customs Act, 1962, Section 104(2)
[72] Customs Act, 1962, Section 105(1)
[73] Customs Act, 1962, Section 110(1)

C

Anti-Regulations & The Indian Online Gaming Industry

1. Introduction

Online gaming has gained popularity, especially in the wake of the Covid-19 pandemic, leading to online casinos, virtual reality games, fantasy sports and electronic sports (**e-sports**) taking over the traditional gaming industry. The online gaming industry majorly consists of two types of games – game of skill and game of chance.

Games of skill can be divided into categories such as e-sports (i.e. online video games played in an organised way between professional players, such as FIFA), fantasy sports (i.e., games for choosing a team of real sports players from different teams and winning points according to how well the players perform in real life, such as Dream11), and casual online gaming. Games of chance are *inter alia* casino games, bingo, and lottery. As per a joint report prepared by Interactive Entertainment, Innovative Council and WinZO Games, the Indian online gaming industry is poised for magnificent growth, with the market size expanding to more than INR 750 billion by 2029.[1] Against the backdrop of technological advancements in the gaming sector, the Ministry of Electronics and Information Technology (**MeitY**) established a seven-member high-level Inter-Ministerial Task Force (**IMTF** or the **Panel**) to develop guidelines for national-level legislation to regulate online gaming and to chart rules and regulations for the online gaming sector in May 2022.[2] The IMTF included Niti Ayog's CEO and secretaries of home affairs, revenue, industries & internal trade, electronics & IT, information & broadcasting, and sports.[3] The Panel examined issues faced by the online gaming industry, scrutinised global best practices surrounding legal and legislative frameworks, and advocated introducing a comprehensive and uniform regulatory regime for a transparent and safe online gaming environment.

The IMTF's report to the Prime Minister's Office raised several concerns around the regulations of online gaming in India.[4] The Report highlighted the need for a new

[1] ET GOVERNMENT, *WinZO-IEIC report predicts $60 bn market, 2 mn jobs, $26 bn IPO boom for India's gaming industry*, available at: Indian Online Gaming Industry: WinZO-IEIC report predicts $60 bn market, 2 mn jobs, $26 bn IPO boom for India's gaming industry, ET Government (indiatimes.com)
[2] TIMES OF INDIA, *Government Forms Inter-ministerial Panel to Regulate Online Gaming*, available at: Govt forms inter-ministerial panel to regulate online gaming - Times of India (indiatimes.com)
[3] *Id.*
[4] HINDUSTAN TIMES, *Inter-ministerial Panel Proposes Central Law to Govern Online Gaming*, available at: Interministerial panel proposes central law to govern online gaming | Latest News India - Hindustan Times

legislation that not only covers the full spectrum of technology and internet-based gaming, but also provide coverage for extraterritorial jurisdictions, which were absent in the Public Gambling Act 1867 (**PG Act**).[5] The Report proposed the establishment of a central regulatory body for the industry, distinguishing between the games of skill and chance, and placing online gaming under the purview of the Prevention of Money Laundering Act of 2002 (**PMLA**).[6] This chapter focusses on the intersection of online gaming and anti-money laundering laws in India against the backdrop of the proposed new central legislation on online gaming.

2. Money Laundering in Online Games

The massive growth of online gaming industry in India has drawn both users and investors alike. It has also led to a surge in criminal activities, specifically the money-laundering activities that can be carried out by misusing gaming platforms.

Often, virtual currencies are used to launder money through online games.[7] While playing such games, players are offered the choice to buy in-app virtual items through fiat currency to enhance their gaming experience or advance in the game. The in-game purchases, such as weapons or equipment, may carry real-life monetary value. These can appreciate and be sold to other players, which can then be exchanged back into fiat currency. This creates an unregulated market that can be easily exploited,[8] since the in-game items can be purchased or traded with money obtained illegally, such as through stolen credit cards, account hacking or phishing, or by a maze of exchange-based transactions between characters in multiplayer online role-playing games.[9] These activities are difficult to monitor in the absence of proper regulations, and they often facilitate undetected cross-border financial activity. This enables money laundering through the transfer of the virtual in-game items in *lieu* of real money and allows illicit financial activity to be buried in a heap of legitimate transactions.[10]

The IMTF adequately recognises this and recommends that an online gaming platform must not allow or facilitate transactions through unauthorised payment systems, nor should it encourage or facilitate any money laundering activities,

[5] *Id.*
[6] INDIAN EXPRESS, *The Online Gaming Market in India and the Proposed Rules to Regulate it*, available at: The online gaming market in India, and proposed rules to regulate it | Explained News,The Indian Express.
[7] Jay B. Sykes & Nicole Vanatko, *'Virtual Currencies and Money Laundering: Legal Background, Enforcement Actions, And Legislative Proposals'* R45664 Congressional Research Service 1 (2019)
[8] Shane Kelly, *'Money Laundering Through Virtual Worlds of Video Games: Recommendations For A New Approach To AML Regulation'* 71 Syracuse Law Review 1487 (2021)
[9] *Id.*
[10] THE HINDU BUSINESS LINE,*Online Gaming Yes, Money Laundering No*, available at: Online gaming yes, money laundering no - The Hindu BusinessLine

financing of terrorism activities or transactions in violation of the Foreign Exchange Management Act, 1999 (**FEMA**)[11]

3. Inconsistency in Gambling Legislation in India

The antiquated PG Act does not address the challenges posed by the technological advancements in gaming and gambling, which includes online gaming and digital casinos. It is imperative to frame a new legislation to address the loopholes.

Even at the state level, there is an inadequacy in dealing with online gaming and gambling. While gambling and betting, and taxation arising as a result, are state subjects as provided in the Constitution of India, no uniform law governs the same.[12] The IMTF Report has found that the lack of a uniform regulatory approach towards online gaming among states is a cause for concern.[13] States like Sikkim, Nagaland, and Meghalaya[14] have drafted specific laws to regulate public gambling in their jurisdictions and are the only states in India that have specific laws to govern online gaming. However, states like Delhi, Madhya Pradesh, and Uttar Pradesh have largely adopted the PG Act, which prohibits games of chance but allows games of skill.[15] At

[11] HINDUSTAN TIMES, Inter-ministerial Panel Proposes Central Law to Govern Online Gaming, available at: Interministerial panel proposes central law to govern online gaming | Latest News India - Hindustan Times
[12] Constitution of India 1950, Schedule VII, List II, item 34
[13] HINDUSTAN TIMES, *Inter-ministerial Panel Proposes Central Law to Govern Online Gaming*, available at: Interministerial panel proposes central law to govern online gaming | Latest News India - Hindustan Times.
[14] NORTHEAST TIMES, *Meghalaya Becomes the Third Northeastern State to Legalize Online Gaming, Gambling*, available at: Meghalaya Becomes Third Northeastern State To Legalize Online Gaming, Gambling (northeasttoday.in)
[15] THE QUINT, Explained: *Which Indian States Have Banned Online Gaming and Why*, available at: https://www.thequint.com/explain- ers/india-law-gambling-online-gaming-betting-state-ban-illegal-legal#read-more#read-more

the other end of the spectrum, some states like Karnataka, Andhra Pradesh, Kerala, and Tamil Nadu had earlier sought to prohibit both games of skill and games of chance.[16] While Karnataka attempted to ban all online gambling in 2021, the High Court declared much of the law unconstitutional in 2022. The state's appeal to the Supreme Court is now pending, leaving the legal status of online gambling uncertain.[17]

As per recent developments, Karnataka is preparing to create a new regulatory framework that would prohibit online gambling while allowing skill-based games to operate within the state. This action mirrors the regulations implemented by Chhattisgarh, which has been effective since March 2023. This move comes as India's gaming sector rapidly grows, necessitating clearer legal guidelines. The state aims to resolve previous legal challenges and foster industry growth while protecting consumers.[18]

On February 07, 2025, the Governor of Tamil Nadu approved regulations aimed at real-money online games, prohibiting minors from participating in real-money online games, making Know Your Customer (**KYC**) and Aadhaar verification mandatory.[19] The state also set up the Tamil Nadu Online Gaming Authority (**TNOGA**) to implement the regulations. Some states like Rajasthan are still in the process of framing their gambling laws, especially with respect to fantasy sports and e-sports.[20]

Furthermore, the variation in the understanding of "game of skill" and "game of chance" across states may differ, creating further inconsistencies. High courts have also taken different legal positions in different states for the same games. The Gujarat High Court held poker to be a game of chance and, hence, illegal,[21] whereas the Calcutta High Court declared it to be a game of skill and, hence, legal.[22]

With respect to fantasy gaming, several Indian High Courts, including Punjab & Haryana, Bombay, and Rajasthan, have classified the fantasy sports format popularised by Dream11 as a game of skill, shielding it from state gambling prohibitions and validating it as a constitutionally protected business. The Hon'ble Supreme Court, in *Avinash Mehrotra v. State of Rajasthan*,[23] reinforced this, stating

[16] The Tamil Nadu Prohibition of Online Gambling and Regulation of Online Games Ordinance, 2022; Karnataka Police (Amendment) Act 2021

[17] *Junglee Games India Private Limited v. State of Tamil Nadu*, SCC OnLine Mad 2762; *All India Gaming Federation of India v. State of Karnataka*, WP 18703/2021

[18] Tech Story, *Karnataka to Introduce New Law Banning Online Gambling, Allowing Skill-Based Games*, available at: Karnataka to Introduce New Law Banning Online Gambling, Allowing Skill-Based Games – TechStory

[19] CNBCTV18, *TN Law On Online Gambling: Why India Needs A Centralised Regulatory Framework — A Top Law Firm's Perspective*, available at: TN law on online gambling: Why India needs a centralised regulatory framework — a top law firm's perspective - CNBC TV18

[20] HINDU BUSINESS LINE, *Rajasthan draft law could put online skill gaming industry in disarray*, available at: Rajasthan draft law could put online skill gaming industry in disarray - The Hindu BusinessLine.

[21] *Dominance Games Pvt. Ltd. v. State of Gujarat*, 2017 SCC Online Guj 1838

[22] *Indian Poker Association v. State of West Bengal*, WPA No. 394 of 2019 (Cal HC)

[23] *Avinash Mehrotra v. The State of Rajasthan & Ors.*, SLP (C) No. 18478/2020

the legality of fantasy sports is well-established due to repeated dismissals of challenges. However, the Supreme Court also acknowledged a pending appeal from a Bombay High Court decision in *Gurdeep Singh Sachar v. Union of India & Ors.*,[24] which remains at a preliminary stage.

Therefore, as it can be seen, the regulatory framework across states varies substantially, which leads to gaming app developers resorting to "geo-fencing", a mechanism by which their games are available in some states, but unavailable in others. This is dangerous as the access to such games can be easily illegally obtained in states where the regulatory framework is stricter, defeating the purpose of the prohibitions. Furthermore, state laws alone cannot authorise State Governments to block offshore betting or gambling websites due to lack of extra-territorial jurisdiction,[25] but require a central legislation to tackle offshore illegal gambling sites.[26]

Foreign-based online gaming platforms more often than not are used for facilitating illegal international money transfers. To address this, India is pushing for these companies to be subject to PMLA and the Countering the Financing of Terrorism framework.[27]

In April 2023, MeitY introduced new regulations for online gaming by amending the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (**IT Rules, 2021**). These "Online Gaming Rules" establish a system where self-regulatory bodies (**SRBs**), recognised by MeitY, will approve real-money online games before they can be offered to the public, based on set criteria. Online gaming platforms are now classified as "online gaming intermediaries" (**OGIs**) and must adhere to specific due diligence requirements. Games are considered "permissible" if they do not involve real money or if a recognised SRB has verified a real-money game.[28]

4. Key Takeaways from the 2023 Amendments to the IT Rules, 2021

The purpose of the amendments to the IT Rules, 2021, was to mitigate risks to online game players and impose a stricter regulatory structure on the industry.

[24] *Gurdeep Singh Sachar v. Union of India* (2019) 75 GST 258
[25] TIMES OF INDIA, *Curbing Offshore Online Betting and Gambling*, available at: Curbing offshore online betting and gambling
[26] *Id.*
[27] Business Standard, *India Seeks FATF Oversight For Online Gaming To Curb Money Laundering Risks*, available at: India seeks FATF oversight for online gaming to curb money laundering risks | News - Business Standard
[28] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2023, Ministry of Electronics and Information Technology, April 6, 2023, https://www.meity.gov.in/content/gazette-notification-vide-gsr-275e-dated-642023-regarding-amendments-it-intermediary

Nevertheless, significant issues have been brought to light, necessitating official action. The amendments essentially fall short of regulatory fairness and the following observations have been made in that regard:

a. The definitions vide the amendments made to the IT Rules 2021 introduce significant ambiguity. Rule 2(qa) defining an "online game" as "*a game that is offered on the Internet and is accessible by a user through a computer resource or an intermediary*" and Rule 2(qd) defining an "*online real-money game*" as "*an online game where a user makes a deposit in cash or kind with the expectation of earning winnings on that deposit*" fails to address the grey area of free-to-play games that incorporate in-app purchases, blurring the distinction between free and paid experiences. Moreover, Rule 2(qd)'s inclusion of non-monetary exchanges in "deposits" and "winnings" expands the regulatory scope to games without real money, leaving unclear how "in kind" transactions should be regulated.

b. The new amendment's definition of online gaming intermediaries, in Rule 2(qb), contrasts with the traditional definition of intermediaries as passive conduits of third-party content as provided in the Information Technology Act, 2000 (**IT Act**). Online gaming platforms, however, operate more like publishers, fostering direct and interactive relationships between players and the platform. This departure from the typical intermediary role means they cannot rely on the "safe harbour" provisions of Section 79(1) of the IT Act, potentially creating liability issues that could undermine developer and publisher confidence.

c. The amendments to the IT Rules 2021 are deficient in directly regulating data collection by gaming platforms, which, as intermediaries, handle user data. While Section 72A of the IT Act provides some protection against unlawful information disclosure, its efficacy in safeguarding minors and preventing personal data sales is uncertain. International precedents and frameworks like Health Insurance Portability and Accountability Act (**HIPAA**) in the United States and General Data Protection Regulation (**GDPR**) in Europe, underscore the necessity for explicit data protection provisions. To align with international best practices, the amended IT Rules should have incorporated a dedicated section for data protection than relying on the general provisions of Section 72A of the IT Act.

d. The amended IT Rules require OGIs to perform due diligence and register with SRBs. While regulatory bodies like the All-India Gaming Federation (**AIGF**) and the Federation of Indian Fantasy Sports (**FIFS**) have established charters, they lack uniformity. Positive steps in this aspect could be to include added website information and mandatory personnel appointments. However, strict RBI-mandated KYC requirements, including Aadhaar and digital signatures, may impede user onboarding and industry growth. These KYC norms as provided under Rule 4(11)(b)

of the amended IT Rules 2021 do not fully address issues like gambling addiction or inclusivity, and disproportionate penalties could harm platforms.

e. Due to existing legal gaps, e-sports could be wrongly classified as online games, negatively impacting both gamers and the industry. The ambiguity surrounding prize-based e-sports, which incentivise purchases but aren't gambling, creates regulatory uncertainty. This lack of clarity could impede the industry's growth, as companies become hesitant to offer promotional incentives. In contrast, many global jurisdictions have established separate legal frameworks tailored to e-sports. A tailored KYC strategy is recommended for the online gaming industry to mitigate its unique challenges. This would involve applying strict KYC protocols to high-value financial activities and streamlined checks for low-value ones.

f. The amendments to India's IT Rules 2021 seek to regulate the rapidly expanding online gaming sector, aiming to protect players. However, they have generated concerns regarding consumer safety, privacy, and market competition. The stringent regulatory approach, which redefines gaming companies as intermediaries, may disproportionately affect market integrity. Given the consistent government scrutiny of digital marketplaces in India, including "over-the-top" (**OTT**) platforms and e-commerce platforms, new regulations for online gaming should be grounded in principle-based regulatory practices, ensuring fairness and adaptability.

5. Regulatory Licenses, Permits, Authorisations, or other Official Approvals

The necessity of licensing for online games in India is determined by both the type of game and its distribution. Certain types of games require licenses. While most state gaming laws exempt skill-based games, Nagaland and Sikkim mandate licenses for online skill games like poker, rummy, and fantasy sports.

In Tamil Nadu, under the implemented regulations, online game providers must obtain a "certificate of registration" from the TNOGA,[29] and skill games require verification from an SRB to operate online. With respect to social gaming, while free-to-play games are generally exempt from licensing across India, with OGIs only needing to conduct due diligence, Tamil Nadu mandates that all online game providers, even those offering free-to-play games, obtain a TNOGA registration. The TNOGA grants "certificates of registration" to local online game providers who

[29] *Why we are, Tamil Nadu Online Gaming Authority*, available at: Tamil Nadu Online Gaming Authority

adhere to the Tamil Nadu Prohibition of Online Gambling and Regulation of Online Games Act, 2022, its rules, and submit a complete application, particularly ensuring no prohibited games are offered. However, the TNOGA's decision is discretionary, and denied applicants have a right to a hearing.[30]

In Sikkim, obtaining a gaming license requires a three-stage payment process: an initial application fee, an additional fee for a 120-day provisional license following government inquiry, and a significant fee for a regular license after equipment setup.[31] With respect to recent amendments, Sikkim effectuated an amendment to the Sikkim Online Gaming (Regulation) (Amendment) Act in August 2024.[32] The amendment updated the definition of "gaming terminal" to explicitly include "internet gaming terminals" and Uniform Resource Locators (**URLs**) of the licensee, allowing licensed operators to offer online games to Sikkim residents via these platforms. However, strict geo-restriction to the state is mandated. The amendment also restates penalties for unlicensed operators, including asset seizure, and expands reporting capabilities to include third parties.[33]

In Nagaland, operators applying for a gaming license must submit a comprehensive application, including game details, financial records, and business plans, to the Finance Commissioner (Nagaland Authority), along with a non-refundable fee.[34] The application is then rigorously reviewed by empanelled firms (legal and financial experts) within 30 days, who provide certification or recommendations. The Nagaland

[30] ICLG, *Gambling Laws and Regulations India 2025*, (November 19, 2024), available at: https://iclg.com/practice-areas/gambling-laws-and-regulations/india
[31] Nishith Desai Associates, *Chambers Global Practice Guide, Gaming Law India, 2019*, available at: https://nishithdesai.com/Content/document/pdf/ResearchArticles/Chamber_Global_Practice_Guide_Gaming_Laws.pdf
[32] NORTHEAST LIVE, *Sikkim Amends Online Gaming Regulations Act to Curb Fraud, Protect Revenue*, (August 12, 2024), available at: Sikkim Amends Online Gaming Regulations Act to Curb Fraud, Protect Revenue
[33] Notification No. 11(656)L&PAD/2021/50, The Sikkim Online Gaming (Regulation) Amendment Ac, 2024, Law & Parliamentary Affairs Department, Gangtok, Government of Sikkim, dated August 27, 2024 available at: 414_20240925.pdf
[34] SBSB FINTECH LAWYERS, *Gambling License in India*, available at: Online Gambling license in India Gambling license in India from sb-sb.com

Authority may also refer the application to Ad Hoc or Expert Committees for further evaluation, with a two-week turnaround. Upon receiving certification from the empanelled firms, the Nagaland Authority issues the license within 14 days. Operators must obtain licenses to offer online skill games, which encompass diverse categories like fantasy sports, card games (poker, rummy), virtual stock/monopoly games, virtual adventure games, virtual combat games, puzzle games, etc. Licensing is restricted to Indian-incorporated entities with significant Indian ownership and operational control within India. Technology infrastructure, including servers, must also be located in India. Additionally, applicants must have clean criminal records and no association with any gambling operations.[35]

Although not a license, OGIs offering real-money games must obtain verification from an SRB to operate in India. OGIs must join a MeitY-registered SRB, comply with regulations, and submit game formats for review. However, no SRBs are currently registered, so the verification process remains undefined.[36]

6. Anti-Money Laundering Regulations in India

a. Prevention of Money Laundering Act

The PMLA and the rules issued thereunder (**PMLA Rules**) provide the key legislative framework for prosecution of offences and enforcement of anti-money laundering laws in India. The primary legal authority responsible for investigating and prosecuting money laundering offences under PMLA at the national level is the Directorate of Enforcement (**ED**), under the aegis of the Department of Revenue, Ministry of Finance.

The PMLA defines money laundering as any act where a person directly or indirectly attempts to indulge, or knowingly assists, or knowingly is a party, or is actually involved in any process or activity connected with the proceeds of crime, including its concealment, possession, acquisition, or use and projecting or claiming it as untainted property. Further, any property derived or obtained directly or indirectly, by any person as a result of a criminal activity relating to an offence specified in the schedule to PMLA, including the value of any such property or where such property is taken or held outside the country, then the property equivalent in value held within the country or abroad, amounts to proceeds of crime and hence, amounts to money laundering. Therefore, by the very nature of

[35] ICLG, *Gambling Laws and Regulations India 2025*, (November 19, 2024), available at: https://iclg.com/practice-areas/gambling-laws-and-regulations/india
[36] *Id.*

its definition, money laundering involves obtaining/deriving proceeds arising from commission of a criminal offence.

In May 2023, the Ministry of Finance widened the ambit of the term "*Reporting Entity*" under PMLA, as per Section 2(1)(wa) which now means "*a banking company, financial institution, intermediary or a person carrying on a designated business or profession*".[37] The compliance obligations for such entities mandate robust KYC procedures to verify the identities of their clients and beneficial owners. This process involves the use of valid identification methods, such as Aadhaar or Passport, to establish the authenticity of the individuals engaging in business relationships with these entities, to ensure accountability, and minimises the risk of financial crimes.

The PMLA lays down the broad framework for anti-money laundering (**AML**) compliance requirements applicable to Reporting Entities. Section 2(1)(sa) of PMLA defines "person carrying on designated business or profession" to include *"a person carrying on activities for playing games of chance for cash or kind, and includes such activities associated with casino."*

PMLA and PMLA Rules mandate reporting entities to undertake certain AML measures, including customer identification, enhanced client due diligence (**CDD**), customer acceptance, maintenance of records, and tracking and reporting of certain types of transactions.[38] Reporting Entities must ensure implementation of PMLA provisions, including operational instructions issued from time to time. Such entities are required to maintain records of prescribed transactions, such as cash transactions crossing INR 10 lakh, and "suspicious transactions", whether or not effected in cash.[39]

Additionally, reporting entities must conduct comprehensive CDD when establishing an account-based relationship. This entails the identification and verification of clients, as well as an understanding of the purpose and nature of the business relationship. Furthermore, each reporting entity is required to communicate to the authorised officer of the government the information of a Designated Director, a person designated by the reporting entity to ensure compliance with the obligations under Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (**PMLA Records Rules, 2005**), and the Principal Officer, an officer designated by the entity under PMLA Records Rules, 2005.

[37] Prevention of Money Laundering Act, 2002, Section 2(1)(wa)
[38] Prevention of Money Laundering Act, 2002, Section 12; Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, Rules 3,4,5,7 and 8
[39] Prevention of Money Laundering Act, 2002, Section 12

In March 2023, the government classified businesses involved in certain virtual digital asset ("**VDA**") activities as "designated businesses", which means entities exchanging or transferring virtual assets with traditional currencies are now considered reporting entities.[40]

Despite the PMLA's initial focus on domestic "reporting entities", the central government has broadened its scope to include foreign companies providing services to Indian consumers. Consequently, gambling operators are advised to maintain comprehensive transaction records from Indian users to meet potential PMLA information requests.

While the obligation cast on reporting entities is wide enough to cover non-monetary transactions, it is not wide enough to cover the current scenario of online gaming and virtual games especially with respect to so-called games of skill. Therefore, it is necessary to expand the scope of the legislation to bring the Indian online gaming sector under its purview. The Financial Intelligence Unit – India (**FIU**) has also emphasised the need for AML laws to cover entities that facilitate cross-border transactions through various payment systems.

b. Foreign Exchange Management Act

Under the FEMA read with the Foreign Exchange Management (Current Account Transaction) Rules (**Current Account Rules**), remittance (i) out of lottery winnings, (ii) for purchase of lottery tickets, banned/prescribed magazines, football pools, sweepstakes, etc., and (iii) of income from racing/riding, etc., or any other hobby, is prohibited.

The above provisions have the potential to cover skill games under the word "hobby", as such games have not been defined or expressly categorised. In 2023, the Bombay High Court resolved the question of Foreign Direct Investment in online gaming, ruling that no restrictions are applicable on foreign investment in platforms offering games such as online rummy and fantasy-based sports.[41]

Regarding using virtual currency, while India currently lacks a legal framework that regulates VDAs as well as virtual currencies, the Income Tax Act, 1961(**ITA**), provides for a definition for VDAs and has imposed tax obligations related to the buying, selling, and transferring of VDAs. Additionally, PMLA amendments have also captured VDA businesses within the definition of "reporting entities" and

[40] Gazette notification, Ministry of Finance, March 7, 2023, available at: 244184.pdf
[41] *Play Games 24*7 Pvt Ltd v RBI*, 2023 SCC Online Bom 2966

warrants such businesses to adhere to the KYC, CDD, reporting, and monitoring obligations. Goods and Services Tax (**GST**) laws have also brought VDAs under its ambit in alignment with its definition as per the ITA and thus these laws will apply to the VDAs in a similar manner.

While free-to-play online games generally fall outside the scope of traditional state gaming laws and the Online Gaming Rules due to the absence of monetary stakes, platforms offering these games are still subject to the due diligence requirements for OGIs. Additionally, these games must comply with other relevant legislation, including intellectual property, information technology, consumer protection, and obscenity laws, which could be triggered based on their content. Examples of applicable laws include the Bharatiya Nyaya Sanhita, the IT Act, and the Indecent Representation of Women (Prohibition) Act 1986.

c. Tax Regulations

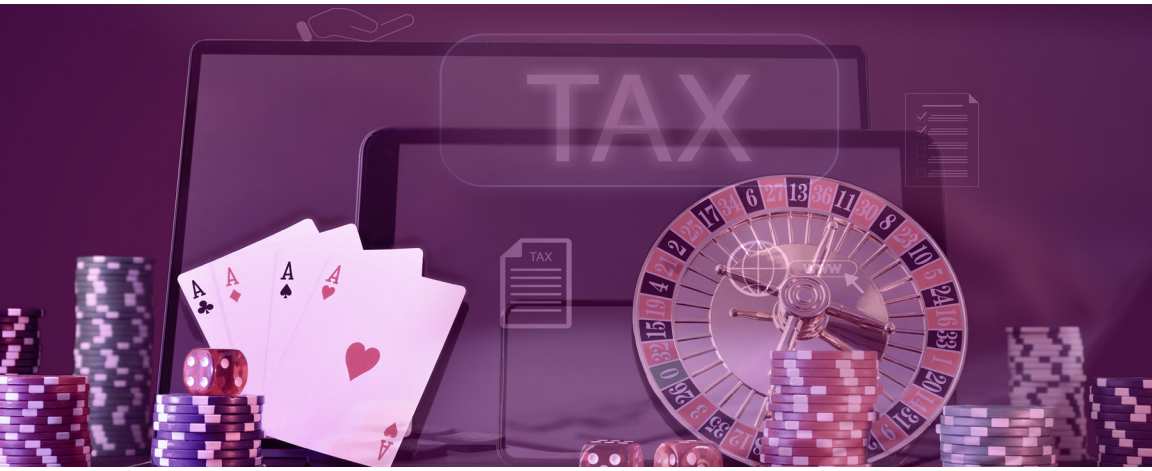
i. Indirect Tax

In August, 2023 the Goods and Service Tax Council brought amendments to the Central Goods and Services Tax Act, 2017 (**CGST Act**), and the Integrated Goods and Services Tax Act, 2017 (**IGST Act**) with respect to online money gaming, introducing the definition of online money gaming as *"online gaming in which players pay or deposit money or money's worth, including virtual digital assets, in the expectation of winning money or money's worth, including virtual digital assets, in any event including game, scheme, competition or any other activity or process, whether or not its outcome or performance is based on skill, chance or both and whether the same is permissible or otherwise under any other law for the time being in force."*[42]

Services by way of admission to entertainment events or access to casinos, etc., are taxable at the rate of 28 per cent GST. Online gaming is categorised under "online information and database access or retrieval services" (**OIDAR**), as it includes services that are largely automated, require little to no human interaction, and cannot be guaranteed without the use of information technology. The rate of tax is 28 per cent for games of chance (i.e., betting/gambling) and 18 per cent for games of skill. The tax is levied on the service fee/commission charged by the gaming operators.[43]

[42] 'Ministry of Finance on Recommendations of 51st GST Council Meeting, PRESS INFORMATION BUREAU (August 2, 2023) , available at: Press Release:Press Information Bureau

[43] Sangeeta Ojha, *GST on betting and gambling: Tax structure and liabilities in case of default*, LIVEMINT (Oct 5, 2022), available at: GST on betting and gambling: Tax structure and liabilities in case of default | Mint (livemint.com)



ii. Direct Tax

The income a resident earns from winnings in games of any sort, betting, gambling, etc., is liable to tax at 30 per cent (plus applicable surcharge and cess) in the hands of such taxpayer.

However, the tax under the ITA will not be applicable if the income is subject to Equalisation Levy (**EL**). Introduced in 2016, EL taxes digital transactions via Indian IP addresses, which can cause an accrual of income to foreign companies. Initially only applied to business-to-business transactions involving online marketing, EL was expanded to include goods or services provided by non-resident e-commerce operators in 2020. EL at 2 per cent is applicable on the amount of consideration received or receivable by an e-commerce operator from e-commerce supplies or services made, provided, or facilitated by it to a person resident in India; a non-resident in certain specified circumstances; or a person who purchases such goods or services or both using an IP address located in India. The specificity of the business model will determine whether EL applies to international gambling operators or not.[44]

Further, under the Black Money (Undisclosed Foreign Income Assets) and Imposition of Tax Act, 2015, the Central Board of Direct (**CBDT**), issued a circular providing clarifications pertaining to the Black Money Act. The circular clarified

[44] *Equalisation Levy: A critique on India's unilateral measure*, EY INDIA (Aug 17, 2020), available at: Equalisation Levy – Provisions, Scope, Modifications (ey.com)

that an offshore virtual/e-wallet account used for playing online games/ poker and funded by taxable income in India on which tax has not been paid must disclose the account details to Indian tax authorities if profits are made from said gaming. The circular also clarified that a virtual/e-wallet account be treated like a bank account because of similar inward and outward cash movements and that the e-wallet account ensure valuation and declaration along the same principles as that of a bank account.[45]

7. Risk Mitigation in the Online Gaming Sector

To mitigate the risks associated with the online gaming sector and subsequent imposition of fines, gaming operators should consider AML risk mitigation measures, such as having algorithms in place to monitor in-game transactions, flagging suspicious transactions, placing transaction limits, and tracking payment between users. Other preventive measures include blocking accounts that do not provide authentic information or have multiple accounts set up from the same IP or physical address.[46]

Given the online gaming sector's absence of comprehensive legislation and its niche and nuanced functioning, self-regulation appears to be the most effective option/solution for this industry. While the costs associated with such risk-mitigation practices could disincentivise many gaming operators, they provide a better alternative than accruing criminal liability from thriving illegal activities on these platforms. Online gaming platforms should also consider implementing these measures as good business practices to augment their reputation and profits and attract investments from foreign investors who would not want to attract regulatory scrutiny by association and are bound by stringent AML regulations themselves in their respective country.

8. Recommendations: The Way Forward

In light of the rising risk of money laundering via online gaming platforms, comprehensive steps are essential to curb the same and mitigate the risks associated with it. Companies should bear the onus of demonstrating that they have taken appropriate steps to identify, assess, understand, and mitigate AML risk and to construct their AML compliance procedures to counter any possible threats.

---

[45] *Government issues another set of FAQs on one time compliance window scheme of The Black Money Taxation Act, 2015*, PWC (Sept 11, 2015), available at: government-issues-another-set-of-faqs-on-one-time-compliance-window-scheme-of-the-black-money-taxation-act-2015.pdf (pwc.in).

[46] HINDU BUSINESS LINE, *Online Gaming Yes, Money Laundering No*. available at: Online gaming yes, money laundering no - The Hindu BusinessLine.

Taking inspiration from some of the best practices across the globe, following measures can be adopted to improve the regulation of online gaming:

Expanding the definition of gaming: As mentioned in the IMTF Report, India's current legislation governing gambling is not sufficient to address the intricacies of the growing online gaming sector. Therefore, it is necessary to expand the legislation beyond the physical understanding of gambling to the digital realm. The definition of gaming should not be limited to land-based casinos but extend to all providers of gambling services.

Licensing for online games: One way to regulate the online gaming industry is to establish the requirement of licensing for gaming operators across all states. Under this regime gaming operators would have to seek licenses from the government to host online games. This would allow for scrutiny of online gaming applications. As discussed above, currently only very few states require licensing on the part of gaming operators.

The benefit of the licensing regime is that a license can be issued by the government upon fulfilment of certain conditions by gaming operators, including compliance with AML laws. In such a regime, licensees could be required to implement several AML procedures as part of their day-to-day operations, including:

a. appointing a designated Money Laundering Reporting Officer;

b. bringing gaming operators explicitly under the definition of reporting entities under the PMLA, mandating client due diligence and enforcing penalties for non-compliance;

c. having fraud management procedures in place; and

d. having AML/CFT training for employees.

Identifying Politically Exposed Persons (PEPs): Online gaming companies should consider both foreign PEPs and domestic PEPs as high-risk clients. They must also perform enhanced due diligence with respect to PEPs. It shall also be the obligation of gaming companies to monitor the risk posed by a PEP status for a given period after it is classified as one.

Implementation of KYC: One of the foremost ways of tackling fraud and money laundering is for online gaming operators to ensure implementation of KYC verification. As more and more players enter the online gaming industry, the importance of regulatory compliance will be crucial in scaling the player base and minimising efforts to reduce fraud.

KYC need not be conducted physically, instead an e-KYC can be implemented to make the process easier. The e-KYC verification may include online document verification, ID verification through Aadhaar and Pan card, and real-time biometric face authentication, etc. In April 2022, the government considered introducing KYC obligations for online skill gaming operators in an attempt to curb money laundering.[47]

Age verification should also be a prerequisite for online games, especially in light of WHO's declaration that gaming can create addictive behaviours and lead to gaming disorders amongst teenagers.[48] Age verification will help verify and protect underaged users from accessing the game.

The Indian online gaming market is reaching a major turning point, with its value predicted to touch INR 388 billion by 2026.[49] The Indian government is proactively contemplating measures to enhance the growth of the online gaming industry by proposing an overhaul of archaic gambling laws and introducing legislation that would cover the nuances of the online gaming sector. These could potentially protect consumers, stimulate investment, and consequently, increase employment. India is on the path to providing regulated lucrative opportunities in this booming industry for operators and players, which would bring this regime at par with international online gaming regimes.

[47] Rahul Rajpal, *Status Of Gambling In India: The Need For Uniformity,* INDIA LAW JOURNAL, available at: https://www.indialawjournal. org/status-of-gambling-in-india-the-need-for-uniformity.php.
[48] World Health Organisation, *Addictive Behaviours: Gaming disorder*, available at: https://www.who.int/news-room/ques- tions-and-answers/item/addictive-behaviours-gaming-disorder.
[49] INVEST INDIA, *Media*, available at: Investment Opportunities in Media - Invest India

D

Internal Investigations – Procedures And Legal Framework

1. Introduction: Defining Internal Investigation

The past few decades have witnessed an increased focus on internal investigations in Indian companies. Usually conducted through in-house company mechanisms, such investigations are responses to complaints filed, either by employees or outsiders on different matters, including financial irregularity and employee misconduct. The company initiates a formal inquiry to determine any violation of law, regulation, or internal organisational policy.

Traditionally, companies engaged forensic experts or accountants or legal professionals to conduct such internal investigations. Although India does not have a set mechanism or procedure for conducting such investigations and the investigations are highly subjective, internal investigations are conducted in accordance with procedures defined in the internal policies of companies and international standards and best practices, to ensure integrity and fairness of the internal investigation process.

a. Relevance to White-Collar Crimes

An internal investigation proves to be vital in cases involving white collar crimes. When suspicions of commission of white-collar crimes emerge in a business, such as fraud, corruption, or embezzlement, the business needs to act to clarify the situation and recover from it. In such situations, a feasible option is to hire private investigators to conduct financial crime examinations. Such an investigation not only helps suspend public distrust and disbelief against the activities of a company, but also safeguard the business against humiliating raids. This, in turn, allows the company to self-correct any past wrongdoings.

An internal investigation is conducted for a clear picture of the facts, including what and when it happened, who was in charge, who might have suffered harm, and what additional steps would be required to stop the alleged crime from happening again. For this reason, internal audits act as a way of thwarting undesirable behaviour by individuals, which may fall within the purview of white-collar crime.

2. Significance of Internal Investigations

Internal investigations have many crucial benefits, including demonstrating a business's dedication to compliance and ethics, thus enhancing its reputation. Any internal investigation conveys a positive message to the public and the company's employees. By initiating an inquiry and through an investigation, the organisation shows that it is taking the alleged violation seriously. The ensuing corrective action that the organisation takes, portrays an expectation that its employees are required to abide by all laws and corporate standards.

Internal investigations also help companies with information gathering, defence building, and problem solving. These are particularly helpful in identifying employees that need reprimanding (or worse) and rules or procedures that need improvement. A reduction in civil and criminal penalties, which the government or the judiciary imposes on the company, may also be enhanced in its effect with the help of corrective actions by the company.[1] In fact, if a company accused of regulatory or legal violations fails to initiate an internal investigation, the same may lead to significant legal and regulatory exposures for the company. This may leave the company susceptible to a significant enforcement or regulatory action through the imposition of significant civil and criminal penalties as well as additional scrutiny from government investigators, the judiciary and the media.[2]

Ordinarily, the trigger for conducting an internal investigation may be an actual or potential violation of law or an internal policy or code of conduct, such as the Companies Act, 2013 (**Companies Act**), or Prevention of Corruption Act, 1988 (**PCA**).

---

[1] M. Missal, B. Ochs, & R Kline Dubill, *Conducting corporate internal investigations*,4(4), INT'L J. OF DISCLOSURE AND GOVERNANCE, 297, 297–308 (2007)

[2] Bruce A. Green & Ellen S. Podgor, *'Unregulated Internal Investigations: Achieving Fairness for Corporate Constituents'*, 54, BC L REV., 73 (2013)

When a corporation learns of possible wrongdoing, it may commence an internal investigation to ascertain the level and breadth of any misconduct. Such corporations are notified of any potential wrongdoing through various sources, including internal whistleblowers, external *qui tam* actions, implementation of routine internal compliance measures, etc.

Moreover, internal investigations may also be relevant considering the reporting and disclosure requirements of a company under various legislations it must comply with. Some of these include provisions relating to internal controls and audits in the Companies Act, and the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015 (**SEBI LODR**), among others. Under the Companies Act, though the companies are not expressly required to report bribery, fraud, and corruption, but if the fraud discovered exceeds a set monetary threshold, the company's auditors must notify the Central Government.[3] Moreover, any fraud committed by the company, or on the company, must be disclosed in the auditor's report as per the Companies (Auditor's Report) Order, 2020.[4]

Similarly, the LODR, requires listed companies to disclose to stock exchanges the initiation of any forensic audit, the name of the entity initiating the audit, the reasons for the same, and the final forensic audit report.[5] A person may also be punished for failing to report the commission of certain offences by another entity, or the intention to do so, under Section 33 of the Bharatiya Nagarik Suraksha Sanhita, 2023 (**BNSS**), previously under Section 39 of the Code of Criminal Procedure. Similarly, anti-corruption investigations, for instance, probing allegations of improper payments made by company employees to government officials – to either obtain or retain business – may also reveal a reportable violation of India's anti-corruption legislation, the PCA.

The 2023 Digital Personal Data Protection Act (**DPDP Act**) has altered how internal investigations handle data by expanding the definition of "personal data" to any information that can identify an individual. While the Act prioritises informed consent, data minimisation, and security, it also provides exemptions under Section 17(1)(c) that permit access to personal data for specific purposes, which may cover instances of internal investigations.[6]

The newly introduced Bhartiya Nyaya Sanhita, 2023 (**BNS**), laid down the definition of "economic offences" and includes them under organised crime for the first time.

[3] Companies Act 2013, Section 143(12)
[4] Companies (Auditor's Report) Order, 2020, available at: Companies Auditor Report Order, 2020
[5] Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations 2015, available at: SEBI | Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015 [Last amended on July 10, 2024]
[6] Digital Personal Data Protection Act 2023, Section 17(1)(c)

The legal framework has been updated to extend abetment to offenses outside India and to impose stricter penalties on white-collar crimes, including corporate fraud and insider trading. Dedicated courts for economic offenses have also been created to improve case processing efficiency.

3. Who Should Conduct an Internal Investigation?

The instant allegations of misconduct are uncovered; it is important to evaluate whether such misconduct *actually* mandates an investigation. The company's general counsel may draft a memorandum conforming to the requirements of attorney–client privilege and should set forth the allegations made, the potential legal issues involved, and, as appropriate, the need to obtain legal advice. These steps together constitute a preliminary assessment of whether an investigation is warranted.

Accordingly, where the *prima facie* assessment indicates that further investigation is needed, the company must determine who should conduct the investigation, considering the nature of the allegations and the company's internal policies and procedure. Often corporate internal investigations may serve as a prelude to forthcoming criminal prosecutions and negotiations with the government.[7]

In an internal investigation, the "client" needs to be recognised first. The client, often the company, or the general counsel or the Board, is the point of contact for the investigation and provides the requisite assistance to the attorneys for conducting the investigation. Usually, it is recommended that the investigation be managed by the company's Board of Directors, or the Ethics and Compliance Officer, as they would be viewed as impartial. Similarly, an external counsel/or law firm is hired in the role of an attorney—firstly, to ensure the integrity of the investigation and, secondly, to preserve the legal professional privilege from the company's end with respect to any advice sought or communication made.[8]

4. Steps Preceding an Internal Investigation

Before an internal investigation, it is important to identify and articulate the investigation's scope, nature, and goal. For this, the investigating team should create an investigation plan or strategy, specifying the parameters of the probe to help

[7] Green & Podgor, *Unregulated Internal Investigations: Achieving Fairness for Corporate Constituents* (December 3, 2012), Boston College Law Review, Vol. 54, 2013, Fordham Law Legal Studies Research Paper No. 2184348, Stetson University College of Law Research Paper No. 2012-22, Available at: Microsoft Word - 02_green & podgor

[8] Miller & Chevalier, *How Can Outside Counsel Sidestep Ethical Pitfalls in Internal Investigations of Antitrust Wrongdoing?*, CORPORATE COMPLIANCE INSIGHTS (June 8, 2022), available at: How Can Outside Counsel Sidestep Ethical Pitfalls in Internal Investigations of Antitrust Wrongdoing? | Miller & Chevalier

detect potential problems along the road and keep the investigation on schedule and under budget.

An investigation may commence from traditional sources, such as whistleblowers, formal complaints, self-reporting, or directions from courts or the federal or state government.[9] The investigative plan should typically include an evaluation of the firm's operations, people, jurisdictions potentially involved and the primary emphasis of the investigation. It must provide an outline of the documents and data to be examined, the people to be questioned, and the financial records that will be the focus of any forensic audit component of the inquiry, etc.[10]

Furthermore, before starting an internal inquiry, it is crucial for an organisation to have its policies and personnel documentation updated and in order. To avoid creating any uncertainty between an employee and the organisation, it is imperative for organisations to properly write their rules, manuals, handbooks, documents, and consents before initiating an investigation. These manuals must include the necessary safeguards and approvals for not only storing data on company owned devices but also processing, imaging, and transferring them to third parties regardless of their location. Even if the investigation reveals corporate wrongdoing, robust and consistently applied recordkeeping policies lend credibility to the investigative process, which may help mitigate liability for the company.[11]

a. Choosing the Appropriate Investigation Team

The need to engage the right professionals – particularly forensic experts and legal counsels – increases due to the specialised knowledge required during an investigation, because the tasks may be intricately complicated and unique, ranging from data gathering and server analysis to accounting irregularities and misstatements. The engagement of such experts should be through external counsel, to protect communication with such experts as privileged.

b. Preservation of Documents

As soon as the corporate entity becomes aware of allegations or evidence of misconduct, it should preserve all relevant documents, including e-mails. If the company has become the target or subject of an investigation, potentially responsive documents cannot be destroyed, regardless of general document

[9] Sherbir Parag, Tanya Ganguli and Lavanya Chopra, *India: navigating a new era of white-collar enforcement* (November 13, 2024), GLOBAL INVESTIGATIONS REVIEW, available at: India: navigating a new era of white-collar enforcement - Global Investigations Review

[10] *Guide to Internal Investigations at Brandon University*, BRANDON UNIVERSITY, available at: Guide to Internal Investigations at Brandon University | Diversity and Human Rights

[11] Lorraine Campos, *'Lawyers on the Front Line: Identifying Risk and Managing Internal Investigations'* CROWELL, (December 06, 2017), available at: Lawyers on the Front Lines: Identifying Risk and Managing Internal Investigations | Crowell & Moring LLP

retention policies. A clear document retention policy is a critical component of the in-house counsel's investigative toolbox as it enables an organisation to perform internal investigations and respond to requests for production readily. Moreover, to preserve documents, the investigative team must ensure that a hold is in place and every company in possession of pertinent records is notified.

c. Collection of Data and Documents

During an investigation, it is important to conduct a thorough assessment of the entity's business records, financial statements, observations generated in response to a statutory audit, and internal policies and practices as well as the level of adherence to those policies. Analysis of the entity's interactions with relevant third parties is also necessary. Moreover, modern investigations will almost always contain relevant Electronically Stored Information (**ESI**), which needs to be quickly preserved in a defensible manner. Forensic investigators are an invaluable asset to an investigative team for collaboration on strategy and identification, preservation, and analysis of electronic data.[12] The process of forensically collecting ESI captures additional information that may not be available using standard Information Technology (**IT**) tools. Formally recording the chain of custody – a chronological paper trail revealing who obtained, handled, or otherwise had control over an item of evidence throughout the probe – would be crucial to any security process, considering it helps maintain the integrity of the gathered evidence. Additionally, obtaining a consent letter from each custodian attesting to their understanding of, and agreement with, the data-gathering procedure is equally important.[13]

Therefore, collection of all necessary data and documents becomes crucial. The assessment of the corporate entities' documents requires a suitable information-collection strategy, as certain crucial aspects in collection of information need to be considered, such as the following:

i. Data Privacy and Protection

Considering the initial stage of acquiring documents requires meeting with internal staff members, the team should locate any relevant hard-copy or electronic document. However, many data privacy concerns surround the collection of such documents. During such investigation, employers – either through forensic firms or law firms – need to process large amounts of personal

[12] *'Digital Forensics: A vital component of Internal Investigations'*, 4JOURNEY, (June 25, 2020), available at: Digital forensics: A vital component of internal investigations | COSMOS Compliance Universe

[13] Kunal Gupta, Tanuj Sharma & Pankhuri Bhatnagar, *'Conducting Effective Internal Investigations and Procuring Evidence in India'*, BW LEGALWORLD.COM, (March 09, 2021), available at: [Exclusive] Conducting Effective Internal Investigations and Procuring Evidence in India - BW Legal World

data related to employees identified as subject matter of that investigation; hence, it is imperative to make a correct assessment of the rights and obligations of the corporate entity and the employees subjected to the investigation. Currently, India does not have any explicit legislation protecting data or privacy, with the Information Technology Act, 2000 (**IT Act**) being the main piece of legislation in this area. In addition, the enactment of DPDP Act in August, 2023, once notified, will repeal the erstwhile Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data and Information) Rules, 2011 (**SPDI Rules**), which is a key regulation for protecting sensitive personal data. The DPDP Act, which ensures protection of "digital personal data" – data pertaining to an individual or data – allows for the identification of an individual. Corporate entities collecting, storing, processing, exchanging, transferring, using, deleting, or erasing personal data must comply with the provisions of the DPDP Act. This specifically applies to entities or employers using personal data for internal investigations. If any other statue or regulatory body requires the entities to comply with additional obligations related to data processing or protection, they would apply alongside the requirements laid down by the DPDP Act.

In cases involving illegal disclosure, misuse, and violation of contractual obligations relating to personal data, the IT Act deals with it by imposing fines and imprisonment under civil and criminal legislation. While defining the right to privacy as a basic right in *Justice Puttaswamy (Retd) v. Union of*

India,[14] (**Puttaswamy**), the Supreme Court of India concluded that it was not an absolute right and may be made conditional on acceptable grounds.

The *Puttaswamy* judgment states that investigations related to communications and data carriers must be conducted keeping in mind the privacy concerns of those involved in the investigations. According to the widely used principles of law of proportionality and subsidiarity, investigative methods should be proportional to the goal (and to the interest of the client for reaching this goal), and the least intrusive method should be used when possible.

This, in turn, obligates companies to (a) ensure, in instances of sensitive personal data or information or personal information, a legitimate reason for collecting and using such data; (b) provide adequate privacy notice to the affected employees; (c) obtain prior consent of the affected employees; and (d) maintain reasonable measures to protect the security and confidentiality of such data.[15]

d. Review of Documents and Data Collected

Document review is a critical component of any internal investigation. Among other things, documents assist counsel in obtaining information from witnesses, and in educating law enforcement officials on issues under review. To the extent practicable, a careful document and data review should be completed before key witness interviews, to ensure that the interviewer is in the best position to examine relevant documents with the witness. To efficiently review documents, creating a "list of key phrases" is of utmost significance, as these phrases form a part of the subject of inquiry and are likely to come up within the data. Such searches are normally conducted by forensics via certain AI tools and platforms like Relativity.

The emails, documents, and data found are then physically evaluated, with the reviewers individually labelling (or identifying) the emails, documents, and flagging the data appearing pertinent to the investigation's subject, for further examination and action. Once collected, documents should be reviewed for relevance and privilege. Privileged documents should be segregated immediately and made accessible only to the counsel and its agents to prevent inadvertent waiver of attorney–client privilege. Preferably, a preliminary list of potential

[14] *Justice Puttaswamy (Retd) v. Union of India*, (2017) 10 SCC 1 (India)
[15] Srijoy Das, Siddharth Seshan and Disha Mohanty, *'India-A Guide to Conducting Internal Investigations in India'*, GLOBAL INVESTIGATIONS REVIEW, (March 04, 2016), available at: India - A Guide To Conducting Internal Investigations In India - Global Investigations Review

interviewees can be drawn up during the initial document review phase so that a separate set of relevant documents can be assembled in preparation for each interview.

e. Processing the Information Collected

Data processing involves evaluating its legal admissibility and value, while keeping confidentiality in mind. The data to be analysed will largely depend on the company's technological sophistication and the alleged wrongdoing, but it consists of a mixture of ESI (emails, electronically-stored documents, chat messages), physical documents, and, occasionally, files stored on personal devices of company employees (text messages, personal emails, etc.). When found, the right information sources – such as employee email accounts, business communications, and pertinent files – can be quickly uploaded to a document review platform or any pre-existing integration with data sources may be used for instant collection, thus enabling investigators to start establishing the relevant facts.

Additionally, forensic accounting could be used to integrate accounting, auditing, and investigative skills to conduct an examination into a company's financial statements.[16] The admissibility of such independently gathered evidence is frequently questioned before a legal authority, despite forensic diligence reports being crucial in understanding the facts and liability of a firm and its officers or employees.

f. Confidentiality Concerns and Client-Attorney Privilege

India has adopted a strict approach towards privileged professional communication between clients and legal advisors. Sections 132–134 of BSA (Sections 126–129 of the erstwhile Indian Evidence Act) deal with data confidentiality that the client shares with the attorney, ensuring that any communication made for seeking legal advice from an attorney is protected. In India, persons seeking advice from a practicing advocate registered under the Advocates Act, 1961, have the benefit of legal privilege and their communication is protected under Section 132 of BSA (Section 126 of the erstwhile Indian Evidence Act). However, in the Indian legal framework, this protection does not generally extend to an in-house counsel.

An attorney, cannot disclose, on behalf of a client, any communication the client makes without the express consent of the client during the course of or for the

[16] Bhasin, M.L., Forensic Accounting: A New Paradigm for Niche Consulting. The Chartered Accountant Journal, 1000-1010 (2007)

purpose of his/her engagement of such attorney. Furthermore, an attorney cannot state the contents or conditions of any document he/she may have become acquainted with during his/her engagement as an attorney or disclose the advice provided to the client. The Hon'ble Bombay High Court, in *Larsen & Toubro Ltd v Prime Displays (P.) Ltd.*[17] held that any document prepared by an attorney in anticipation of litigation would also be protected by privilege.

In a leading case involving the Serious Fraud Office of England and Wales, and Eurasian Natural Resources Corporation Limited, a company based out of London, the appellant company successfully asserted litigation privilege over documents produced during internal investigations into alleged bribery and corruption.[18] The England and Wales High Court of Appeal recognised that litigation privilege extended to materials prepared by solicitors, including preliminary legal work, records of evidence provided by individuals, and documents created by forensic and accounting firms engaged by the solicitors as part of the investigation. Moreover, legal advice aimed at preventing, mitigating, or settling reasonably anticipated proceedings was deemed to hold the same level of litigation privilege as advice for defending or contesting litigation.

g. Notice of Mandatory Leave

As a matter of best practice and to preserve the independence, fairness, and the sanctity of the investigation, the company may issue a notice of mandatory leave to the employees to be interviewed in relation to the allegations under the said investigation. Mandatory leave is a standard procedure in matters of this nature and should not be viewed as punishment or a reprimand or an attempt to hassle, intimidate, or victimise the employees. The mandatory leave notice is issued in accordance with the policies of the company and with a view to complete the fact-finding process in a fair, efficient, and timely manner.

Pursuant to the notice, during the mandatory leave period, employees are advised not to contact or attempt to contact any employee of the company or any client, customer, dealer, supplier, agent, professional adviser, etc., without prior written permission of the company. The employees are also required to hand over all company properties, devices, and materials. However, in the interest of fairness, employees continue to receive monthly remuneration (full or certain percentage) and other employment-related benefits during the mandatory leave period. If no wrongdoing or misconduct is found on the employee's part, then the mandatory leave is revoked, and the employee is reinstated to his or her position and role.

[17] Larsen & Toubro Ltd v Prime Displays (P) Ltd., [2003] 114 Comp Cas 141 (Bom)
[18] Eurasian Natural Resources Corporation Ltd v. Director of the Serious Fraud Office, [2018] EWCA Civ 2006

h. Investigation Interviews and Questionnaires

Interviews, – another important means of data collection – are usually conducted by the General Counsel or the Ethics and Compliance Officer of the company and assisted by external counsels/law firms.

Interviewees are given an Upjohn warning and are apprised of attorney–client privileges and the importance of maintaining confidentiality during such interviews. Derived from the decision in the landmark case of *Upjohn Co. v. the United States*, an Upjohn warning refers to the notice that attorneys (in-house or outside counsel) provide company employees, informing that they represent only the company and not the employees individually.[19] Additionally, the company has the option to forego the aforementioned privilege and give the interviewee's information to any governmental body, law enforcement agency, or other third party.

Similarly, the interviewees should be told to preserve pertinent documents and data in accordance with any prior preservation notice that has been issued. (If no notice has been issued, the witness should be instructed to preserve specific documents and data, and a written notice should follow as soon as practicable.) The interviewees should also be given the investigator's/company's point of contact information for questions or requests for further information.

5. Steps Following an Investigation

On the conclusion of the aforementioned procedures, the following steps are undertaken to close an investigation:

a. Investigation Report

The investigation team drafts an Investigation Report to help the company evaluate the future course of action. Any inquiry should end with a written report summarising the steps taken, the methods used, and the information discovered.

As the investigation progresses, a skilled and trained professional will take copious notes and maintain flawless records, adding to them with each successive interview and information review. The aforementioned points will be crucial for compiling the entire history of the problem, incident, and situation and will serve as the foundation for the investigative report.

[19] *Upjohn Co. v. United States*, 449 U.S. 383 (1981)adigm for Niche Consulting. The Chartered Accountant Journal, 1000-1010 (2007)

b. Legal Obligations and Future Course of Action

After the internal investigation ends, the corporation will still have obligations under the law, including taking further action, based on the findings of the report. Additional actions could include reporting to the board/audit committee, the statutory auditors, and any regulatory agencies to the extent that doing so is mandated by law or prudent under the circumstances. They could also include taking internal corrective action and considering whether to file a lawsuit. Further, the final report may or may not include recommendations for further actions, remedial measures, and the like.

Companies may also choose to penalise guilty individuals. Depending on the type and seriousness of the offence, the governing law, and company officials or workers, penalties for officials or employees of the company may include suspension, termination, imprisonment, fines, debarment, disgorgement, or a combination of any of these sanctions.

A company also may consider disciplining an employee for refusing to cooperate with an internal investigation. An internal investigator generally has no ability to subpoena witnesses, and therefore, an employee can merely decline to cooperate with the investigators, unless the employer can exercise some reasonable form of leverage. Terminating an employee refusing to cooperate should not be done reflexively, as it can lead to serious consequences for the company under employment laws.

6. Concerns and Issues in Internal Investigations

Several concerns surrounding internal investigations have harmed its efficacy in uncovering white collar crimes in India.

a. Systematic Vulnerabilities of Corporate Structures

Process gaps and systemic vulnerabilities are frequently neglected in India due to the prevailing managerial structures. Employees are frequently reluctant (or afraid) to deviate from the orders coming down the chain (often carrying out instructions with mechanical precision and without independent analysis or judgement), or to report complaints or gaps that they have encountered in the course of their work to anyone other than their direct reporting manager.

This is because the reporting structure is frequently so rigid and the sense of loyalty (whether misplaced or otherwise) is so strong that junior staff members are usually not comfortable with disregarding instructions, even if they seem irrational or outside of the course of business.

b. Lack of Integration and Consensus within Corporate Entities

Lack of integration within the company and the operation of teams is quite prevalent, with certain teams within an organisation operating independently, instead of being fully integrated with the processes of the company. In cases where the team undertakes complicated, highly technical processes (involving convoluted manufacturing, technology systems, etc.), the rest of the company is likely to be unfamiliar with or fully understand these processes, and the team is left to run on its own. Such actions lead to reduced visibility (into their operations), allowing such teams to escape accountability from the rest of the company and evade any control over them.

Similarly, companies must investigate claims of misbehaviour with considerable caution in deciding whether to initiate an internal investigation. Such a decision is rarely unanimous. From the start, support in favour of investigation may deteriorate, considering the management may hesitate to conduct an investigation for fear of potential reputation damage or liability.

7. Conclusion

Internal investigations serve an important role in tackling white-collar crimes by uncovering issues relating to ethics and non-compliance, code of conduct violations, fraud, corruption, bribery, etc. Any outcome of such investigations is then considered in deciding future actions, including reprimanding its employees and changing company policies. Occasionally, companies also report alleged wrongdoings to the authorities during or after the investigation, especially in the instances of mandatory compliance norms. Therefore, an internal investigation ensures that the reputation of a company does not suffer owing to the activities of its employees, and that it gets an opportunity to correct and improve its actions. Moreover, voluntarily cooperating with law enforcement and courts can lessen the negative legal, economic, or reputational consequences of direct intervention and hard sanctions.

E

Environmental, Social, and Governance Compliance and Enforcement in India

1. Introduction

Twenty-one years ago, in a report titled "Who Cares Wins", the term Environmental Social Governance (**ESG**) was first coined under the umbrella of the UN.[1] During those days, ESG was considered just a trend. Today, it is at the centre of every decision made by large corporations, businesses, industries, and governments. Even though, conceptually, ESG has been around for nearly two decades, it is only now that the effort has become concerted and organised towards achieving certain goals. The finance sector has witnessed exponential traction for ESG, driven by the changing perspectives of institutional investors.

In the 2016 Paris Agreement, 190 countries agreed on Climate Change measures, bolstering the role of corporates to improve environmental, social and governance parameters for a sustainable future.[2] Undeniably, the environment needs to be continuously regulated to drive sustainable growth. Increasing global demand for ESG compliance, especially among multinational corporations, has rendered law firms to dedicate niche advisory services for it.

Regarding sustainability, it is important to acknowledge that its scope extends beyond environmental concerns. Under ESG, social components constitute elements such as respecting human rights, providing safe products to end consumers and personal data protection. Similarly, topics such as transparency, accountability, anti-bribery and corruption policies are closely linked to governance issues – bribery and corruption can undermine a company's ESG policies. The ultimate objective of ESG is to ensure that businesses run in a responsible manner. Even though numerous companies are taking up ESG targets under the head of CSR initiatives, it is largely considered insufficient. This is due to the traditional nature and functionality of Indian companies, with low gender diversity (women account for typically less than a fifth of the Board) and independence (below 50 per cent), as many entities are family controlled.[3]

[1] United Nations and Swiss Department of Foreign Affairs, *Who Cares Wins*, Connecting Financial Markets to a changing world, (December, 2004), available at: 04-37665.global.compact_REV.2
[2] The Paris Agreement, 2016, available at: The Paris Agreement | United Nations.
[3] Nidhi Singal, *Why India Inc. Is Excited About ESG*, businesstoday.in (July 07, 2022), available at: Why India Inc. Is Excited about ESG

2. Legislations that Address ESG

Under the Indian laws, ESG has not been codified into any statute, rather the regulatory framework related to ESG falls under various pieces of legislation, including Environment Protection Act, 1986, Air (Prevention and Control of Pollution) Act, 1981, Water (Prevention and Control of Pollution) Act, 1974, Hazardous Waste (Management, Handling and Transboundary Movement) Rules, 2016, Factories Act, 1948, Child Labour (Prohibition and Regulation) Act, 1986, Bonded Labour System (Abolition) Act, 1976, Companies Act, 2013, Prevention of Money Laundering Act, 2002, Prevention of Corruption Act, 1988, etc. Various aspects of ESG norms are protected under these legislations. Under the Factories Act, 1948, the working conditions and terms of employment of certain categories of workmen are regulated.

The Indian government has recently formulated four consolidated labour codes in a bid to address contemporaneous concerns in the workforce. India's new labour codes merge and streamline 29 central labour laws into four comprehensive codes that aim to address concerns related to governing wages, industrial relations, social security and working conditions. The codes are yet to be implemented, but the objective is to update labour regulations, make compliance easier for businesses, and strengthen protections for workers.[4]

a. Ensuring fair and equitable pay: The Code on Wages, 2019, aims to standardise and simplify wage regulations, promote pay equity, and enhance worker protections through regular wage reviews, anti-discrimination provisions, clear payment guidelines, and inclusive advisory mechanisms.[5]

[4] Debjani Aich, *Analysing the new labour codes: Impact on employee work hours, leave and overtime*, The Economic Times (January 11, 2025), available at: Analysing the new labour codes: Impact on employee work hours, leave and overtime - The Economic Times

[5] *[India] Key changes to the Wage Code*, GPA (April 12, 2021), available at: [India] Key changes to the Wage Code – GPA

b. Industrial relations: The Industrial Relations Code, 2020, aims to simplify industrial relations, provide more flexibility to employers, extend protections and benefits to a wider range of workers, strengthen the framework for trade unions and improve mechanisms for dispute resolution and worker re-skilling.

c. Social Security: The Code on Social Security, 2020, aims to provide a comprehensive and inclusive social security coverage for India's diverse workforce by consolidating existing laws, expanding coverage to new categories of workers, and streamlining benefit delivery through dedicated social security funds and digital registration systems.

d. Working conditions: Occupational Safety, Health and Working Conditions Code, 2020, aims to standardise workplace safety rules, expand coverage to more workers, formalise employment practices, and ensure better health and welfare provisions for employees across industries.[6]

Furthermore, under the Companies Act, 2013 (**Companies Act**), a company board (of directors) must act *bona fide* in promoting its objects under Section 166. The Supreme Court has held that the duty of a director to act in good faith under Section 166(2) of the Companies Act is not limited to the company and its shareholders, but also extends to the environment.[7] Regulatory filings of Indian companies are typically prepared and made under the authority of key managerial personnel; and in the event of inaccurate reporting, a degree of liability is ascribed to the officers of the company. Further, liability resulting from non-compliance with obligations under the ESG framework is also attributable to officers of the company.

Along with internal controls, the Companies Act also mandates an annual audit of companies by chartered accountants. These reports that provide a broad overview of the financial, operational and government matters are required to be filed with the registrar of companies as they form a part of routine filings.

3. ESG Policies in India

To ensure responsible business conduct by companies, the Ministry of Corporate Affairs (**MCA**) introduced the 'Voluntary Guidelines on Corporate Social Responsibility' in 2009. After prolonged consultations with businesses, government, academia, etc., the guidelines were revised and called the National Voluntary Guidelines on Social, Environment and Economic Responsibilities of Business (**NVG**).[8] In March 2019,

[6] Naina Bhardwaj, The OSH Code, 2020: *A Primer*, India Briefing (February 21, 2024), available at: Key Features of the OSH Code, 2020: India's HR Laws
[7] *M.K Ranjitsinh v. Union of India* (Writ Petition (Civil) No. 838 of 2019)
[8] National Voluntary Guidelines on Social, Environment and Economic Responsibilities of Business' issued by the Ministry of Corporate Affair, (July 2011), available at: BOOKLET PRINT 6711

the NVG was further revised into the National Guidelines on Responsible Business Conduct (**NGRBC**).[9]

After the introduction of NVG, SEBI observed that listed companies have an element of public interest involved since they have access to public funds, rendering continuous disclosures obligatory for them. Thus, in 2012, SEBI instructed the top 100 listed companies by market capitalisation to include Business Responsibility Report (**BRR**) in their annual report, and describe the initiatives taken by them from an ESG perspective.[10] In 2015, this number was extended to 500 companies[11] and, in 2019, it was extended to the top 1,000 companies by market capitalisation.[12]

In 2021, the Business Responsibility and Sustainability Report (**BRSR**) replaced the BRR to make the reporting framework more comprehensive, focusing on measurable key performance indicators across all principles of NGRBCs.[13] The top 1,000 listed companies by market capitalisation were mandated to furnish this report from financial year 2022-23. Furthermore, through the 'Report of the Committee on Business Responsibility Reporting'[14], the MCA has prescribed voluntary ESG disclosures in the format provided as BRSR Lite for other listed and unlisted companies.

In May 2021, the RBI had set up a 'Sustainable Finance Group' (**SFG**), to suggest strategies and introduce a regulatory framework for banks that could propagate sustainable practices and mitigate climate related risks.[15] SFG was thus set up as a medium to co-ordinate with other national and international agencies to deal with climate change.

SEBI introduced the Business Responsibility and Sustainability Report Core (**BRSR Core**) in July 2023, enhancing its 2021 ESG reporting framework.[16] This new core report requires listed companies to disclose specific Key Performance Indicators across nine ESG attributes, including greenhouse gas emissions, water and energy footprints, circular economy practices, and employee well-being. SEBI envisions implementing 'reasonable assurance' for these disclosures in phases. Starting in 2023-24 with the top 150 listed companies, it will expand to the top 1,000 by 2026-27. Additionally, the

[9] National Guidelines on Responsible Business Conduct' published by the MCA, (March 15, 2019), available at: MCA releases national guidelines on responsible business conduct
[10] Securities and Exchange Board of India Circular CIR/CFD/DIL/8/2012, (August 13, 2012), available at: 1344915990072.pdf
[11] *Id*
[12] Report of the Committee on Business Responsibility Reporting (May 8, 2020) published by the MCA, available at: Report of the Committee on Business Responsibility Reporting
[13] Circular on 'Business responsibility and sustainability reporting by listed entities' published by the SEBI, (May 10, 2021), available at: SEBI | Business responsibility and sustainability reporting by listed entities.
[14] Report of the Committee on Business Responsibility Reporting (May 8, 2020) published by the MCA, available at: Report of the Committee on Business Responsibility Reporting
[15] Reserve Bank of India Publications (28 December 2021), available at: Reserve Bank of India - Publications
[16] Securities and Exchange Board of India, Circular SEBI/HO/CFD/CFD-SEC-2/CIR/2023/122, BRSR Core – Framework for Assurance and ESG disclosures for value chain', (July 12, 2023), available at: SEBI | BRSR Core - Framework for assurance and ESG disclosures for value chain

top 250 companies must include value chain disclosures in their annual reports, and their Boards must ensure the assurance provider is qualified.

India's ESG landscape has been significantly influenced by its commitments at the 2024 United Nations Climate Change Conference (**COP-28**) in Dubai. These include a global push to phase out fossil fuels, accelerate net-zero energy systems, and boost renewables and energy efficiency by 2030, as well as the 'Emirates Framework for Global Climate Resilience'. India has pledged to achieve net-zero carbon emissions by 2070 and has established intermediate targets, such as 50% renewable energy capacity by 2030, which are prompting businesses to align their ESG strategies with these national goals.

Furthermore, the New Collective Quantified Goal on Climate Finance (**NCQG**) or Baku Finance Goal agreed at the COP29, held in Baku, Azerbaijan, in November 2024, focuses on scaling resources for climate action in developing nations, with the parties pledging to channel USD 300 billion a year by 2035 to ramp up climate action.[17] However, India has objected to the proposed fund of USD 300 billion as it falls significantly short of the USD 1.3 trillion that is required by the Global South. Additionally, India opposed altering the scope of mitigation and transition frameworks, stressing on the necessity for fair climate finance discussions in light of the draft of the Mitigation Work Programme (**MWP**).

[17] Ministry of Environment, Forest and Climate Change on India's Intervention at the Plenary Session of the UNFCCC-CoP29, PRESS INFORMATION BUREAU (November 21, 2024), available at: Press Release:Press Information Bureau

The aforementioned developments show a continuous legal evolution and ESG growth in India. The increasing SEBI and MCA focus is proof that the regulators are committed towards establishing an uniform ESG disclosure regime, ensuring that corporates are walking the talk. If this continues, it will not be difficult to ascertain a uniform disclosure regime for all companies in India. Enhanced disclosure norms will make ESG conduct mandatory rather than discretionary.

4. Scope of Application of ESG

The degree of compliance is directly related to the nature of operations carried out by an entity. For instance, industries with heavy pollution loads are subject to more stringent obligations related to community reparations and reporting of the impact of their operations on the environment. Some stricter governance norms are the inclusion of independent directors on the Board and constitution of dedicated committees.[18] Typically, any entity that engages 10 to 20 employees as part of its operations in India is required to comply with the labour and corporate governance laws. However, some entities in India are completely exempt from compliance with the ESG framework.

Adjudicative bodies with investigative powers must ensure that Indian companies are enforcing and implementing all their obligations correctly. In case of non-compliance, these bodies have the authority to undertake investigations, request information and adjudicate on matters. The examples for the same are:

a. Pollution Control Boards under the Environment Protection Act, 1986;

b. Regional Provident Fund Commissioners under the Employment Provident Funds and Miscellaneous Provisions Act, 1952; and

c. The Regional Registrars of Companies under the Companies Act, 2013.

d. The National Green Tribunal, a quasi-judicial body, adjudicating on matters relating to environmental protection and conservation, including the enforcement of legal rights and the provisions of relief to victims of polluting activities.

5. ESG and Investors

ESG investing refers to making investments based on both financial and non-financial factors such as environmental, social, and governance (**ESG**) criteria. In today's

[18] 'Ministry of Environment, Forest and Climate Change on Re-Categorisation of Industries a landmark decision, new category of white industries will not require environmental clearance': Javadekar, PRESS INFORMATION BUREAU (March 05, 2016), available at: Environment Ministry releases new categorisation of industries

time, investors heavily rely on ESG as an important metric to guide their investment decisions. Greenwashing is looked at poorly by investors internationally.[19] ESG investing has been gaining momentum due to its positive correlation with rates of return, as well as policy and regulatory actions by governments and regulators, aimed at combating climate change and economic and social inequalities.

On international cross jurisdictional level, to receive relevant information on incidents that breach the law, have serious effects on the environment or have caused loss of life, investors acquire inspection and information rights under transaction agreements. The aim is to receive information on working conditions, environmental and social risk assessment, grievance mechanisms for workers, anti-corruption, and anti-bribery policies, etc.

To further facilitate effective implementation of ESG, companies can resort to:

a. Undertaking and incorporating additional ESG related tasks and responsibilities like increasing the utilisation of renewable sources of energy, decreasing carbon footprint, increasing the amount spent on corporate social responsibility, etc.

b. Establishing dedicated committees for furtherance of ESG goals.

c. Consistent tracking of ESG initiatives and goals for accountability and better understanding of areas of improvement.

d. Appointing a compliance officer to oversee reporting obligations under the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 (**LODR**)[20], and voluntarily adopting suitable ESG compliance framework.

6. ESG Activism and Strategy

ESG activism can broadly be understood as an investor or shareholder taking a position in a company (usually at the board level) and actively and qualitatively analysing and improving not only financial, operational and strategic facets of the company, but also its ESG footprint.[21] A vital role is played by investors and shareholders on account of their access to capital resources and their ability to induce positive changes related to shaping the ESG strategies of companies.

In general, corporate governance is largely being driven by investor and shareholder interest, who are now widely acknowledged as the ultimate owners of a company,

[19] Deena Robinson, *What is Greenwashing*, EARTH.ORG (November 13, 2022), available at: What Is Greenwashing and How to Avoid It | Earth.Org

[20] SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 (September 02, 2015), available at: SEBI | Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015 [Last amended on March 28, 2025]

[21] Kenneth Squire, *Activist ESG investing — the Goldilocks of responsible investing*, CNBC (October 8, 2022), available at: Activist ESG investing — the Goldilocks of responsible investing

and not merely passive bystanders. They are playing an active role in positively monitoring and policing management activities. Over the last couple of years, with growing awareness, investors and shareholders are pushing for community participation and environmental development, as ESG is viewed as a long-term wealth generation tool.[22] Class actions have occasionally been filed in opposition to policies that are thought to be harmful to the immediate environment or ecosystem in which the relevant company functions.

Consequently, companies have a responsibility to actively engage with investors and shareholders on ESG, AML compliance, labour rights, climate risks, etc., with specific focus on white-collar practice. Investor and shareholder activists, employees and others are using both litigation and reputational levers to hold companies accountable for environmental harms and human rights violations.[23]

7. Issues in Implementation and Monitoring of ESG

a. **Lack of skilled ESG professionals**: The duties and responsibilities allocated to today's ESG professionals are much more complex and diverse than before. It includes dealing with multiple stakeholders, being up to date with the changing regulations, driving capital allocation, etc. Simply training employees is not enough and this shortage poses an issue in ESG implementation.

b. **Identification of appropriate material issues**: As mentioned before, ESG compliance varies from industry to industry and so does its issues. Companies should focus on material issues that directly affect their stakeholders, impact society, and contribute to the bottom line. This materiality assessment provides a blueprint for an organisation's ESG strategy in the long run.

c. **Technology integration barriers**: Many companies report that a major obstacle to embedding ESG into their operations is the lack of fully developed, easily deployable technology solutions.[24] The process of implementing new ESG technologies, such as artificial intelligence, blockchain, or advanced analytics can be complicated, which often discourages organisations from fully adopting digital ESG tools.[25] The expenses involved in setting up and maintaining ESG technology

[22] Melissa Sawyer, Lauren Boehmke and Susan Lindsay, 2022 U.S. *Shareholder Activism and Activist Settlement Agreements*, HARVARD LAW SCHOOL FORUM ON CORPORATE GOVERNANCE (January 5, 2023), available at: 2022 U.S. Shareholder Activism and Activist Settlement Agreements

[23] *Prepare for ESG activism*: Parekh, THE TIMES OF INDIA (December 20, 2021); available at: Prepare for ESG activism: Parekh - Times of India

[24] Mark Segal, *Technology Integration a Missing Ingredient to Meeting ESG Ambitions: Accenture*, ESG Today (June 08, 2022), available at: Technology Integration a Missing Ingredient to Meeting ESG Ambitions: Accenture - ESG Today

[25] Anuradha RK, *The Role of Technology in ESG Reporting: A look at Emerging Trends and Best Practices*, LSEG (May 16, 2023), available at: The Role of Technology in ESG Reporting: A Look at Emerging Trends and Best Practices | Issuer Services | LSEG

platforms can be substantial, especially for small and medium-sized enterprises, even though automation and digital tools may lead to savings over time.[26] As the field of sustainability technology is still evolving, it can be difficult for organisations to select the most appropriate tools and platforms for their specific requirements.[27]

d. **Organisational and strategic barriers**: There is often a mismatch between an organisation's ESG aspirations and the actual execution, as technology plans are not always in sync with sustainability targets.[28] Senior technology leaders, like CIOs and CTOs, are not consistently engaged in defining or taking responsibility for ESG objectives, which can hinder the seamless integration of technology with sustainability efforts.[29] Lack of universally recognised ESG frameworks and standardised reporting practices makes technology integration more challenging, forcing companies to navigate a complex landscape of varying requirements and guidelines.[30]

e. **Greenwashing risks**: Greenwashing represents one of the most significant challenges in authentic ESG governance. An organisation may report misleading or unsubstantiated claims about environmental practices being followed. Companies should establish internal verification processes, enabling detection and prevention of greenwashing. There should be accountability structures across departments, which generate ESG claims.

f. **Challenges to Be Addressed**: ESG reporting presently lacks a standardised scheme. There are multiple ways of reporting, which require legislative harmonisation of ESG principles, frameworks and considerations. Other challenges relate to consistency, transparency, comparability, and materiality of ESG standards. These may serve as roadblocks in the effective implementation of ESG reporting. Moreover, high capital costs and lack of expertise can further disadvantage smaller companies. Hence, these concerns must be addressed to formulate an effective and efficient mechanism of ESG reporting in the future.

---

[26] Marc Lepere, *Beating the Barriers to ESG Implementation (ESGgen)*, PrimeGlobal (April 27, 2023), available at: PrimeGlobal | Beating the Barriers to ESG Implementation (ESGgen)
[27] *Lowering the barriers to ESG reporting with technology*, Eco-Business (August 29, 2022), available at: Lowering the barriers to ESG reporting with technology | News | Eco-Business | Asia Pacific
[28] *From Insights to Action: The Technology Impact on Sustainability*, Ecosystm, available at: https://www.kyndryl.com/content/dam/kyndrylprogram/doc/en/2024/technology-impact-sustainability.pdf
[29] Mark Segal, *Technology Integration a Missing Ingredient to Meeting ESG Ambitions: Accenture*, ESG Today (June 08, 2022), available at: Technology Integration a Missing Ingredient to Meeting ESG Ambitions: Accenture - ESG Today
[30] Chris Marsh, *ESG and Technology: Impacts and Implications*, S&P Global, available at: 451-esg-and-tech-dckb-report.pdf

8. Conclusion

It is rightly said that ESG is an important journey that all companies must embark upon, as complying with ESG will only further a business's growth and prosperity. Additionally, policy makers and regulators must also work towards creating and building a more comprehensive and extensive ESG reporting regime. Also, it should not be confined to listed entities alone and should cover unlisted entities as well. Investors must align their portfolios towards sustainable development and not just focus on maximising financial returns. The need of the hour is adherence to ESG norms, and for companies to recognise and expand their focus on ESG related aspects in their core business areas.

With increasing investor and shareholder activism, reliance on climate and ESG-related disclosures and growing demand for investments that are 'ESG-friendly', market regulators are also paying attention to company statements on ESG. This is likely to lead to an uptick in investigations and penalties using readily available tools. At present, environmental and climate-related topics are in focus, but the incorporation of social and social justice related concepts into activism strategies would be an added bonus to ESG themed activism.

F

Cryptocurrency Regulation and White-Collar Crimes Enforcement

1. Introduction

The last decade witnessed a myriad developments in technology and business practices, which paved the way for virtual businesses and financial activities. This space grew further since the emergence of the COVID-19 pandemic. From a legal standpoint, the impact of cryptocurrencies or the virtual assets industry on investment and transaction patterns is particularly intriguing.

Such has been the proliferation of cryptocurrencies in financial markets that governments and authorities are increasingly taking notice of the risks involved, especially related to customer protection, anti-money laundering (**AML**) and combating terror financing. Given the highly speculative character and absence of detailed regulations, cryptocurrencies are vulnerable to frauds and price volatility.[1]

The Enforcement Directorate (**ED**), along with the Finance Ministry's Finance Intelligence Unit-India (**FIU-IND**) have attached assets worth INR 936 crore as of January 2023.[2] More recently, on March 14, 2025, the CBI detained Aleksej Besciokov, a Lithuanian national residing in Russia, for his alleged involvement in laundering at least USD 96 billion in cryptocurrency since 2019, from which he reportedly gained millions in illicit funds.[3] Additionally, the ED had seized assets worth INR 1,646 crore from BitConnect, a now-defunct crypto investment platform, in February 2025. The BitConnect lending programme fraudulently offered unregistered securities, and lured investors to deposit funds in cash and Bitcoin with false promises of generating profits up to 40% per month, using a purported proprietary "volatility software trading bot".[4] The FIU-IND had previously imposed a penalty amounting to INR 18.82 crore on Binance, a cryptocurrency exchange, in June, 2024, for non-compliance with multiple provisions of the Prevention of Money Laundering Act, 2002 (**PMLA**). The FIU-IND had also issued directions for Binance to adhere to the compliances under

[1] *Chapter 1: Macrofinancial risks*, RESERVE BANK OF INDIA (December 29, 2021), available at: Reserve Bank of India - Reports
[2] Ministry of Finance, *Crypto Assets are boderless, require international collaboration to prevent regulatory arbitrage*, PRESS INFORMATION BUREAU (February 6, 2023), available at: Crypto Assets are borderless, require international collaboration to prevent regulatory arbitrage.
[3] Nikita Yadav, *India arrests crypto administrator with Russia links wanted by US*, BBC News, Delhi (March 13, 2025), available at: Kerala: India arrests Russia based crypto administrator wanted by US
[4] *ED seizes 'biggest' crypto fund worth Rs 1,646 crore in PMLA case*, Business Standard (February 15, 2025), available at: ED seizes 'biggest' crypto fund worth Rs 1,646 crore in PMLA case | India News - Business Standard

Chapter 4 of PMLA, and Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (**PML Rules**).[5]

2. Overview of Cryptocurrencies

a. Blockchain Technology

Cryptocurrency is based on blockchain technology. Blockchain is a distributed ledger technology, which enables a shared ledger among the various parties involved in business transactions,[6] thus eliminating the need for a central entity to validate the transactions. The first application of blockchain technology was to design and develop cryptocurrency i.e., Bitcoin, in 2009.

b. Cryptocurrency

While cryptocurrencies are not legally defined in India[7], the defining characteristics of cryptocurrencies are:

- "... decentralised systems where transactions are authenticated by participants themselves by consensus. They are designed to bypass the financial system and all its controls. They cannot be traced or confiscated or frozen by Governments.
- They are anonymous – transactions are verified, but not the purposes or counterparties of transactions.
- They are borderless – that is, they work over the internet without any physical existence."

[5] *Financial Intelligence Unit Penalizes Binance $2.25 Million For Anti-Money Laundering Violations*, LiveLaw (June 24, 2024), available at: Financial Intelligence Unit Penalizes Binance $2.25 Million For Anti-Money Laundering Violations
[6] Ministry Of Electronics & Information Technology, *National Strategy On Blockchain: Towards Enabling Trusted Digital Platforms* (December 2021), available at: Press Release: Press Information Bureau
[7] *Cryptocurrencies- An Assessment: Keynote address delivered by Shri T Rabi Sankar, Deputy Governor, Reserve Bank of India*, RBI (February 14, 2022), available at: Reserve Bank of India - Speeches

On December 29, 2021, the Reserve Bank of India (**RBI**), in a chapter of its report titled "Macro¬financial Risks", noted with concern, the proliferation of Anonymity-Enhanced Cryptocurrencies. Anonymity is the primary issue that the RBI sees as ailing the blockchain industry. Since the source of funds is not ascertained, there exists immense risks of illegal transactions and money laundering.[8]

c. The evolution of the legal status of cryptocurrencies in India

In 2013, in view of the increasing popularity of an unregulated crypto market, the RBI issued a press release, cautioning the public against dealing in virtual currencies.

In November 2017, the Government of India established a high-level Inter-Ministerial Committee to create a report on the numerous concerns relating to the usage of virtual currency. On April 6, 2018, despite the fact that the Inter-Ministerial Committee's report was still pending, the RBI issued a circular *prohibiting* all commercial and cooperative banks, small finance banks, payment banks, and Non-Banking Financial Companies (**NBFCs**) from not only engaging in their own virtual currency trading,[9] but also from providing services to any organisation that engages in such trading. Thereafter, the 2019 Committee Report recommended a complete ban on private cryptocurrencies in India.

From a regulatory perspective, the measure was borne out of safety concerns – the need to prevent potential misuse due to ambiguities and the anonymised nature of virtual assets, which can be used to support illicit financial activity.

The RBI circular was perceived by cryptocurrency industry stakeholders as violative of their right to conduct trade and practice any profession. Since the activity was not patently illegal or opposed to public policy, the stakeholders argued before the Supreme Court that the State and the regulators ought to introduce regulatory framework to safeguard the investors, consumers, and the industry itself.

In early 2020, the Supreme Court overturned the RBI ban and reinstated cryptocurrencies and their usage in India.[10] The Court predominantly examined the matter from the perspective of Article 19(1)(g) of the Indian Constitution, which specifies the freedom to practice any profession or carry out any occupation, trade or business, and the doctrine of proportionality.[11] The Hon'ble Supreme Court held as follows:

"It is clear from the above that the governments and money market regulators

[8] *Chapter 1: Macrofinancial risks*, RESERVE BANK OF INDIA (December 29, 2021), available at: Reserve Bank of India - Reports
[9] *Prohibition on dealing in Virtual Currencies (VCs)*, RBI (April 6, 2018), available at: Reserve Bank of India
[10] Internet and Mobile Association of India v. RBI, (2020) 10 SCC 274
[11] *The Legality of Cryptocurrency in India*, LEGAL500 (April 19, 2021), available at: The legality of Cryptocurrency in India – Legal Developments

throughout the world have come to terms with the reality that virtual currencies are capable of being used as real money, but all of them have gone into the denial mode (like the proverbial cat closing its eyes and thinking that there is complete darkness) by claiming that virtual currencies do not have the status of a legal tender, as they are not backed by a central authority. But what an article of merchandise is capable of functioning as, is different from how it is recognized in law to be. It is as much true that virtual currencies are not recognised as legal tender, as it is true that they are capable of performing some or most of the functions of real currency."

The Central Government has stated that *" [it] does not consider crypto-currencies legal tender or coin and will take all measures to eliminate use of these crypto-assets in financing illegitimate activities or as part of the payment system"*.[12] This was in line with the Government's sentiment of introducing its own digital currency, which the RBI would issue, but not allow any currency run by another organisation become legal tender. In July 2022, the Finance Minister, too, had remarked that effective regulation of cryptocurrencies requires international collaboration to prevent regulatory arbitrage.[13]

Current Status: Cryptocurrencies are not recognised as legal tender in India, but are legal to hold and trade. There is no specific licensing regime for crypto operators. The regulatory environment remains a grey area with ongoing debates, balancing innovation, investor protection, and concerns over misuse.

India's legal stance on cryptocurrency has transitioned from an outright banking ban to a regulated, but non-legal tender status, with taxation and anti-money laundering compliance frameworks in place, while the government continues to deliberate on a comprehensive legislation.

3. Legal Framework in India

a. Anti-money laundering regulations

Currently, there is no regulation governing or forbidding the transmission of Virtual Digital Assets (**VDAs**), aside from the several RBI circulars instructing companies regulated by it — i.e., Regulated Entities — to carry out necessary checks, in accordance with applicable law. The RBI circular dated May 31, 2021,

[12] *Ministry of Finance, Lok Sabha Unstarred Question No. 2138*, GOVERNMENT OF INDIA, LOK SABHA (August 2, 2021), available at: AU2138.pdf

[13] *Cryptocurrency: RBI seeks ban, but India needs global support to regulate it, says FM Nirmala Sitharaman* LIVEMINT (December 14, 2022), available at: India want to regulate crypto, needs global support: FM | Today News

which is currently in effect, allows Regulated Entities to deal in VDAs such as cryptocurrencies, so long as they comply with the existing Know Your Customer (**KYC**), AML and countering the financing of terrorism (**CFT**) requirements.[14]

On April 28, 2022, the Indian Computer Emergency Response Team (**CERT-In**) issued directions under Section 70B of the Information Technology Act, 2000.[15] These directives require that business entities follow the Customer Due Diligence process as prescribed in the RBI's KYC Master Direction of 2016, as updated from time to time.

To combat the growing money laundering cases using cryptocurrency, the Ministry of Finance issued a gazette notification in March 2023, which brought the trading of cryptocurrency and other VDAs within the ambit of PMLA, imposing domestic anti-money laundering standards.[16] The following nature of transactions have been brought under the ambit of the PMLA:

i. Exchange between VDAs and fiat currencies.

ii. Exchange between one or more forms of VDAs.

iii. Transfer of VDAs.

iv. Safekeeping or administration of VDAs or instruments enabling control over VDAs.

v. Participation in and provision of financial services related to an issuer's offer and sale of a VDA.

The Notification has further classified entities dealing with transactions as 'reporting entity' under the PMLA, which must comply with the PML Rules. Section 2(1)(wa) of the Act defines a reporting entity to include '*banking company, financial institution, intermediary or a person carrying on a designated business or profession*'. By classifying VDA service providers as 'reporting entities' under the PMLA, the notification has imposed compliance requirements as outlined in the PMLA Rules. As defined under Section 2(1)(wa) of the Act, these 'reporting entities' must maintain transaction records, report suspicious activities, and perform KYC. Non-compliance can result in potential fines of up to INR 1,00,000. Failure by a VDA service provider to register itself as a reporting entity is also considered non-

[14] *Customer Due Diligence for transactions in Virtual Currencies (VC)*, RBI (May 31, 2021), available at: Reserve Bank of India - Notifications
[15] Nishchal Anand et al., *Blockchain & Cryptocurrency Laws and Regulations*, GLOBAL LEGAL INSIGHTS (2022), available at: global-legal-insights-to-blockchain-cryptocurrency-regulation-2022-chapter-austria-rath-kulnigg-tyrybon.pdf
[16] Ministry of Finance, Notification, The Gazette of India, (07 March 2023), available at: 244184.pdf

compliance with the provisions of the PMLA and shall attract action under Section 13(2) of the PMLA.

For KYC, the Securities and Exchange Board of India (**SEBI**) circular dated April 24, 2020,[17] mandated that procedures as amended from time to time must be referred to.[18] The Circular states that "virtual asset service providers", "virtual asset exchange providers" and "custodian wallet providers" must maintain KYC and records of financial transactions for a period of five years. The Circular mandates the cryptocurrency industry to report any and all "*attacks or malicious/ suspicious activities affecting systems/ servers/ networks/ software/ applications related to … Blockchain, virtual assets, virtual asset exchanges …*" within six hours of knowledge of such incident.

It is imperative to appreciate the unique nature of cryptocurrencies. The existing laws are built for compliance in a traditional market setup, but cryptocurrencies are meant to be anonymous, digital, and global. Thus, an effective KYC module must involve identifying each customer and their jurisdiction, thereby necessitating that a company have the compliance capacity to fulfil this higher responsibility.

b. Regulations under FEMA

Cryptocurrencies are intangible and can be bought and sold, transmitted, transferred, delivered, stored, and possessed. Cryptocurrencies are used for various purposes, such as store of value, transfer of value, micropayments, and decentralised applications, therefore, they may be classified as current account transactions under the Foreign Exchange Management Act, 1999 (**FEMA**).[19]

When an Indian resident pays in cryptocurrencies for services rendered and goods sold by a non-resident, such transaction is classified as export of goods under the Foreign Exchange Management (Export of Goods and Services) Regulations 2015, and the Master Directions on Export of Goods and Services. These regulations require the full value of exports to be received through authorised banking channels only and any set-off import payments to be received only through a bank facilitated process, thereby prohibiting cross-border barter transactions. Thus, any cross-border transfer by Indian residents involving cryptocurrency without the

[17] *Clarification on Know Your Client (KYC) Process and Use of Technology for KYC*, SEBI (April 24, 2020), available at: SEBI | Clarification on Know Your Client (KYC) Process and Use of Technology for KYC

[18] *Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet*, MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY (Apr 28, 2022), available at: CERT-In_Directions_70B_28.04.2022.pdf

[19] Vipul Kharbanda, Aman Nair, *Crypto-Assets: A Challenge To India's Strong Exchange Control Laws*, MEDIANAMA (January 10, 2022), available at: Crypto-assets: A challenge to India's strong exchange control laws

use of fiat currency through an authorised banking channel contravenes Export Regulation.

c. Regulations depending upon the nature of Cryptocurrency

The use case of cryptocurrencies can aid in identifying the laws applicable to it. Typically, it is likely to be used as a utility token or a security token.

A utility token's value is usually pegged to the actual monetary value of the goods and services offered on the platform. Utility tokens may assume the role of prepaid payment instruments (**PPIs**) and thus the relevant provisions of the Payment and Settlement Systems Act, 2007, as well as the RBI circulars on PPIs could become applicable. However, this is unlikely because the RBI's Master Direction on Issuance and Operation of Prepaid Payment Instruments', dated October 11, 2017,[20] defines the term *'prepaid payment instruments' as "payment instruments that facilitate the purchase of goods and services, including funds transfer, against the value stored on such instruments."*

The value stored on prepaid payment instruments should be constant and equal to the amount of money paid to the payment system providers. However, the value of cryptocurrencies is always fluctuating and is a function of demand and supply in the cryptocurrency market, reflected through the crypto exchanges.[21] Therefore, it cannot be termed as a 'prepaid payment instrument'.

In case VDAs are treated as commodities or securities that are generally traded in secondary markets, KYC, AML and CFT guidelines issued by SEBI will become applicable. VDAs are currently not included among commodities that can be exchanged.[22] However, industry is of the opinion that SEBI is the ideal body to regulate VDAs in India, which is a view expected to be reflected in the proposed Cryptocurrency and Regulation of Official Digital Currency Bill, 2019.[23]

In 2017, the high-level Inter-Ministerial Committee was constituted to examine virtual currencies, leading to the 2019 Draft Banning of Cryptocurrency and Regulation of Official Digital Currency Bill. However, a banket ban on cryptocurrency transactions vide this Bill was widely criticised. Later, the 2021 SC Garg Committee Report proposed a revised bill, the Cryptocurrency and Regulation of Official Digital Currency Bill, which emphasised an official digital currency under

[20] *Master Direction on Issuance and Operation of Prepaid Payment Instruments*, RBI (November 17, 2020), available at: Reserve Bank of India - Master Directions

[21] Meenal Garg, *A Regulatory Approach to Cross-Border Transactions through Cryptocurrency in India*, SCC ONLINE BLOG (November 23, 2021), available at: A Regulatory Approach to Cross-Border Transactions through Cryptocurrency in India | SCC Times

[22] List of Commodities Notified under SCRA, SEBI (September 28, 2016), available at: SEBI | List of Commodities Notified under SCRA

[23] *Crypto exchanges say Sebi or a new entity, not RBI, should regulate the sector*, MONEYCONTROL (May 18, 2021), available at: Crypto exchanges say Sebi or a new entity, not RBI, should regulate the sector: Report

the RBI's watch and restricted the private ones. As of April 2025, the latest version of the Bill hangs in the balance, adding to the growing uncertainty.[24]

4. Recent Developments in India

The RBI has consistently supported the creation of India's own Central Bank Digital Currency (**CBDC**). The Government proposed to introduce such a Digital Rupee, using blockchain and allied technologies. In 2022, the amendment to the RBI Act expanded the definition of the term 'bank note' to mean a bank note issued by the RBI, whether in physical or digital form, thereby paving the way for the RBI to issue its own CBDC.[25] CBDC allows the RBI to issue an efficient and cost-effective currency management system.[26] As per the RBI, CBDC may be defined as:

"legal tender issued by a central bank in a digital form. It is akin to sovereign paper currency but takes a different form, exchangeable at par with the existing currency and shall be accepted as a medium of payment, legal tender and a safe store of value." [27]

The introduction of CBDC is further supplemented by the Cryptocurrency and Regulation of Official Digital Currency Bill, 2021, which is currently awaiting clearance from Indian Parliament.[28]

5. Analysis of the Legal Framework in Other Jurisdictions

a. The United States of America

The United States is home to the largest number of crypto investors, exchanges, trading platforms, crypto mining firms and investment funds. But different agencies within the US have different understanding of the nature of cryptocurrencies.

The Internal Revenue Service (**IRS**) defines cryptocurrencies as *"a digital representation of value that functions as a medium of exchange, a unit of account,*

[24] Dr. Shikha Dhiman & Abheyshek Jamwal, *The legal landscape of cryptocurrency in India: Challenges and prospects*, International Journal of Law (January 27, 2025), available at: The legal landscape of cryptocurrency in India: Challenges and prospects (lawjournals.org)
[25] Budget 2022-23: Speech of Nirmala Sitharaman, Minister of Finance, GOVERNMENT OF INDIA: UNION BUDGET (February 1, 2022), available at: bs202223.pdf
[26] Summary of Union Budget 2022-23, PRESS INFORMATION BUREAU (February 1, 2022), available at: Press Release:Press Information Bureau
[27] Concept Note on Central Bank Digital Currency, RBI (Oct 7, 2022), available at: CONCEPTNOTEACB531172E0B4DFC9A6E506C2C24FFB6.PDF
[28] Harshit Rakheja, *What does the road ahead for cryptocurrencies look like in India?*, BUSINESS TODAY (December 23, 2021), available at: What does the road ahead for cryptocurrencies look like in India? | Finance Other News - Business Standard

and/ or a store of value"[29] and has issued tax guidance accordingly. Tax has been imposed on exchange, use, and holding of cryptocurrencies, without recognising any specific coin as legal tender. The IRS requires investors to disclose yearly cryptocurrency activity in their tax returns.

For short term gains, profits from a crypto asset, held less than a year, are taxed at the same rate as whichever income tax bracket one is in. Any losses can be used to offset income tax by a maximum USD 3,000. For long-term capital gains, i.e., for crypto assets held longer than a year, the capital gains tax is much lower; 0%, 15% or 20%, depending on income.

The Treasury's Financial Crimes Enforcement Network,[30] the Federal Reserve Board,[31] and the Commodity Futures Trading Commission (**CFTC**),[32] have issued differing interpretations and guidance. The SEC often views many cryptos as securities, the CFTC calls bitcoin a commodity, and the Treasury calls it a currency. To iron out the regulatory differences, the President's Working Group and the Financial Stability Oversight Council will play important roles in the development of the regulatory framework.

---

[29] *Cryptocurrency Regulations by Country*, THOMSON REUTERS (2022), available at: Cryptos-Report-Compendium-2022.pdf
[30] *The Financial Crimes Enforcement Network Proposes Rule Aimed at Closing Anti-Money Laundering Regulatory Gaps for Certain Convertible Virtual Currency and Digital Asset Transactions*, U.S. DEPARTMENT OF THE TREASURY (December 18, 2020), available at: Treasury News Release: The Financial Crimes Enforcement Network Proposes Rule Aimed at Closing Anti-Money Laundering Regulatory Gaps for Certain Convertible Virtual Currency and Digital Asset Transactions | FinCEN.gov
[31] Alexander Lee et al., *Tokens and accounts in the context of digital currencies*, BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM (December 23, 2020), available at: The Fed - Tokens and accounts in the context of digital currencies
[32] CFTC *Staff Issues Advisory on Virtual Currency for Futures Commission Merchants*, CFTC (October 21, 2020), available at: CFTC Staff Issues Advisory on Virtual Currency for Futures Commission Merchants | CFTC

Interestingly, law enforcement agencies such as the Office of Foreign Asset Control have tried to overcome the challenges posed by the virtual nature of cryptocurrencies by hiring firms that specialise in compliance and investigation, by using software that provides access to databases to trace cryptocurrency transactions;[33] and by providing training to its officials. The software analyses the blockchain public ledger of all cryptocurrency transactions and connects it to real world entities to trace the assets and the involved persons.

In recent times, the Trump government has introduced some major changes in the cryptocurrency regime, which might be concerning. In April 2025, the Department of Justice (**DoJ**) released a statement that it looked forward to realising Trump's vision of ending the "regulatory weaponisation against digital assets [cryptocurrency]." This would essentially include decreased prosecution of securities law and Bank Secrecy Act violations. The Securities and Exchange Commission (**SEC**) has dropped multiple cryptocurrency cases, and the National Cryptocurrency Enforcement Team has been discharged by the DoJ.[34] In a shocking turn of events, the SEC has dropped one of the biggest and high-profile cryptocurrency cases that involved enforcement action against the company, Coinbase, wherein it was alleged that the company had failed to fulfil its registration requirements. The SEC's move of stepping away from ongoing enforcement lawsuits and investigations is a clear indication of how the crypto landscape is evolving under the new administration. The main goal is to create a clearer regulatory framework, which inclines towards collaboration rather than penalisation. The SEC is approaching the dynamic nature of the crypto industry with caution, and they will keep a close eye on transactions, but with more breathability for stakeholders.[35]

Compared to India, the US has a more robust regulatory regime. However, it is marked by a variety of different legislations approaching cryptocurrencies in multiple ways, making compliance more taxing and confusing. Like India, the US does not recognise cryptocurrencies as legal tender, however, crypto exchanges are legal and regulated by each state independently.[36] The US Government is likely to pass a uniform federal law to eliminate any confusion on tax and AML rules soon.

---

[33] Dr. Shikha Brett Wolf, *US law enforcers partner with cryptocurrency tracking firm to fight financial crime*, REUTERS (December 23, 2020), available at: US law enforcers partner with cryptocurrency tracking firm to fight financial crime - Thomson Reuters Institute

[34] Andrew Warren, *The Trump Administration's Policies could unleash a wave of white collar crime*, Opinion (April 16, 2025), available at: The Trump administration's policies could unleash a wave of white collar crime

[35] Christopher Bosch, Maxwell Earp-Thomas, *SEC Withdraws from Prominent Enforcement Amid Regulatory Shift*, White Collar & Government Enforcement Blog, Sheppard Mullin (February 28, 2025), available at: SEC Withdraws from Prominent Crypto Enforcement Amid Regulatory Shift | White Collar & Government Enforcement Blog

[36] Lindsey Choo & Benjamin Pimentel, *Crypto's European win is just the beginning of a global regulatory fight*, PROTOCOL (March 15, 2022)

b. The United Kingdom

The UK Revenue and Customs department provides a comprehensive and thorough definition of cryptocurrencies (referred to as crypto assets). An internal manual titled 'Crypto-assets Manual' defines Crypto assets (also referred to as 'tokens' or 'cryptocurrency') as *"cryptographically secured digital representations of value or contractual rights that can be: (i) transferred, (ii) stored, (iii) traded electronically."*[37]

While cryptocurrency exchanges and other businesses offering such services are supposed to be registered with the Financial Conduct Authority (**FCA**),[38] like the US, the UK too, does not have any specific regulations that mandate the disclosure of cryptocurrency and crypto asset holdings by companies in their financial statements (balance sheets & statements of profit and loss). There are currently no guidelines for accounting practices for cryptocurrencies.[39]

The United Kingdom considers cryptocurrencies as capital assets, thus imposing capital gains tax, basis the existing tax slabs with respect to exchange, payment for goods/ services and giving away cryptocurrencies.[40] This is significantly different from India's law being more suited to consider cryptocurrencies as goods. Cryptocurrency activities fall within the scope of the UK Money Laundering Regulations, 2017, since January 2020. Changes currently proposed at the EU level (and supported by the UK Treasury) would bring cryptocurrency exchanges and custodian wallet providers' activities under the scope of AML laws.

Recently, the UK Government announced a revised framework to regulate the crypto industry, which aims to encourage investors as well as protect consumers from scam risks and frauds. The rapid expansion of digital assets has necessitated major platforms such as Bitcoin and Ethereum, which provide services related to crypto assets, to adhere to revised rules. Since 2021, there has been a significant increase in the number of consumers owning crypto assets, which necessitates a clearer regulatory framework that brings crypto exchanges, dealers and agents into its ambit, sieving out the bad actors and facilitating innovation. Customers will also be required to comply with certain obligations that include transparency

[37] *Aryan Gupta, Cryptocurrency in Financial Statements - A Comparative Analysis*, CENTRE FOR INTERNET & SOCIETY (June 14, 2021), available at: A Comparative Analysis of Cryptocurrency Reporting in Financial Statements — Centre for Internet and Society
[38] FCA *establishes Temporary Registration Regime for cryptoasset businesses*, FINANCIAL CONDUCT AUTHORITY, UNITED KINGDOM (December 16, 2020), available at: FCA establishes Temporary Registration Regime for cryptoasset businesses | FCA
[39] Cryptocurrency regulation around the world & how India compares, LIVEMINT (November 8, 2021), available at: Cryptocurrency regulation around the world & how India compares | Mint
[40] Katherine Lemire, *Cryptocurrency and anti-money laundering enforcement*, REUTEURS (September 26, 2022), available at: Cryptocurrency and anti-money laundering enforcement | Reuters

and operational resilience.[41] The UK government has already published a draft legislation on regulated cryptocurrency. It aims to work in collaboration with the US government, which is already dishing out measures that are pro-crypto.[42]

This Regulation details CDD and KYC requirements as is applicable for other businesses and is also similar to India's the regulatory regime. Additionally, VDAs are not classified in the same manner as other securities, like in India. Similar to the US, the UK finds crypto exchanges to be legal and are regulated by the FCA. However, cryptocurrency is not legal tender in the UK either. It is likely that the UK's cryptocurrency regulations will remain largely consistent with the EU.

6. Conclusion and Recommendations

Improving and harmonising cryptocurrency regulations, particularly in areas such as anti-money laundering, customer identification, and consumer protection, can significantly reduce the likelihood and occurrence of white-collar crimes within the cryptocurrency sector. Nonetheless, as technology and criminal methods evolve, regulators must remain alert and ready to adapt their strategies accordingly.

Some essential steps for updating cryptocurrency regulations could be to enforce more robust procedures for verifying user identities and preventing money laundering across cryptocurrency exchanges, wallet services, and token issuers, making it more challenging for criminals to exploit these platforms. Promoting collaboration among countries to develop unified regulatory standards, helping to eliminate gaps that criminals might use when crossing national boundaries can be used to combat cross-border crimes. It is important to mandate that cryptocurrency businesses monitor transactions in real time and report any suspicious activities, mirroring the practices required in conventional financial institutions. It is essential to apply the same regulatory oversight to stablecoin issuers and crypto exchanges, as is applied to traditional banks and financial service providers, thereby promoting transparency, safeguarding consumers, and ensuring system stability. This can be done by deploying tools such as blockchain analytics and artificial intelligence to spot and stop questionable transactions and uncover patterns linked to laundering and fraudulent schemes.

[41] HM Treasury, The Rt Hon Rachel Reeves MP, *New cryptoasset rules to drive growth and protect consumers*, GOV.UK (April 29, 2025), available at: New cryptoasset rules to drive growth and protect consumers - GOV.UK

[42] digwatch, Geneva Internet Platform, *UK and US join forces to promote responsible cryptocurrency adoption* (April 30, 2025), available at: UK and US join forces to promote responsible cryptocurrency adoption | Digital Watch Observatory

G

Legal Privilege and Investigations

1. Introduction

The legal privilege or the attorney-client privilege is often regarded as the crown jewel of the legal profession. It provides protection from disclosure of communications between an attorney and a client seeking legal advice.

Due to this privilege protection clause, an advocate cannot divulge details of any communication, without the express permission of the client. This protection privilege is for the client and not the attorney. Legal privilege safeguards an individual's right to access justice by encouraging an open and complete discussion between an attorney and a client, who is not only shielded from disclosure of such communication, but can also claim subsequent prejudice due to the disclosure.

The earliest known instance of the principle of legal privilege in English common law dates back to 1577. In *Berd v. Lovelace*[1], the court had refused to compel the attorney to depose against his client. The position was further cemented in *Greenough v. Gaskell*[2], where lord Brougham observed that in the absence of privilege, a client would not be able to fully disclose the facts to his attorney, which in turn would hinder his ability to seek legal advice.

2. Legal Position in India

Under the Bharatiya Sakshya Adhiniyam, 2023 (**BSA**), any professional and confidential communication with the legal advisor is protected. Sections 132 to 134 of the BSA (previously, Sections 126 to 129 of the Indian Evidence Act, 1872 (**IEA**)) codify the common law principles of privileged professional communication between an attorney and the client. It can be essentially summarised to say that any professional communication to an attorney, made for the purpose of seeking legal advice, would be protected. In India, any person who seeks advice from a practicing advocate, registered under the Advocates Act, 1961, would have the benefit of legal privilege and his/ her communication would be protected under the provisions of the BSA.

The Hon'ble Bombay High Court, in *Cecilia Fernandes v. State*[3], held that the right to personal liberty, provided under Article 22(1) of the Constitution of India, can be

[1] *Berd v Lovelace*, (1577) Cary 62
[2] *Greenough v Gaskell*, (1833) 39 ER 618
[3] Cr. Misc. Application No. 9 of 2005, see also; *Moti Bai v. State* 1954, CriLJ 1591

meaningfully exercised only in confidence. Therefore, a police officer cannot insist on standing at such a distance from the accused that would hinder the accused from freely instructing his lawyer in confidence. The Court acknowledged that the right to legal representation should not be obstructed by procedural delays, which would otherwise render the fundamental right infructuous. Through this judgement, the Court reiterated the necessity to uphold the constitutional rights of accused individuals, professional duties advocates are required to fulfill and procedural integrity the judicial process is required to carry. The interpretation of the term 'legal privilege' in India is severely diluted, especially in terms of enforcement investigation. Investigative agencies, in such cases, have access to certain documents that might be objectively considered confidential.

While the erstwhile IEA applies broadly to "barristers, pleaders, attorneys, or vakils" and outlines the confidentiality of client communications made during "professional employment", with just exceptions, the newly enacted BSA focuses on "advocates" specifically and uses the term "professional service" instead of "professional employment".

The Union Ministry of Law and Justice released the draft Advocates (Amendment) Bill, 2025, which aimed to expand the term '*legal practitioner*' to include not only advocates practicing in courts, but also corporate lawyers, in-house counsels, and individuals involved in legal work in private and public organizations, statutory bodies, and international law firms. However, the draft Bill has now been withdrawn due to widespread protests and strong opposition.[4]

An attorney, without the express consent of the client, cannot disclose any communication made by the client, on behalf of such client, during or for the purpose

[4] THE HINDU, *The contentious amendments to the Advocates Act and their implications*(March 5, 2025), available at: The contentious amendments to the Advocates Act and their implications - The Hindu

of his/ her engagement as such attorney. Furthermore, an attorney cannot state the contents or conditions of any document he/ she may have become acquainted with, during his/ her engagement as an attorney or disclose the advice provided to the client.

However, the privilege is subject to limitations. It no longer applies if the disclosures are made with the express consent of the client, or where the communication is made in furtherance of any illegal purpose or where, post his/ her engagement, the attorney discovers or observes a fact that a crime was committed, or a fraud was perpetuated. It is immaterial whether or not the attention of the attorney was or was not directed to such a fact, by or on behalf of the client.

Section 132(3) of the BSA expands the scope of privilege provided under Section 132(1) and Section 132(2), by imposing a similar duty on interpreters, clerks and servants of the advocate. Section 133 of the BSA provides that an attorney cannot disclose any information, which is deemed privileged under Section 132(1), unless the client calls upon the legal adviser as a witness and questions him on the same. Furthermore, Section 134 of BSA lays down that a client or attorney cannot be compelled to disclose to the court any confidential communication, which has taken place between the client and his legal professional advisor, unless he offers himself as a witness. In such a scenario, the attorney may be compelled to disclose any communication as deemed necessary by the court to explain any evidence provided by him/ her, but no other. The Hon'ble Calcutta High Court, in *Sudha Sindhu v. Emperor*[5], held that all communications between an accused person or indeed any litigant and his legal advisors are privileged and confidential.

Courts in India have further clarified on the issue of legal privilege by holding, *inter alia*, that to claim privilege under Section 132 of BSA, (previously Section 126 of the IEA), a communication by a party to his/ her pleader must be confidential.[6] However, privilege does not extend to communications prior to the creation of attorney-client relationship.[7]

Further, in India, the work-product doctrine or the work-product privilege, which protects any tangible or intangible document created in anticipation of litigation, has been upheld. The Bombay High Court, in Larsen & Toubro Ltd v Prime Displays (P.) Ltd.[8], while deciding a winding up petition filed by the respondents against the petitioner company, held in favour of the petitioner company that attorney-client work in anticipation of litigation is entitled to protection under Sections 132 to 134 of

[5] *Sudha Sindhu v. Emperor* (AIR 1935) Cal 101
[6] *Memon Hajee Haroon Mohomed v. Abdul Karim*, [1878] 3 Bom 91
[7] *Kalikumar Pal v. Rajkumar Pal*, 1931 (58) Cal 1379, Para 5
[8] *Larsen & Toubro Ltd v Prime Displays (P) Ltd.*, [2003] 114 Comp Cas 141 (Bom)

BSA. All documentation created (whether tangible or intangible) and communication between a client and an attorney in anticipation of litigation will be privileged communication, including any communication for the purpose of securing advice for the litigation; for obtaining or collecting evidence to be used in the litigation; and for obtaining information that will lead to such evidence, drafts of notices, pleadings and so forth, exchanged between the attorney and the client.

Unlike the legal privilege, which generally refers to communications between an attorney and a client, the work-product doctrine extends to materials prepared by individuals other than the attorney, provided that these materials were prepared for ongoing or potential litigation.[9] This goes on to show that attorney work-product doctrine covers a more comprehensive track than legal privilege.

In addition to the provisions under BSA, professional communication between a legal advisor and a client is accorded protected status under the Advocates Act, 1961, and the Bar Council of India rules (the **BCI Rules**). The BCI Rules, Part VI, Chapter II, Rule 17 stipulates that *"an advocate shall not, directly or indirectly, commit a breach of the obligations imposed by Section 126 of the Evidence Act."* In addition, Rules 7 and 15 of the BCI Rules talk of an advocate's duty towards a client and state that communication between the client and the attorney cannot be disclosed by the attorney, in any manner whatsoever, and that an advocate should not take advantage or abuse a client's confidence.[10] Violation of these rules would subject the attorney to disciplinary proceedings.

With respect to an in-house counsel, the legal position was clarified by the Hon'ble Supreme Court in *Satish Kumar Sharma v. Bar Council of Himachal Pradesh*[11], wherein, the Hon'ble Supreme Court held that:

> *"...if a full-time employee is not pleading on behalf of his employer, or if terms of employment are such that he does not have to act or plead but is required to do other kinds of functions, then he ceases to be an advocate. The latter is then a mere employee of the government or the body corporate".*

The judgment also referred to Rule 49, Section VII, Chapter II, Part VI of the BCI Rules, stating that:

> *"an advocate shall not be a full-time salaried employee of any person, government, firm, corporation or concern, so long as he continues to practice and shall, on taking up any such employment intimate the fact to the bar*

[9] *Woolley v North London Railway*, (1868-1869) LR 4 CP 602
[10] The Bar Council of India, Rules on Professional Standards, Rule 7 and Rule 15, available at: Rules on an Advocate's Duty Towards the Client | Bar Council of India
[11] *Satish Kumar Sharma v. Bar Council of Himachal Pradesh*, AIR 2001 SC 509

> *council on whose roll his name appears, and shall thereupon cease to practice as an advocate so long as he continues in such employment. An advocate cannot be a full-time salaried employee. The only exception is if the person is a law officer of the Central Government of a state or of any public corporation entitled to be enrolled in the bar."*

In *Municipal Corporation of Greater Bombay v. Vijay Metal Works*[12], the Hon'ble Bombay High Court held that:

> *"a salaried employee who advises his employer on all legal questions and also other legal matters would get the same protection as others, viz., barrister, attorney, pleader or vakil, under Sections 126 and 129, and, therefore, any communication made in confidence to him by his employer seeking his legal advice or by him to his employer giving legal advice should get the protections of Sections 126 and 129."*

Thus, in India, to qualify as privileged, communications between clients and in-house attorneys must be evaluated based on whether the inhouse counsel is an employee[13] or retained to provide legal advice to the company. Further, determining whether the advice sought is in legal or executive capacity would be a key distinguishing factor.

3. Privilege during Internal Investigations

Internal investigations pose a great challenge in terms of preserving legal privilege due to the sheer size and involvement of a wide nature of non-legal parties. The objective of an internal investigation is to understand the scope of the issue, remediate the problem, and to formulate a suitable response to regulators, government authorities or investigative agencies in one's own or a foreign jurisdiction, as the case may be. Maintaining legal privilege is paramount in the context of an investigation. It is essential to structure and conduct the internal investigation in a manner that maximizes the legal privilege available within the specific jurisdiction. It is imperative to note that in many jurisdictions worldwide, legal privilege often does not extend to communications with in-house counsel, and hence it may not be protected by attorney-client privilege.

It is advisable for corporations or clients in the process of commencing an internal investigation to engage an external attorney or law firm at the outset and ensure that the investigation is carried out at the direction of the attorney. It is

[12] *Municipal Corporation of Greater Bombay v. Vijay Metal Works*, AIR 1982 Bom 6
[13] Rule 49, Section VII, Chapter II, Part VI of BCI Rules

recommended to create and preserve written records, demonstrating the purpose behind the investigation and the legal advice sought in connection with the anticipated litigation, if any. The records should show that key decision-makers at the company are part of the client group to ensure clarity regarding the applicability of privilege to communications between the client and the attorney.

While creating written reports of the investigation or witness interviews, the distinction between ordinary work-product and opinion work-product must be kept in mind. It would be wise to consider the possibility of having to disclose written reports due to divergence and variation in the scope and nature of protection under privilege laws in other jurisdictions, where the company may face potential litigation or enforcement action.

The company as well as the attorney must take steps to avoid any inadvertent waiver, by ensuring that the investigation and any related documents or reports are treated as confidential, limiting disclosure to the investigation team.

4. Privilege during Investigations under the Prevention of Money Laundering Act and Prevention of Corruption Act

a. Investigative powers under Prevention of Money Laundering Act

Under the Prevention of Money Laundering Act, 2002 (**PMLA**), the Directorate of Enforcement has been given wide powers to conduct searches and seizures when it suspects someone has engaged in any act constituting money laundering or is in possession of records, property, or proceeds of crime connected to money laundering.[14] An application or complaint must be made to the Adjudicating Authority, which has been established to exercise jurisdiction, powers, and authority granted by or under the PMLA, if any property or document is attached or confiscated. Typically, a criminal court or a special court, set up for this purpose, is appointed and vested with the powers of the Adjudicating Authority under the PMLA. Under Section 8 of the PMLA, the Adjudicating Authority can serve a notice if it suspects money laundering or possession of proceeds of crime. The notice requires the person to specify the sources of their income, earnings, or assets used to acquire the seized, attached, or frozen property and provide supporting evidence.

[14] Prevention of Money Laundering Act 2002, Section 17, Prevention of Money Laundering Act 2002, Section 18

For the purposes of the PMLA, an adjudicating authority has been vested with powers akin to that of a civil court under the Code of Civil Procedure, 1908 (**CPC**). These include, among other things, the right to discovery and inspection, the right to order the production of documents, the right to hear evidence based on affidavits, the right to require attendance of any person, etc.

b. Investigative powers under the Prevention of Corruption Act

Section 9 of the Prevention of Corruption Act, 1988 (**PCA**), stipulates that if a commercial organisation provides or promises to provide a public servant any undue advantage in exchange for obtaining/ retaining a business or a business advantage, the person in charge of the organisation, who authorized the undue advantage, shall be punishable with imprisonment of three years, extendable to seven years with fines.

c. Legal Privilege during Search and Seizure

Legal privilege does not protect against compulsory disclosures, such as search warrants or discovery requests by enforcement agencies. However, an exception lies in the Companies Act, 2013 (**Companies Act**), which recognises privilege in the context of an investigation by the Serious Fraud Investigation Office (**SFIO**) into offences of corporate fraud.

It would be immaterial whether the documents are held by the client or the attorney. In 2019, law firms and consultants reportedly received notices from

the SFIO under Section 217(1) of the Companies Act, requesting them to reveal information regarding debt-ridden Infrastructure Leasing and Financial Services (IL&FS). Failure to comply, would result in consequences under Section 217(8) of the Companies Act.[15] Furthermore, in 2021, a Public Interest Litigation filed for regulating search and seizure on an advocate's premises, in light of privilege, was dismissed by the Hon'ble Delhi High Court. It was stated that the Code of Criminal Procedure, 1973 (**CrPC**), had adequate safeguards relating to search and seizure.[16] Therefore, it may be inferred that legal privilege has limited application in the face of search and seizure warrants by enforcement agencies.

d. Legal Privilege during an Internal Investigation in anticipation of raid under PMLA or PCA Act

If a company receives any information about the possibility of an ED raid or an investigation (of a commercial organisation) for violation of Section 9 of the PCA, it might conduct an internal investigation to assess the liability that might be accrued, and the persons associated with the alleged wrongdoing. In such a scenario, there may be documents prepared and/ or advice sought from in-house or external counsel with respect to anticipated litigation. Such documents or communication exchanged between a client and an attorney in anticipation of litigation will qualify as privileged communication.[17]

Depending on the facts and circumstances, privilege may be attached to some aspects of the internal investigation. Legal advice sought or obtained regarding investigation, lawyers' notes taken during an investigation, and communications or documents prepared primarily for litigation are generally protected under legal privilege, provided litigation is ongoing or reasonably anticipated.

Legal privilege, however, does not extend to letters exchanged between employees, pertaining to information that could potentially become useful to their attorney,[18] or to statements made by an employee regarding the subject matter of the suit proceedings that were not intended to be submitted to their attorney.[19] It is for this very reason that counsels assisting with the investigation must identify the relevant form of privilege and devise a strategy to ensure that the organisation

[15] ET NOW, *SFIO sends notices to top law firms, consultants to reveal all information related to IL&FS*(October 9, 2019), available at: ILFS Crisis: SFIO sends notices to top law firms, consultants to reveal all info related to debt-laden IL&FS | Business News
[16] Akshita Saxena, *No Adverse Presumption Against Investigation Agency: Delhi High Court Dismisses Plea To Regulate Search & Seizure Operations On Advocates' Premises* (October 6, 2021), available at: No Adverse Presumption Against Investigation Agency: Delhi High Court Dismisses Plea To Regulate Search & Seizure Operations On Advocates' Premises
[17] *Larsen & Toubro Limited v. Prime Displays Pvt. Ltd., Abiz Business Pvt. Ltd. and Everest Media Ltd* (2003) 105(1) BomLR 189
[18] *Bipro Doss Dey v Secretary of State for India in Council* (1885) ILR 11 Cal 655
[19] *The Central India Spinning Weaving and Manufacturing Co Ltd v G I P Railway Co,* AIR 1927 Bom 367

can take advantage of privilege and protect itself from making unnecessary or damaging disclosures, before embarking on the search for documents and evidence.

In civil cases, a party may refuse to produce certain documents on grounds of attorney-client privilege, when the opposing party requests discovery under the CPC. However, attorney-client privilege over documents or communications is inapplicable if a judge issues summons in a criminal proceeding under Section 94 of the BNSS (previously, Section 91 of the CrPC). Section 145 of the BNSS (previously, Section 126 of the CrPC) does not place any restrictions on the ability to issue notices under Section 94.

5. Preserving and Protecting Privilege: Best Practices

Privilege applies only to communications where an attorney's role is primarily to render legal advice or assistance. While determining applicability of privilege, the following factors are deemed relevant:

i. The context of the communication and the content of the document;

ii. Preservation of information;

iii. Whether the legal purpose permeates the document and can be separated from the rest of the document;

iv. Whether legal advice is specifically requested and the extent of the recipient list; and

v. Best practices in the age of virtual interactive platforms.

Furthermore, to determine legal professional privilege between in-house counsel and corporate employees, United Kingdom (**UK**) courts have adopted two methods: one, the control group test, and two, the subject matter test. Under the first approach, communication from individuals outside the control group (i.e. the officers authorised to seek legal advice or control the legal affairs of a company) is not protected. Under the subject matter test, privilege is limited to communication from corporate employees for the specific purpose of securing legal advice for the corporation. Communication with an in-house counsel in relation to business as opposed to legal advice may not be protected by privilege.

In a recent decision, the UK Court of Appeal confirmed that legal advice privilege is subject to a 'dominant purpose' test. In doing so, the court has confirmed that legal advice and litigation privilege are two limbs of the same privilege, and similar

considerations apply.[20] Simply put, for legal advice privilege to apply, the dominant purpose of communication must be to obtain, or give, legal advice.

Many communications are presumed privileged, such as those in which "attorneys are examining and commenting upon a legal instrument, like a patent application, contract for a study, or retention of experts." In view of this, it is recommended that:

i. While seeking legal advice, it must be clarified at the outset that the communication is for the dominant purpose of "seeking legal advice" or "for the purpose of providing legal advice", as such statements assist in substantiating claims of legal professional privilege.

ii. Irrespective of the platform or mode, while providing legal advice to a client, attorneys must document the communication as 'legal privileged' and provide legal support for any advice provided.

iii. It is advisable to clarify that any non-legal business issues or documents are provided or discussed separately, and the purpose of the said communication is to seek or provide legal advice.

iv. Where the client is a large organisation or a company comprising legal and non-legal staff, the presence of non-legal staff or those outside the control group on attorney communications may undermine the privilege. Therefore, it is advisable to limit access to such communication only to those legal and non-legal team members, with direct connection to the said legal matter.

v. In addition, labelling the communication with 'do not forward' and instructing the team involved to limit circulation of the communication is recommended.

It is highly recommended that companies while conducting internal investigations strive to protect privilege at the outset, so as to retain the flexibility to decide later whether and to what extent a privilege waiver is advisable. An internal investigation structured to maximise legal privilege will allow the company greater control over how and when to disclose the relevant information.

Although there is a legal obligation to disclose inquiry findings during litigation, these findings can be safeguarded by appropriately asserting and maintaining privilege over all or parts of the investigation. However, it is critical to comprehend the scope of privilege as well as its application in the context of internal investigations. There is a balance to be struck between a full and proper investigation, and the need to protect legal rights through privilege, which can pose

[20] *The Civil Aviation Authority v Jet2.Com Ltd, R. (on the Application of Jet2.com Limited),* [2020] EWCA Civ 35

difficulties and present hard choices when faced with an investigation. Counsel assisting with investigations need to be aware of the best ways to organise their internal investigations to maintain privilege, without flouting the principles established in case law. It is important to correctly identify and mark documents as privileged and confidential.

Key Contacts

Cyril Shroff
Managing Partner
cyril.shroff@cyrilshroff.com

Faraz Alam Sagar
Partner (Co-Head - White Collar & Investigations)
faraz.sagar@cyrilshroff.com

Contributors

Faraz Alam Sagar
Partner (Co-Head - White Collar & Investigations)

Pallavi Choudhary
Principal Associate

Kinjal Sharma
Associate

Aditi Goyal
Associate

Irene Sarkar
Associate

Offices of Cyril Amarchand Mangaldas

mumbai

Peninsula Chambers,
Peninsula Corporate Park,
GK Marg, Lower Parel,
Mumbai – 400 013, India
T: +91 22 6660 4455 F: +91 22 2496 3666
E cam.mumbai@cyrilshroff.com

bengaluru

3rd Floor, Prestige Falcon Tower,
19, Brunton Road, Off M G Road,
Bengaluru – 560 025, India
T: +91 80 6792 2000
E cam.bengaluru@cyrilshroff.com

chennai

11th Floor, Awfis, Prestige Palladium Bayan,
No.43/1 (Door No.129 to 140), Greams Road, Egmore,
Chennai – 600 006
T: +91 44 4904 2874
E: cam.chennai@cyrilshroff.com

gift city

Office No. 501, 5th Floor, PRAGYA 2 Tower,
Road No. 11, GIFT SEZ area, GIFT City,
Gandhinagar – 382 355, Gujarat.
T: +91 79 6959 3500
E: cam.ahmedabad@cyrilshroff.com

abu dhabi

2459, Al Sila Tower, Abu Dhabi Global Market Square,
Al Maryah Island, Abu Dhabi, United Arab Emirates
(CAM Middle East)
E: cam.abudhabi@cyrilshroff.com

delhi-ncr

Level 1 & 2, Max Towers,
C-001/A,Sector 16 B,
Noida – 201 301,
Uttar Pradesh, India
T: +91 120 669 9000 F: +91 120 669 9009
E cam.delhi@cyrilshroff.com

ahmedabad

Block A-1512, 15th Floor, Navratna Corporate Park,
Ambli Bopal Road, Bodakdev,
Ahmedabad – 380 058, India
T: +91 79 3503 9999
E: cam.ahmedabad@cyrilshroff.com

hyderabad

Ground Floor, AWFIS Ohris Tech Park, Plot No.13,
Survey 64/2, (New) Software Units Layout, Madhapur,
HiTech City, Hyderabad – 500 081, India
T: +91 40 4433 4323
E cam.delhi@cyrilshroff.com

singapore

61 Robinson Road,
#11-03, Singapore – 068 893
T: +65 6329 2260
E cam.singapore@cyrilshroff.com
(CAM Singapore Pte Ltd., UEN: 202137213R)

www.cyrilshroff.com

www.cyrilshroff.com/blogs


INVESTIGATION


RULES
REGULATIONS