cyril amarchand mangaldas
ahead of the curve

Investigations and White Collar Crimes Enforcement Trends

A Cyril Amarchand Mangaldas Thought Leadership Publication

Disclaimer:

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

This handbook has been updated till January 20, 2023.

This handbook is not intended to be used as the basis for trading in the shares of any company or for undertaking any other complex or significant financial transaction without consulting appropriate professional advisers. No part of this publication may be copied or redistributed in any form without the prior written consent of Cyril Amarchand Mangaldas.

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 expected to become the third-largest economy in the world, beating Japan and Germany, on the back of investment boost to the manufacturing sector, energy transition, rising per capita income, advanced digital infrastructure, a burgeoning middle class, and strengthening trade ties with global economies, among others, according to many research reports. At USD3.5 trillion, the Indian economy is already the fifth largest. It is further expected that by 2050, twenty percent (20%) of the global GDP will come from India. In the post-Covid-19 world, India is poised to become a *de facto* and *de jure* world leader.

India is one-sixth of the world. Therefore, when India grows, the world grows. When India reforms, the world transforms.

Shri Narendra Modi, the Prime Minister of India

At the intersection of the rule of law and progressive capitalism, the renewed impetus on sustainability and Environmental, Social and Governance ("**ESG**") accountability is a manifestation of the new, more holistic and inclusive social contract. Similar to the European Union's recently adopted Sustainable Finance Disclosure Regulations; the Securities and Exchange Board of India ("**SEBI**") has mandated Indian listed companies to include a Business Responsibility and Sustainability Reporting section in their annual reports, initiating an era of accountability, environmentally and socially conscious business practice in India. While the Indian ESG reporting and regulatory framework is still in its nascent stages, it will only grow from here and broaden its reach.

As part of the country's global commitments announced at the 27th Conference of the Parties to the United Nations Framework Convention on Climate Change ("**COP27**"), India's renewable energy initiatives find further gravitas in the Energy Conservation (Amendment) Bill 2022. The Amendment proposes to introduce a carbon trading scheme, requiring consumers to meet a proportion of their energy needs from non-fossil sources, as well as set out energy consumption standards for automobiles, and codes for residential and commercial properties.

The Constitution and Supreme Court of India have a seminal role to play qua these factors, in addition to ensuring the certainty and consistency of our commercial laws. It is also interesting that some of the deepest issues on constitutional law and the most hard-fought constitutional principles have evolved in the context of issues of economic rights and liberties. In 2022, the Supreme Court of India decided on widely contested constitutionality issues raised by the Indian anti-money laundering legislation. The Supreme Court's decision concurs with the investigative and enforcement powers of the authorities under the legislation. The decision further cements the

critical provisions pertaining to search and seizure, arrest, and most importantly, attachment of assets. Globally, financial markets have witnessed significant ups and downs in the cryptocurrency and virtual asset industry, and their unprecedented impact on the development of law and challenge to law enforcement authorities. The year also witnessed attachment of virtual currency in India, initiating a discourse on the regulation of virtual assets that tests the existing paradigms of our laws.

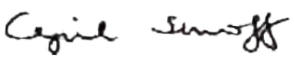
The Digital Personal Data Protection Bill, 2022, adds another layer of compliance and data protection considerations for financial institutions, required to monitor financial activity under the anti-money laundering laws. These developments require the regulatory and enforcement frameworks to adapt and remain flexible to the increasingly digitised future, while bolstering internal governance and compliances.

The changes will force all stakeholders to adapt to the developments, develop a futuristic outlook, and adopt sustainable practices in their management and operations. Ease of doing business has been at the core of India's economic policy development, along with ensuring compliance with international norms, which domestic players as well as foreign entrants have to adhere to. Sanctions and trade controls, in response to recent geopolitical developments, further alter the dynamics of law and enforcement, especially with the Reserve Bank of India introducing settlement of international trade in Rupees. This also marks a step towards a more inclusive international financial system, allowing for stressed economies to access international markets through the rupee alternative. The world today needs to be more inclusive, resilient, and focused on sustainability. Our policies need to be reoriented, reimagined for a better world.

In order to understand the seismic shifts in India's compliance, enforcement, and regulatory landscape and as part of the Cyril Amarchand Thought Leadership Initiative, we have compiled essays on trends in enforcement and investigation of white-collar crimes in India, the fundamentals of the legal framework and the direction in which the development of the legal framework appears to proceed. In the production of this book, I must appreciate the efforts of the contributors who have worked very hard to produce it.

I hope you will find this an informative read. We welcome your feedback and comments for our future editions.

Thank you,



Cyril S. Shroff
Managing Partner
Cyril Amarchand Mangaldas
cyril.shroff@cyrilshroff.com
January, 2023

Content

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 reports, and corporate governance systems, etc. One of the key amendments is the constitution of RMC for a larger number of listed entities (from top 500 to top 1000)[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, the SEBI, to prevent crimes in trading, 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] The MIIs have to formulate a code of conduct to regulate, monitor and report trading by designated persons and their immediate relatives. The administration is to be conducted by a compliance officer.[5] Furthermore, MIIs are required to establish an institutional mechanism for precluding fraud or market abuse by the MIIs themselves, their designated persons and such immediate relatives, coupled with internal controls and whistle-blower policy.[6]

On similar lines, the Central Vigilance Commission ("**CVC**") restructured the advisory board of its department of 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 Indian Rupees ("**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**").[7] 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.[8]

---

[1] *Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) (Second Amendment) Regulations*, SEBI, (May 5, 2021), https://www.sebi.gov.in/legal/regulations/may-2021/securities-and-exchange-board-of-india-listing-obligations-and-disclosure-requirements-second-amendment-regulations-2021_50100.html.

[2] *Id.*

[3] *Id.*

[4] *Code of Conduct & Institutional mechanism for prevention of Fraud or Market Abuse*, SEBI, (March 3, 2021), https://www.sebi.gov.in/legal/circulars/mar-2021/code-of-conduct-and-institutional-mechanism-for-prevention-of-fraud-or-market-abuse_49374.html.

[5] *Id.*

[6] *Id.*

[7] Prevention of Corruption Act, 1988, Section 17A.

[8] *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), https://persmin.gov.in/.

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 to five years from two.[9] Lastly, by an August 2021 notice, SEBI empanelled 16 entities, including Binder Dijker Otte India, Ernst & Young and Deloitte Touche Tohmatsu India, to conduct forensic audits of listed companies.[10]

2. Recent Judicial Decisions

a. Anti-Corruption

Recently, the Hon'ble Supreme Court in *Neeraj Dutta v State (Govt of NCT Delhi)*,[11] settled the debate on whether the demand and acceptance of illegal gratification by a public servant can be proved by circumstantial evidence in the absence of direct evidence due to the passing away of the complainant or his or her failure to support the prosecution case. While explaining the difference between direct and indirect evidence, the Hon'ble Supreme Court stated that direct evidence proves something is real, either by direct production or through the testimony or verifiable declaration of someone who has personally experienced it and believed that it established a fact in issue. Direct evidence establishes the existence of a fact in issue without the use of any inference or presumption. On the other hand, indirect evidence or circumstantial evidence gives rise to the logical inference that such a fact exists, either conclusively or presumptively.

Addressing the issue, the Constitution Bench held that in the absence of evidence by the complainant or direct or primary evidence of demand of illegal gratification, it is permissible to draw inferential deduction of culpability or guilt of a public servant under Section 7 and Section 13(1)(d), read with Section 13(2) of PCA, based on other evidence adduced by the prosecution. The Hon'ble Supreme Court observed that if it was established that there was a demand for, payment of, or acceptance of gratification and that the fundamental circumstances had been established, then presumption of payment or acceptance of illicit gratification was relevant, provided that it was not refuted. Accordingly, then under Section 20 of PCA, legal presumption was to be derived from the said gratification that was acknowledged as a "motivation or reward" for performing or refraining from performing any act. Therefore, in the instant case, circumstantial evidence was used to establish the grant of illegal gratification.

---

[9] *Sandeep Phukan, CBI, ED chiefs can now have five-year terms*, THE HINDU (November 14, 2021), https://www.thehindu.com/news/national/cbi-ed-directors-can-now-have-tenures-of-up-to-five-years-centre-issues-two-ordinances/article37487617.ece.

[10] *SEBI Empanels 16 Entities to Conduct Forensic Audit*, ECONOMIC TIMES (August 24, 2021), https://economictimes.indiatimes.com/markets/stocks/news/sebi-empanels-16-entities-to-conduct-forensic-audit/articleshow/85588000.cms?from=mdr.

[11] *Neeraj Dutta v. State (Govt, of NCT, Delhi), Criminal Appeal 1592 of 2022.*

b. Anti-Money Laundering

Recently, in a landmark judgement in *Vijay Madanlal Chaudahry and Ors v Union of India and Ors*,[12] the Hon'ble Supreme Court clarified various sections of the Prevention of Money Laundering Act, 2002 ("**PMLA**"), which were alleged to be unconstitutional. Under the PMLA, Section 5, Section 17, and Section 8(4), give ED broad discretionary investigative powers, including search and seizure and attachment of property without a trial. Section 5 deals with the power to attach property of a person said to be in possession of proceeds of crime. Section 17 focuses on the power to enter and search any place suspected to be used to keep proceeds of crime. And Section 8(4) is concerned with the ED's power to take possession of attached property at the stage of confirming provisional attachment. Additionally, under Section 50, the ED can summon and compel an accused to make admissible statements under penal threats. Section 50 was similarly challenged on the grounds of being violative of Article 20 of the Constitution and was alleged to be manifestly arbitrary and exempt from the safeguards under the Code of Criminal Procedure, 1973 ("**CrPC**"). These practices and powers were the grounds for challenge before the apex court.

The Hon'ble Supreme Court, through its judgement, enunciated the principles contained in the various sections whilst upholding their constitutional character. The Hon'ble Supreme Court upheld the constitutionality of Section 5, Section 17, and Section 8(4) of the PMLA. The point to be considered was the requisite nature of registering a complaint or report concerning a predicate offence before commencing actions of provisional attachment or searches and seizures under Sections 5 and 17, respectively. The Hon'ble Supreme Court held that after the ED was content with its reasons recorded in writing that the accused is in possession of the "proceeds of crime", it could proceed with provisional attachment or search and seizure under Sections 5 and 17 without a pre-registered complaint or report with regard to the predicate offence.

The Hon'ble Supreme Court further elaborated that there are adequate safeguards enshrined in the PMLA to prevent any potential ED abuse. Any action taken by the authorised officer if vexatious, could be prosecuted and punished under Section 62 of PMLA. As a result, the constitutionality of Section 50 of the PMLA was upheld, allowing the ED to summon any person to record their statement during an investigation. It was held that the ED does not have unfettered police powers and is required to follow procedure to ensure fairness and transparency. The Hon'ble Supreme Court clarified that summons under Section 50 of the PMLA are not for prosecution as there is no formal accusation. Resultantly, it does not infringe Articles 20(3) and 21 of the Constitution. Moreover, the Hon'ble Supreme Court also explained that if such statements are recorded subsequent to the arrest of an accused, protection granted under Article 20(3) of the Constitution in relation to testimonial compulsion would apply. Consequently, such statements cannot be used to prove anything against the accused.

[12] Vijay Madanlal Choudhary and Others v. Union of India and Others, Special Leave Petition (Criminal) No. 4634 OF 2014.

c. Criminal Procedure

In *G. Krishnegowda v. Karnataka*,[13] 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 a First Information Report ("**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*,[14] 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 Delhi High 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*,[15] the Hon'ble Supreme Court held that the CBI need not conduct preliminary enquiry before filing FIRs in corruption 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 Hon'ble 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. Oftentimes, accountancy and legal firms are engaged for preparing 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.[16]

Whereas, when such breaches of the law are probed into by governmental agencies for unearthing cases of bribery, money laundering, corruption, fraud, etc., it is termed as external investigations. External investigations tend to bring the company under the radar of such

[13] *G. Krishnegowda v. Karnataka Crl.P.No.2801 of 2021.*

[14] *Ravina and Associates Pvt. Ltd. v. CBI, 2021 SCC OnLine Del 4249.*

[15] CBI v. Thommandru Hannah Vijayalakshmi, 2021 SCC OnLine SC 923.

[16] Bruce E Yannett and David Sarratt, *Beginning an Internal Investigation: The US Perspective*, GLOBAL INVESTIGATION REVIEW (January 4, 2023), https://globalinvestigationsreview.com/guide/the-practitioners-guide-global-investigations/2023/article/beginning-internal-investigation-the-us-perspective.

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, there is no one particular method 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, oftentimes, companies have condensed and almost universally agreed upon certain best practices. Across the board, these practices are both accepted and implemented for the smooth conduct of internal investigations.

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.[17] 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 to 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 126 to 129 of the Indian Evidence Act, 1872 ("**Evidence Act**").[18] 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.[19] 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.[20]

---

[17] Miller & Chevalier, *How Can Outside Counsel Sidestep Ethical Pitfalls in Internal Investigations of Antitrust Wrongdoing?*, CORPORATE COMPLIANCE INSIGHTS (June 8, 2022), https://www.corporatecomplianceinsights.com/outside-counsel-healthcare-antitrust/.

[18] Indian Evidence Act, 1872, Sections 126, 127, 128, 129.

[19] Payel Chatterjee and Sahil Kanuga, *Internal investigations: There is no escaping anymore*!, INTERNATIONAL BAR ASSOCIATION (September 1, 2022),https://www.ibanet.org/internal-investigations-there-is-no-escaping-anymore.

[20] *Id.*

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 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 and the concerned management regarding 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.[21]

c. Disclosures

There are a variety of laws which 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.[22] 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.[23] 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.[24] 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 CrPC.[25]

However, it must also be noted that an internal investigation and its findings are matters of confidentiality and therefore the overall process has to be conducted in such a manner. 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 refers to the notice that an attorney (in-house or outside counsel) provides to a company's employee to inform the employee that the attorney represents only the company and not the employee individually. 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.[26]

---

[21] *Guide to Conducting Workplace Investigations*, CORPORATE COMPLIANCE (2008), https://assets.corporatecompliance.org/Portals/1/Users/169/29/60329/Workplace_Investigations_Guide.pdf.

[22] Companies Act 2013, Section 143(12).

[23] Companies (Auditor's Report) Order, 2020, https://www.mca.gov.in/Ministry/pdf/Orders_25022020.pdf.

[24] *Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) (Third Amendment)* Regulations, SEBI, (October 8, 2022), https://www.sebi.gov.in/legal/regulations/oct-2020/securities-and-exchange-board-of-india-listing-obligations-and-disclosure-requirements-third-amendment-regulations-2020_47821.

[25] *Criminal Procedure Code, 1972, Section 39.*Regulations, SEBI, (October 8, 2022), https://www.sebi.gov.in/legal/regulations/oct-2020/securities-and-exchange-board-of-india-listing-obligations-and-disclosure-requirements-third-amendment-regulations-2020_47821. html.

[26] Sherbir Panag, Tanya Gaunguly & Lavanyaa Chopra, *The Practitioner's Guide to Global Investigations: India*, GLOBAL INVESTIGATIONS REVIEW, (February 8, 2021), https://globalinvestigationsreview.com/guide/the-practitioners-guide-global-investigations/2021/article/india.

d. Collection and Retention of Information

Information such as the companies' financial statement, business records, observations of statutory audit, employee's personal data, etc., is collected and retained for a successful investigation. A review of all these documents is crucial and may be stored in multiple different locations and formats like 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.[27] However, there are certain crucial aspects such as data privacy concerns in the collection of information. The major laws governing data privacy in India are the Information Technology Act, 2001 ("**IT Act**"), and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data and Information) Rules, 2011 ("**IT Rules**").

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 and confidentiality of such data.[28] Violation of the prescribed security practices and procedures is punishable under Sections 43-A and 72-A of the IT Act.[29]

e. Interviewing Witnesses

Witnesses may be segregated into the below 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. The employee must ensure that the information so provided remains confidential and the organisation shall do the same. However, the organisation might waive attorney client privilege and disclose the information obtained if it becomes necessary.

ii. Implementing Witnesses

There is liability arising due to *respondeat superior*, where a violative act has been committed under the directions of a superior, but there is absence of personal liability. The witness is typically not adverse to the organisation. The counsel should nevertheless inform the witness that the purpose of the interview is to form legal advice for the organisation.

---

[27] Robert Keeling, Chapter 18 – *Corporate Internal Investigations*, in THE GENERAL COUNSEL'S GUIDE TO GOVERNMENT INVESTIGATIONS, (2nd ed., 2018).

[28] Srijoy Das, Siddharth Seshan and Disha Mohanty, *India-A Guide to Conducting Internal Investigations in India*, GLOBAL INVESTIGATIONS REVIEW, (March 4, 2016), https://globalinvestigationsreview.com/review/the-asia-pacific-investigations-review/2016/article/india-guide-conducting-internal-investigations-in-india.

[29] Information Technology Act, 2001, Section 43-A, 72-A.

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.[30]

Employee feedback is an effective way of detecting compliance violations. Information of potential threats that are safely and anonymously communicated 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.[31]

Although telephone hotlines exist, they still do not 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.[32]

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.

In the context of ESG investigations, it is necessary to focus on both hard law, which has substantially developed considering the growing importance of ESG, and soft law and other frameworks. The soft law framework is primarily the Organisation for Economic Co-operation and Development's ("**OECD**") and United Nations Environment Programme's ("**UNEP**") guidelines for multinational enterprises.[33] 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.

---

[30] Moritz Hozman, *What is a whistleblowing system*? (FAQ), INTEGRITY LINE (Oct. 24, 2022), https://www.integrityline.com/expertise/blog/faq-whistleblowing-system/.

[31] Christian Hauser, Nadine Hergovits and Helene Blumer, *Whistleblowing Report 2019*, EQS (2019), https://public-concern-at-work.s3.eu-west-1.amazonaws.com/wp-content/uploads/images/2019/05/20161953/WhistleblowingReport2019_EN-002.pdf.

[32] *Id.*

[33] *A legal framework for the integration of environmental, social and governance issues into institutional investment*, UNITED NATIONS ENVIRONMENT PROGRAMME (October 2005), https://www.unepfi.org/fileadmin/documents/freshfields_legal_resp_20051123.pdf.

In 2012, SEBI made it mandatory for the top 100 listed companies by market capitalisation to include the Business Responsibility Report ("**BRR**") as part of their annual report so that they could describe the initiatives taken from an ESG perspective.[34] 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 ("**NGRBC**").

4. Way Forward

The circumference of white-collar crimes is expanding with the increasing use of technology, especially post the COVID-19 pandemic. 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 it ensures disclosures and reporting are aptly balanced. Frauds and misconducts are brought to the attention of the authorities before they can escalate. The presence of artificial intelligence and predictive analysis is a trend that is on the horizon and is likely make a possible entry to assist in investigations. Forensic data analytics can play a role in monitoring, investigating and decrementing frauds, non-compliance, and misconduct. Professionals are likely to engage and develop mechanisms for focusing on governance, compliance, ethics, industry standards and greater cooperation with the agencies for nabbing the culprits. Further inclusion of best industry practices in the Indian setup would help overcome the loopholes in the existing framework.

[34] Securities and Exchange Board of India Notification, (September 2, 2015), 1441284401427.pdf (sebi.gov.in).

B

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 of the functions of law enforcement. Investigation, according to Section 2(h) of the Code of the Criminal Procedure, 1973, comprises every proceeding carried out by the police or any prescribed authority (other than a magistrate), who is authorised by a magistrate, required for collecting evidence, such as going to the crime scene, making arrests, etc. The government and other such authorities use the investigative apparatus to inquire into potential legal violations to determine if any violations are occurring, and the what and why of it.

Law enforcement agencies conduct investigations on matters ranging from corruption, bank frauds, money laundering, to murders, forgery, swindles and scandals, terrorism, riots, etc. In addition to state and local level law enforcement there are several specialised investigating agencies in India like the Directorate of Enforcement, the Central Bureau of Investigation, the Serious Fraud Investigation Office, Income Tax Officials, Customs Officials, and Competition Commission of India. These investigating agencies have several powers including search and seizure, arrest, summon, document production, etc., under various laws that are briefly discussed in this Chapter.

2. Directorate of Enforcement

The Directorate of Enforcement ("**ED**") is a multi-disciplinary organisation mandated with the investigation of offences related to money laundering and violations of foreign exchange laws.[1] ED was established as an "Enforcement Unit" in 1956 within the Department of Economic Affairs of the Ministry of Finance, subsequently in 1957, the agency was renamed as 'Directorate of Enforcement'. ED primarily deals with the implementation of Foreign Exchange Management Act, 1999 ("**FEMA**"), and the Prevention of Money Laundering Act, 2002 ("**PMLA**"). ED has led some of the most well-known 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] 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.

Under FEMA, the Central Government has authorised ED to conduct investigation into any person or company suspected of transgressing the law or rules and regulations made pursuant to FEMA.

---

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

[2] Id.

[3] ED *files charge sheet against BRD Group, its chairman and 5 others*, ZEE BUSINESS (November 23 2022), https://www.zeebiz.com/india/news-ed-files-chargesheet-against-brd-group-its-chairman-and-5-others-209240.

In accordance with Section 13 of FEMA, ED examines the violations and is also permitted to compound offences committed by an accused.[4] Section 37 of FEMA gives the Director and Assistant Director of 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.[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] 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]

Under the PMLA, ED is entrusted with the responsibility of carrying out investigations to identify assets acquired through the proceeds of crime, undertake attachment of assets, institute necessary steps concerning the confiscation of proceeds of crime.[9] These steps are conducted in response to the proceeds of crime obtained from the Scheduled Offenses mentioned under the PMLA. The PMLA overall lists 156 offences under 28 statutes as Scheduled Offenses. Additionally, the ED is empowered to undertake steps to recover 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 with the authority 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 includes: (a) entering and searching any building, place, vessel, vehicle or aircraft where the ED has reason 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; and (c) seizing any record or property found as a result of such search. The ED also has the power to arrest any person guilty of any offence, punishable under the PMLA, and the manner in which the arrest can be affected is postulated under Section 19 of PMLA.[12] Moreover, under Section 50 of PMLA, the ED has the same power as a Civil court under CPC regarding discovery, inspection, production of evidence, summons, examining, issuing commissions, etc.[13]

Recently, 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 and issue summons to any person

[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] Suman Sehgal v. Union of India, 2006 SCC OnLine Del 429
[9] *Directorate of Enforcement*, GOVERNMENT OF INDIA (2023), https://enforcementdirectorate.gov.in/.
[10] *Prevention of Money Laundering Act, 2002, Section 5, 8(4).*
[11] *Prevention of Money Laundering Act, 2002, Section 17.*
[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, Special Leave Petition (Criminal) No. 4634 of 2014.

as constitutional, and noted that these provisions do not suffer from the vice of arbitrariness. The PMLA also empowers the ED to make arrests without mandatorily providing a copy of the Enforcement Case Information Report ("**ECIR**") to the accused. Upholding this provision, the Hon'ble Supreme Court said that an ECIR is an internal document of the agency and is not required to be supplied to an accused mandatorily.

3. Central Bureau of Investigation

The Central Bureau of Investigation ("**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.[15] 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**").[16] Under DSPE, the CBI is authorised to only investigate offences in Union Territories,[17] however, the Central Government can extend the CBI's jurisdiction to other areas, including States and Railways.[18] However, the CBI is not allowed to exercise powers without the permission of the relevant State Government.[19] As per Section 2(2) of the DSPE, the CBI has all the powers, duties, privileges, and liabilities that police officers have in connection with the investigation of offences committed.[20]

The procedure for conducting investigation by the CBI is majorly governed by the procedural law i.e., the Code of Criminal Procedure, 1973 ("**CrPC**"). Additionally, detailed guidelines on CBI investigation is provided in the CBI (Crime) Manual, Government of India (2005).[21] CBI's power of arrest is derived from Section 41 of CrPC, pursuant to which the CBI may arrest an individual, for any cognizable offence notified under Section 3 of the DSPE, against whom a reasonable suspicion exists of being involved in a crime, without any arrest warrant issued by a competent Court.[22]

As per 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.[23] 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 93 of CrPC, the CBI has the power to conduct searches after obtaining warrants for the search,[24] whereas under Section 165 of CrPC, the CBI has the power to conduct search without the issuance of a warrant.[25] Section 165 of CrPC provides that if the document(s) or

---

[15] *Central Bureau of Investigation*, GOVERNMENT OF INDIA (2023), https://cbi.gov.in/about-us?search=who-we-are.
[16] *Id.*
[17] Delhi Special Police Establishment Act, 1946, Section 2.
[18] Delhi Special Police Establishment Act, 1946, Section 5.
[19] Delhi Special Police Establishment Act, 1946, Section 6.
[20] Delhi Special Police Establishment Act, 1946, Section 2(2).
[21] Central Bureau of Investigation (Crime) Manual, (2005).
[22] Code of Criminal Procedure, 1973, Section 41.
[23] Code of Criminal Procedure, 1973, Section 91.
[24] Code of Criminal Procedure, 1973, Section 93.
[25] Code of Criminal Procedure, 1973, Section 165.

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.[26] Copies of any record made under Section 165 (1) or (3) shall forthwith be sent to the nearest Magistrate or Special Judge empowered to take cognizance of the offence.[27]

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 which create suspicion of the commission of any offence.[28] The Investigating Officer, who seizes any such property, is required to report the seizure to the Magistrate having jurisdiction.[29] Moreover, the CBI may by order require the attendance of any person before itself.[30] Furthermore, the CBI is also empowered to interrogate witnesses (orally) under Section 161 and 162 of the CrPC.[31]

4. Serious Fraud Investigation Office

The Serious Fraud Investigation Office ("**SFIO**") is a multi-disciplinary organization established under the aegis of the Ministry of Corporate Affairs ("**MCA**"), consisting of experts in the field of accountancy, forensic auditing, law, information technology, investigation, company law, capital markets and taxation for detection, investigation and prosecution of white-collar crimes.[32] In response to the Naresh Chandra Committee's recommendations, the SFIO was established in July 2003. In 2002, the Naresh Chandra Committee had recommended establishing a 'Corporate Serious Fraud Office' to track down corporate fraud and oversee prosecutions under various economic legislations. 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.[33]

Under Section 212 of the Companies Act, an investigation into the affairs of a company is assigned to the SFIO, where the Government is of the opinion that it is necessary to investigate into the affairs of the company (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.[34]

The SFIO has the sole power to undertake investigations allotted to it under the Companies Act, barring any other investigating agency of the Central Government or any State Government to

[26] Code of Criminal Procedure, 1973, Section 165.

[27] Code of Criminal Procedure, 1973, Section 165(5).

[28] *Code of Criminal Procedure, 1973, Section 102.*

[29] *Code of Criminal Procedure, 1973, Section 102(3).*

[30] *Code of Criminal Procedure, 1973, Section 160(1).*

[31] *Code of Criminal Procedure, 1973, Section 161, 162.*

[32] *Serious Fraud Investigation Office*, GOVERNMENT OF INDIA (2023), https://www.mca.gov.in/content/mca/global/en/about-us/affiliated-offices/sfo.html.

[33] *Serious Fraud Investigation Office*, GOVERNMENT OF INDIA (2023), https://sfio.gov.in/en/about-sfio-history

[34] *Id;* Companies Act, 2013, Section 212.

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 documents and records to the SFIO.[35] The SFIO conducts the investigation in the manner and procedure provided under Chapter XIV of the Companies Act.[36] 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.[37] The Investigating Officer may, with prior approval of the Central Government, also conduct investigations into the conduct of related companies, if he considers the results of such investigation relevant to the investigation of the affairs of the company for which he is appointed.[38] The company under investigation and 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.[39]

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 reason to believe that the person is guilty of any offence punishable under the Sections referred to in Section 212(6).[40] This reason to believe should be recorded in writing by the Investigating Officer.[41] Provisions in relation to arrest under the CrPC applies *mutatis mutandis* to arrests made by the SFIO.[42] Moreover, if the Investigating Officer has reason 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.[43] Based on the report submitted by the SFIO to the Central Government,[44] if any person is considered guilty of any offence for which he is criminally liable, the Central Government may prosecute such person for the offence.[45]

5. Income Tax Authorities

Income Tax Act, 1961 ("**ITA**"), is an act to levy, administrate, collect & recover Income-tax in India. It came into force on April 01, 1962.[46] 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.

---

[35] Companies Act, 2013, Section 212(2).
[36] Companies Act, 2013, Section 212(3).
[37] Companies Act, 2013, Section 212(4).
[38] Companies Act, 2013, Section 219.
[39] Companies Act, 2013, Section 212(5).
[40] Companies Act, 2013, Section 212(8).
[41] Companies Act, 2013, Section 212(8).
[42] Companies (Arrests in Connection with Investigation by Serious Fraud Investigation Office) Rules, 2017, Rule 9.
[43] Companies Act, 2013, Section 220(1).
[44] Companies Act, 2013, Section 223.
[45] Companies Act, 2013, Section 224.
[46] *Income Tax Department, History of Taxation Pre- 1922*, GOVERNMENT OF INDIA (2023), https://incometaxindia.gov.in/pages/about-us/history-of-direct-taxation.aspx#:~:text=Income%2Dtax%20Act%2C%201961%20came,w.e.f.%201%2D4%2D1962.

The various Income Tax Authorities constituted for the purposes of ITA are: (1) The Central Board of Direct Taxes ("**CBDT**") constituted under the Central Boards of Revenue Act, 1963; (2) Directorate General 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.[47]

For the purposes of any investigation connected with any proceedings under ITA, certain officers of the Income Tax Authorities have been given the same power as a Civil Court under CPC regarding discovery, production of evidence, summons, issuing commissions, etc.[48] 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.[49]

Section 132 of the ITA empowers certain authorities to carry out search and seizure. In this regard, the authorities may enter and search any building or place where he has reason to believe that any relevant books of account or other documents, money, bullion, jewelry or other valuable articles or thing are being kept and examine them.[50] While exercising the powers of search, the authorities are permitted to break open the lock of any door, box, locker, safe, almirah or other receptacle where the keys thereof are not available.[51] The authorities also have the power to seize these things or place marks of identification thereon or make extracts or copies therefrom.[52] 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.[53]

6. Competition Commission of India

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.[54] The Central Government has established the Competition Commission of India ("**CCI**") with effect from October 14, 2003, for the purposes of achieving the objectives of the Competition Act.[55] 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.[56]

---

[47] Income Tax Act, 1961, Section 116.
[48] Income Tax Act, 1961, Section 131(1).
[49] Income Tax Act, 1961, Section 131(3).
[50] Income Tax Act, 1961, Section 132.
[51] Income Tax Act, 1961, Section 132.
[52] Income Tax Act, 1961, Section 132.
[53] Income Tax Act, 1961, Section 132(4).
[54] *Competition Commission of India,* GOVERNMENT OF INDIA (2023), https://www.cci.gov.in/about-us.
[55] *Id.*
[56] *Id.*

The Director General ("**DG**") acts as the investigative arm of the CCI and assists it in investigating anti-competitive business practices of enterprises. Any person aggrieved by an enterprise's anti-competitive actions may submit information to the CCI and request an investigation.[57] If the CCI determines that there is a *prima facie* case with respect to the information received regarding an enterprise's anti-competitive actions then under Section 26(1) of the Competition Act, the CCI has the authority to direct the DG to conduct an investigation into the same.[58] The DG is then required to submit a report of his findings within such period as may be specified by the CCI.[59] 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 regarding discovery and production of evidence, summons, examining on oath, receiving evidence on affidavit, issuing commissions, etc.[60] 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,[61] which empowers the DG to carry out search and seizure with the authorisation of the Magistrate.[62]

The Hon'ble Supreme Court in *Excel Crop Care Ltd. v. Competition Commission of India*,[63] 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 their 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.[64]

Under Section 100 of the Customs Act, a customs officer may undertake search on suspected persons entering or leaving India, if he has reason to believe that any person to whom this section applies has secreted about his person, any goods liable to confiscation or any documents relating thereto.[65] If any goods liable to confiscation is secreted inside the body of the suspected person, then the customs officer may detain such person and produce him

[57] Competition Act, 2002, Section 19.
[58] Competition Act, 2002, Section 26(1).
[59] Competition Act, 2002, Section 26(3).
[60] Competition Act, 2002, Section 41(2), 36(2).
[61] Competition Act, 2002, Section 41(3).
[62] Companies Act, 1956, Section 240A.
[63] Excel Crop Care Ltd. v. Competition Commission of India, (2017) 8 SCC 47.
[64] Customs Act, 1962, Section 5.
[65] Customs Act, 1962, Section 100.

without unnecessary delay before the nearest magistrate.[66] In certain other cases involving gold, diamonds, manufacture of gold and diamonds, watches, etc., the customs officer, having been empowered by general or special order, may carry out search of a suspected persons.[67] They also have the power to summon persons to give evidence and produce documents.[68]

A customs officer, empowered in this behalf, has the power to execute arrest of any person in Indian or within the Indian customs water, if he has reason to believe that such a person has committed certain offences punishable under the Customs Act.[69] Every person arrested shall, without unnecessary delay, be taken to a magistrate.[70] Additionally, the customs officer may on authorisation from the required authority, search any premises where there is reason to believe that any goods liable to confiscation, or any documents or things which in his opinion will be useful for any proceeding under the Customs Act, are secreted.[71] 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 if he has reason to believe that such goods are liable to confiscation under the Customs Act.[72]

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 external factors such as politics, bureaucracy, frequent challenges to the powers of the investigating agencies under various Acts, etc., that lead to inefficient working and becoming 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 operation, unbiased investigation and to promote national welfare without favouring any individual or institution in particular.

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

C

Anti-Money Laundering Regulations & The Indian Online Gaming Industry

1. Introduction

Online gaming has grown in popularity, especially in the wake of the Covid-19 pandemic and since then online casinos, virtual reality games, fantasy sports and electronic sports ("**e-sports**") have taken over the traditional gaming industry. The online gaming industry majorly consists of two types of games namely, 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 KPMG report, by 2025, the Indian gaming industry is expected to be valued at INR 290 billion.[1] Against the backdrop of these 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 and 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 bringing in 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 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]

---

[1] KPMG, Beyond the Tipping Point: A Primer on Online Casual Gaming in India, available at: Beyond the tipping point - A primer on online casual gaming in India (assets.kpmg)

[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

[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.

In this article, we will focus 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, that 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 multi-player online role-playing games.[9] These activities are difficult to monitor in the absence of proper regulations and they often enable cross-border financial activity to take place undetected. This enables laundering of money through transfer of the virtual in-game items in lieu of real money and allows illicit financial activity to get lost in a host 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, 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, digital casinos, etc. It is imperative to frame a new legislation which can address the loopholes.

Even at the state level, there is an inadequacy in dealing with online gaming and gambling. Even though gambling and betting, and taxation arising thereof is a State subject as provided in the

---

[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).

[8] *Id.*

[9] *Id.*

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

[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

Constitution, there is no uniform law governing the same[12] The IMTF Report has found that the lack of uniform regulatory approach for 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 which have specific laws to govern online gaming. However, states like Delhi, Madhya Pradesh, and Uttar Pradesh have largely adopted the Public Gambling Act, which prohibits games of chance but allows games of skill.[15] On the other end of the spectrum, some states like Karnataka, Andhra Pradesh Kerala and Tamil Nadu sought to prohibit both games of skill and games of chance.[16] Such prohibitions in Karnataka and Tamil Nadu were challenged before the High Courts and were declared unconstitutional.[17] Some states like Rajasthan are still in the process of framing their gambling laws, especially with respect to fantasy sports and e-sports.[18]

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 game. The Gujarat High Court held poker to be a game of chance and hence, illegal[19] whereas the Calcutta high court declared it to be a game of skill and legal.[20]

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, and 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,[21] but require a central legislation to tackle offshore illegal gambling sites.[22]

---

[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] CBI v. Thommandru Hannah Vijayalakshmi, 2021 SCC OnLine SC 923.

[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/explainers/india-law-gambling-online-gaming-betting-state-ban-illegal-legal#read-more#read-more

[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] 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.

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

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

[21] TIMES OF INDIA, Curbing Offshore Online Betting and Gambling available at: https://timesofindia.indiatimes.com/blogs/voices/curbing-offshore-online-betting-and-gambling/

[22] Id.

4. Anti-Money Laundering Regulations in India

a. Prevention of Money Laundering Act

The PMLA and the rules issued thereunder ("**PML 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 its definition, money laundering involves obtaining/deriving proceeds arising from commission of a criminal offence.

The PMLA lays down the broad framework for anti-money laundering ("**AML**") compliance requirements applicable to banking companies, financial institutions, intermediaries, and persons carrying on a designated business or profession (collectively, "**Reporting Entities**"). Section 2(1)(sa) 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.*"

Pursuant to PMLA and PML Rules, Reporting Entities are required to undertake certain AML measures that *inter alia* includes customer identification, enhanced client due diligence ("**CDD**"), customer acceptance, maintenance of records, and tracking and reporting of certain types of transactions.[23] 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 like cash transactions crossing INR 10 lakh, and "suspicious transactions" whether or not effected in cash.[24]

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.

[23] Prevention of Money Laundering Act, 2002, Section 12; Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, Rules 3,4,5,7 and 8.

[24] Prevention of Money Laundering Act, 2002, Section 12.

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.

c. Tax Regulations

i. Indirect Tax

Services by way of admission to entertainment events or access to casinos, etc., are taxable at the rate of 28% GST. Online gaming is included in the category of '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% for games of chance, i.e., betting/gambling, and 18% for games of skill. The tax is levied on the service fee/commission charged by the gaming operators.[25]

ii. Direct Tax

Where the income of a resident includes income by way of winnings from games of any sort, betting, gambling, etc., such income would be liable to tax in the hands of such taxpayer, at 30% (plus applicable surcharge and cess).

The tax under the Income Tax Act, 1961 ("**ITA**") will not be applicable in cases where the income is leviable to Equalisation Levy. Equalisation Levy ("**EL**") was introduced in 2016 to tax digital transactions done via Indian IP addresses, which can cause an accrual of income to foreign companies. The levy, which initially only applied to business-to-business transactions involving online marketing, was expanded to include goods or services provided by non-resident e-commerce operators in 2020. EL at 2% 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.[26]

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

[25] 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).

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

virtual/e-wallet account is used for playing online games/poker and is funded by income chargeable to tax in India on which tax has not been paid and the person makes profit from the said gaming, the person must disclose the account details to Indian tax authorities.[27]

5. Risk Mitigation in the Online Gaming Sector

In order 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 that can monitor in-game transactions and flag suspicious transactions, place transaction limits and track payment between users. Other preventive measures include blocking accounts which do not provide authentic information or have multiple accounts set up from the same IP or physical address.[28]

In the absence of comprehensive legislation governing the online gaming sector and the sector having such niche and nuanced functioning, self-regulation appears to be the most effective option/solution for this industry.

Although the costs associated with putting such risk mitigating practices in place would be a disincentive for many gaming operators, it shall be a better alternative than accruing criminal liability due to 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.

6. Recommendations: The Way Forward

In light of the increase in risk of money laundering via online gaming platforms, comprehensive steps need to be taken to curb the same and mitigate risks associated with it. Companies should have the onus to demonstrate 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.

Taking into account a few of the best practices across the globe, some measures can be taken as follows:

Expanding the definition of gaming: As mentioned by the IMTF Report, the current legislation governing Gambling in India is not sufficient to address the intricacies of the growing online gaming sector. Therefore, the legislation needs to be expanded beyond the physical

---

[27] *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).

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

understanding of gambling into the digital realm. The definition of gaming should not be limited to land-based casinos but should include all types of providers of gambling services.

Licencing for online games: One way to regulate the online gaming industry is to establish the requirement of licensing for gaming operators. 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.

Some States like Sikkim and Meghalaya already have a licensing regime for Online games. Under the Sikkim Online Gaming (Regulation) Act, 2008, operators are required to obtain a license under the act and only allowed to offer the games at intranet terminals.

The benefit of the licensing regime is that a license can be issued by the government upon fulfilment of certain conditions by gaming operators. These conditions could include compliance to AML laws. Licensees would be required to implement a number of anti-money laundering procedures as part of their day-to-day operations such as:

i. Appointing a designated Money Laundering Reporting Officer;

ii. Bringing gaming operators explicitly under the definition of Reporting Entities under the PMLA so that there shall be a requirement of client due diligence along with penalties associated with non-compliance of the same;

iii. Having fraud management procedures in place;

iv. Having AML/CFT training for employees.

Identifying Politically Exposed Persons ("PEP"): Online gaming companies should not only consider foreign PEPs but also domestic PEPs as high-risk clients. Furthermore, companies must 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 the time when the PEP is classified as one.

Implementation of Know Your Customer ("KYC"): One of the foremost ways of tackling fraud and money laundering is to ensure that KYC verification is implemented by online gaming operators. As more and more players pour into the online gaming industry, the importance of regulatory compliance will be crucial in scaling the player base and minimizing efforts to reduce fraud.

KYC need not be done physically, instead e-KYC can be implemented to make the process easier. The e-KYC verification shall include online document verification, ID verification like Aadhaar and Pan card, real-time biometric face authentication, etc. In April 2022, the government was contemplating introducing KYC obligations for online skill gaming operators in an attempt to curb money laundering.[29]

[29] 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.

Age Verification should also be a pre-requisite for online games. This is especially in light of the fact that the WHO has declared that gaming can create addictive behaviours and lead to gaming disorders amongst teenagers.[30] Age verification will help verify and protect underaged users from accessing the game.

The evolution of the Indian online gaming market appears to be reaching a major turning point. By 2026, its value, which is currently estimated to be USD 2.2 billion, is predicted to reach USD 7 billion.[31] The Indian government is proactively contemplating measures to enhance the growth of the online gaming industry by proposing to overhaul the archaic gambling laws and bringing in a legislation which would cover the nuances of the online gaming sector. This would potentially protect consumers, increase investment, and consequently, employment. India is on the path to provide regulated lucrative opportunities in this booming industry for operators and players, which would bring this regime at par with international online gaming regimes.

[30] World Health Organisation, Addictive Behaviours: Gaming disorder, available at: https://www.who.int/news-room/questions-and-answers/item/addictive-behaviours-gaming-disorder.

[31] Vivek Dubey, I*ndia's gaming market is worth $2.6 billion, expected to reach $8.6 billion by 2027: Report*, BUSINESS TODAY (November 4, 2022), https://www.businesstoday.in/latest/economy/story/indias-gaming-market-is-worth-26-billion-expected-to-reach-86-billion-by-2027-report-351928-2022-11-04.

D

Sanctions Enforcement and Compliance: An Indian Perspective

1. Introduction

Sanctions are political, diplomatic, or economic measures under International law, deployed by an International organisation or States against a State or States either to protect national security interests, or to protect international law, and defend against threats to international peace and security. Sanctions can be economic, targeting specific commodities, trades, etc., military, diplomatic, and also include travel bans, asset freezes, or arms embargoes.

Economic sanctions are essentially foreign policy tools deployed by governments and international organisations or trade regulation bodies to govern or alter the strategic decisions of state and non-state actors that threaten their interests or violate international norms of behaviour. Economic sanctions often constitute a withdrawal from customary trade and financial relations, for foreign policy and national security purposes. Sanctions may be comprehensive and non-comprehensive. Comprehensive sanctions prohibit commercial activity with regard to an entire country, for instance the US embargo against Cuba, or they may be targeted, blocking transactions by and with particular businesses, groups, or individuals. On the other hand, non-comprehensive sanctions target specific activities or areas, but do not generally target an entire geographic region. Non-comprehensive sanctions also target activities that are not confined to a country or area, such as drug trafficking and terrorism.

2. United Nations & Sanction Regimes

The basis for United Nations ("**UN**") sanctions under international law derives from Chapter VII of the UN Charter, and more specifically, Article 41, which covers enforcement measures not involving the use of armed force.[1] In terms of principal objectives sought by the Security Council, the use of sanctions can be grouped into five main categories: conflict resolution, non-proliferation, counterterrorism, democratisation and the protection of civilians (including human rights).[2]

The Security Council can take action to maintain or restore international peace and security under Chapter VII of the United Nations Charter. Security Council sanctions have taken different forms in pursuit of a variety of goals. The measures have ranged from comprehensive economic and trade sanctions to more targeted measures such as arms embargoes, travel bans, and financial or commodity restrictions. The Security Council has applied sanctions to facilitate peaceful transitions, deter non-constitutional changes, constrain terrorism, protect human rights and promote non-proliferation. Examples of UNSC regimes includes, Counterterrorism

[1] *Security Council Report, Monthly forecast,* SECURITY COUNCIL REPORT, (Jan 2023), SCR-SRR-sanctions-p5d4.indd (securitycouncilreport.org).PublicationReportDetails.aspx?ID=1195

[2] *Id*

(UNSC 1373) sanctions regime; Democratic People's Republic of Korea (North Korea) sanctions regime; Former Federal Republic of Yugoslavia sanctions regime[3].

3. India's Sanctions Regime

i. India has an autonomous sanctions regime, which is generally compliant with the UNSC Resolutions/ UN sanctions through the United Nations (Security Council) Act, 1947 ("**UNSCA**"). Under the UNSCA, the Government of India has the power to take any measures to give effect to the decisions of the UNSC. India through notifications to the Foreign Trade Policy ("**FTP**"), enforced under the provisions of the Foreign Trade (Development & Regulation) Act, 1992 ("**FTDR Act**") by the Director General of Foreign Trade ("**DGFT**"), implements specific sanctions which may be outside the UNSCA. The sanctions may include such measures as arms embargoes; embargoes on nuclear related and ballistic missile related materials; or embargoes on other UN-specified goods or materials. Typically, most commonly imposed sanctions under the FTP and are in the nature of export controls or trade bans. The trade restrictions are outlined in the FTP of India, and is notified from time to time as the case may be by the DGFT further to adoption of UNSC Resolution by India or under any other law for the time being in force, such as Unlawful Activities Prevention Act, 1967 ("**UAPA**"), etc.

ii. In addition to the above, the Government of India through its respective departments such as the Ministry of Home Affairs ("**MHA**"), Ministry of Corporate Affairs, or the Finance Ministry may notify prohibitions or additional restrictions including tariffs on trade from specific countries, banning export/ import under the Indian customs laws or Foreign Exchange Management Act, 1999; as well as ban software applications under the Information Technology Act, 2000; or telecommunication channels under the respective statutory provisions.

iii. Application and Scope

a. The Indian sanctions regime targets individuals and entities that have been listed by the UN and under UAPA10, as well as against specific individuals, organisations, or countries. The sanctions imposed by India can generally be classified into two categories:

   i. trade / economic sanctions in respect of exports from and imports into India, and

   ii. sanctions relating to the security and integrity of India.

b. Under the relevant provisions, the sanctions measures must be complied with by any person in India or doing business in India.

c. Under Section 2 of the UNSCA[4], the Indian Government may pass provisions with extra-territorial operation to give effect to the UNSC Resolutions as may be necessary or expedient

[3] Id.

[4] The U.N. Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007,("**MHA Order**") issued by MHA notifies the implementation of the UN Sanctions list in India under the UAPA. The Schedule under UAPA enumerates the list of entities sanctioned under the UAPA that inter-alia includes organizations listed MHA Order made under Section 2 of UNSCA.

Notably, the UAPA provides for punishment for offences committed outside India. It provides that: "*Any person, who commits an offence outside India, which is punishable under this Act, shall be dealt with according to the provisions of this Act in the same manner as if such act had been committed in India.*"

to do so. Currently, economic sanctions by India against Iraq, Iran, Somalia and North Korea, are as follows-

i. The import/export of Arms and related material from/to Iraq is 'Prohibited'. However, export of Arms and related material to Government of Iraq is permitted, subject to a 'No Objection Certificate' from the Department of Defence Production.

ii. Trade with the Islamic State in Iraq and the Levant ("**ISIL**, or **Daesh**"), Al Nusrah Front ("**ANF**") and other individuals, groups, undertakings, and entities associated with Al Qaida has been prohibited.

iii. Direct or indirect import/export from/to Democratic People's Republic of Korea, import of charcoal form Somalia is prohibited.

iv. Direct or indirect import to Iran or import of specified items, materials or goods from Iran is restricted.[5]

iv. Enforcement and Regulatory Framework

a. Please note that India has a licensing or authorisation system in place; the FTP and certain other sector-specific regulations restrict or regulate the import and/or export of certain goods and/or services and require that such export or import may be made in accordance with the licenses granted by the DGFT.

b. The trade restrictions are outlined in the FTP and is notified from time to time, as the case may be, by the DGFT. The penalties for violation of the FTP are provided in the Foreign Trade Regulation Act, 1992. Penalties include fines and potential imprisonment in certain cases.

c. Regulators such as Reserve Bank of India ("**RBI**"), Securities and Exchange Board of India ("**SEBI**"), Insurance Regulatory and Development Authority of India ("**IRDAI**") are responsible to further compliance of the sanctions imposed pursuant to the UNSC Resolutions and FTP by entities in India. Further to the FTP, the RBI, and the SEBI may notify any applicable compliance requirements further to the FATF Guidelines to enforce compliance of AML/CFT policies and prevent transactions enabling such activities.

d. Under Section 51A of the UAPA, the Central Government is empowered to freeze, seize, or attach funds of and/or prevent entry into or transit through India any individual or entities that are suspected to be engaged in terrorism. Additionally, further to the FATF guidelines on AML/CFT Compliance, RBI also provides guidelines with respect to conduct of business and transactions with countries falling under FATF's Grey List, etc.

e. Please note that as India does not currently have a sanctions program targeting Russia, there is no specific notification/ regulation setting out a detailed monitoring, disclosure, and reporting obligation in this respect. However, it may be relevant to note in case of sanctioned entities, IRDAI, RBI and SEBI issue directives for compliance from time to time further to the FTP as well as in view of FATF Recommendations to counter money-

[5] Sanctions-India-A Q&A Guide, LEXIS NEXIS (August 31, 2022) https://www.lexisnexis.co.uk/legal/guidance/sanctions-india-q-a-guide.

laundering/ terrorist financing, etc. In the case of a listed insurance company, the following sanctions/ financial crimes risk related compliance regulations may be relevant to note:

i. SEBI issued Notification notifying the Implementation of Section 51A of UAPA,1967: Updates to UNSC's 1267/1989 ISIL (Da'esh) & Al-Qaida Sanctions List: Further to the UN Sanctions List and underlying policy framework implemented by the Indian Government under the FTP, and Section 51A, UAPA, regulated bodies are required to monitor and report entities that are listed in the aforementioned UN List.

ii. AML/CFT Guidelines for General Insurers issued under Section 34 of the Insurance Act, 1938 dated February 8, 2013 mandates as follows:

   a. Insurers are advised to maintain an updated list of designated individuals/entities in electronic form and run a check on the given parameters on a regular basis to verify whether designated individuals/ entities are holding any insurance policies with the company. An updated list of individual and entities which are subject to various sanction measures as approved by Security Council Committee established pursuant to UNSC 1267 can be accessed in the United Nations website at http://www.un.org/sc/committees/1267/consolist.shtml.

   b. Freezing of Accounts: In the event any matching records are identified, insurance companies are required to immediately report such a match within 24 hours along with full particulars of the policy held by such customer to Joint Secretary (IS-I), Ministry of Home Affairs and share a copy of the communication to the UAPA Nodal Officer of the State/UT where the account is held, IRDA and FIU- IND.

      i. Furthermore, in case of designated individuals/ entities, insurance companies are required to prevent them from conducting any transactions.

   c. Suspicious Transaction Reporting: The insurance companies shall file a Suspicious Transaction Report ("**STR**") with FIU-IND in respect of the insurance policies to designated individuals/ entities, carried through or attempted, in the prescribed format. Upon a positive identification of such designated individuals/ entities, upon receipt of such report by the IS-I Division of MHA., and if the results of the verification indicate that the insurance policies are owned by or are held for the benefit of the designated individuals/ entities, an order to freeze these insurance policies under Section 51A of the UAPA would be issued within 24 hours of such verification and conveyed electronically to the concerned office of insurance company under intimation to IRDA and FIU-IND. The said order shall take place without prior notice to the designated individuals/entities. It may be noted that 'freezing of insurance contracts' would require not permitting any transaction (financial or otherwise) against the specific contract in question.with full particulars of the policy held by such customer to Joint Secretary (IS-I), Ministry of Home Affairs and share a copy of the communication to the UAPA Nodal Officer of the State/ UT where the account is held, IRDA and FIU- IND. The said order shall take place without prior notice to the designated individuals/entities. It may be noted that 'freezing of insurance contracts' would require not permitting any transaction (financial or otherwise)

against the specific contract in question.

d. Reporting Obligations: Suspicious activity monitoring program should be appropriate to a company and the products it sells. Special attention should be paid to all complex, unusually large transactions and all unusual patterns having no apparent economic or visible lawful purpose.

Background of such transactions, including all documents /office records / memorandums pertaining to such transactions, as far as possible, should be examined by the Principal Compliance Officer (refer para 2 (iii)) for recording his findings. These records are required to be preserved for ten years.

i. Insurance companies should report the suspicious transactions immediately on identification. Such reports should include attempted transactions, whether or not made in cash, irrespective of the monetary value involved. When such transactions are identified post facto the contract, a statement may be submitted to FIU-IND within seven working days of identification in the prescribed formats.

ii. Directors, officers and employees (permanent and temporary) shall be prohibited from disclosing the fact that a Suspicious Transactions Report or related information of a policyholder/prospect is being reported or provided to the FIU- IND.

v. Consequences of Breach of Sanctions

a. Where any person attempts, makes or abets the carrying out of any import or export in contravention of the provisions of the FTDR Act, 1992 and the FTP, that person will be liable to a penalty of not less than INR 10,000 and not more than five times the value of the goods or services or technology in respect of which any contravention is made or attempted to be made, whichever is more. The person may also be liable to a penalty under the Customs Act 1962, which includes imprisonment.

b. Without prejudice to any other penalty which may be imposed, in the case of a contravention relating to specified goods, services or technologies (as defined in the FTDR Act), the penalty will be in accordance with the provisions of the Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act 2005, which includes imprisonment. To summarise, non-compliance with export regulations can result in:

c. The suspension or cancellation of the importer-exporter code and export licence.

d. Penalties not amounting to less than INR 10,000 and not more than five times the value of the goods, services or technology in respect of which any violation is made or attempted to be made (whichever is higher).

e. Other penalties under the Customs Act 1962.

4. Introduction of International Trade Settlement in Rupees

The Reserve Bank of India ("**RBI**") has allowed the invoicing of international trade in Rupees, in efforts to keep the Indian currency stable and reduce the use of the US Dollar.[6] A Rupee Vostro account is a foreign bank's account with an Indian bank in rupees in India. Foreign parties will be able to send and receive money to and from Indian exporters and importers via these Rupee Vostro accounts. On the other hand, a Nostro account refers to an Indian bank's account with a foreign bank in foreign currency in the foreign country. Vostro and Nostro account accept payments in rupees, and authorised dealer banks will be able to open special Rupee Vostro accounts. All exports and imports under this arrangement may be denominated and invoiced in rupee ("**INR**") and the exchange rate between the currencies of the two trading partner countries may be market determined.

The RBI had previously allowed settlement of international trade in Rupees in wake of the 2019 Office of Foreign Assets Control ("**OFAC**") sanctions against Iran by setting up an alternative 'rupee-rial' trading mechanism for its crude oil purchases. Under this arrangement, Iran opened a bank account with an Indian Bank with no exposure to the US financial system, and the same was used to make payments in rupees.

The Indian position is that India "will abide by UN sanctions", and is "not duty-bound to implement unilateral sanctions by the US and the EU.[7] The Government of India issues notifications from time to time to impose sanctions, which may be against specific individuals, organisations, or countries. Sanctions imposed by India can broadly be classified into economic or trade-related sanctions affecting India's exports and imports, and sanctions relating to India's security and integrity. Sanctions on Russia due to its war on Ukraine, and the West subsequently cutting off Russia from the Society for Worldwide Interbank Financial Telecommunications ("**SWIFT**") payments system is likely one of the motivating factors behind this decision. The 2022 decision to allow international trade settlement in rupees is aimed at easing trade with Sri Lanka, which is running low on forex reserves, and Russia, which cannot make payments in US dollars due to sanctions by the West.

Trade settlement in INR with countries where India has trade surplus is expected to be beneficial, but settlement with trade deficit countries is likely to be difficult unless a strong line of credit mechanism is also put in place. RBI would also need to permit seamless setoff of trade payables against service receivables and vice versa to make this arrangement successful. This step would also help support trade with countries such as African and South American countries and neighbouring Sri Lanka that have little access to other currencies.

It is important to note that non-compliance with OFAC sanctions may be subject to 'secondary sanctions', hence, before proceeding with any commercial activity that may be subject to sanctions, it is important to review the touchpoints for concerned jurisdictions.

---

[6] *RBI sets up system to settle trade in rupees*, THE HINDU, (June 11,2022), https://www.thehindu.com/business/Economy/rbi-sets-up-system-to-settle-trade-in-rupees/article65627987.ece#:~:text=The%20Reserve%20Bank%20of%20India,the%20regulator%20to%20facilitate%20this.

[7] *RBI's gameplan for conducting international trade settlements in rupees* (Jul 15,2022), LIVEMINT, https://mintgenie.livemint.com/news/markets/rbi-s-gameplan-for-conducting-international-trade-settlements-in-rupees-151657851763522.

5. Sanctions Compliance and Risk Assessment

It is important that Indian businesses operating globally are aware of the potential ways in which sanctions violation may be triggered. Sanctions may apply to non-US persons and entities who have significant investments, interests or assets in sanctioned regions and sectors. Furthermore, OFAC is authorised to block non-US persons and entities from the US financial system where such a person or entity is engaging in activities prohibited by the sanctions program.

Based on the regulatory and legislative developments across the world, it is imperative for entities and individuals involved in business in the sanctioned regions or with designated individuals to assess and address the extent of their exposure to the sanctioned jurisdictions and entities. In view of the complications, it may be prudent to explore exit option where necessary. It is also important to ensure compliance with the sanctions programme, as may be applicable, based on territoriality or facilitation rule. Furthermore, it is important to carry out all necessary due diligence before pursuing any continuing or new transactions with persons or entities located in the sanctioned regions. Sanctions programmes generally include exemptions to allow:

i. general licences that, among other things, permit humanitarian aid such as food, medicine, medical equipment, etc., and legal representation to defend against embargo, and

ii. specific licences that permit specific transactions post OFAC review and approval.

Additionally, it may be helpful to ensure that the end-user or beneficiary of any good supplied or services provided are not on the Specially Designated Nationals ("**SDN**") List or the Sectoral Sanctions Identifications ("**SSI**") List by enhancing the customer KYC and due diligence measures. In view of the developments, it may be helpful to screen further transactions in the regions to assess the beneficiaries and owners of counter-parties and customers. Furthermore, in the event of a red flag or potential trade with a designated entity, appropriate disclosures may be required under the law.

It is advisable to seek legal counsel in this regard, prior to proceeding with a transaction with parties located in sanctioned regions. It is also recommended that organisations conducting businesses outside India have an internal compliance program to develop, implement, and routinely update a robust Sanctions Compliance Program, highlighting senior management commitment, encouraging a compliance culture, and training employees to understand and abide by the compliance program. Companies also need to implement necessary measures, policies, and procedures such as assessment of risks and identification of red flags to reduce potential violations and improve the system and internal controls by regular audits. An adequate and effective economic sanctions compliance by incorporating sanctions compliance training must focus on:

a. Issuing and updating relevant compliance policies and procedures for economic sanctions reflecting current regulatory requirements;

b. Ensuring that such policies and procedures are clearly understood by relevant employees;

c. Ensuring regular appropriate training measures for relevant employees;

d. Regular reviewing of the procedures outlined in this Policy (at least annually) by the Legal and Compliance Department to ensure their effectiveness, identifying and intimating senior management of potential weaknesses as well as providing guidance wherever sanctions risks touchpoints/ red-flags are identified;

e. Having a process in place for identifying, monitoring, and reporting suspected violations; and

f. Ensuring the maintenance of records as mentioned under this Policy and as prescribed by Regulators from time to time.

Corporations, including non-financial institutions, must have an effective sanctions compliance programme to manage their risk, which addresses legal, technological, operational and cultural aspects to ensure ongoing compliance with all relevant sanctions imposed by various governments and other bodies. Furthermore, corporations should carry out a risk assessment to assess their sanctions-related exposures, identify potential root causes, and implement mitigating procedures and controls.

The risk assessment is also key for scoping out the exposure to secondary and primary sanctions as well as identifying potentially sanctioned counter-parties or customers. The findings of the risk assessment must then be incorporated into the wider internal compliance framework to ensure appropriate emphasis and attention from management. In case of any exposure to sanctions, subsequent voluntary reporting to the appropriate authorities must be encouraged.

E

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. Such investigations are usually conducted through in-house company mechanisms, in response to complaints filed, either by employees or outsiders on different matters, such as financial irregularity, employee misconduct, etc. Accordingly, the company initiates a formal inquiry to determine whether there has been any violation of law, regulation, or internal organisational policy.

Traditionally, companies would engage forensic experts or accountants or legal professionals to carry out such internal investigations. Owing to the highly subjective nature of the investigations, though India does not have a set mechanism or procedure in place for conducting such investigations, internal investigations are conducted as per the procedures defined in internal policies of companies as well as in accordance with international standards and best practices, in order 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 safeguards the business from humiliating raids. This, in turn, allows the company to self-correct any past wrongdoings.

An internal investigation is conducted to get 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

There are many crucial benefits of internal investigations. An internal investigation can demonstrate a business's dedication to compliance and ethics, thus enhancing its reputation. It also conveys a positive message to the public and the company's employees. The organisation, through such an investigation, shows that it is taking the alleged violation seriously by initiating an inquiry. The ensuing corrective action that the organisation takes thereafter,

portrays an expectation that its employees are required to abide by all laws and corporate standards.

Additionally, internal investigations help companies in information gathering, defence building, and problem solving. Internal investigations are particularly helpful in identifying employees that need to be reprimanded (or worse), as well as 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**"). 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 whistle-blowers, 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, which a company 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, then the auditors of the company are required to notify the Central Government of the same.[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] 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 Code of Criminal Procedure, 1973 ("**CrPC**").[6] Similarly, anti-corruption investigations, for instance, that probe 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.

---

[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).

[3] Companies Act 2013, Section 143(12).

[4] Companies (Auditor's Report) Order, 2020, https://www.mca.gov.in/Ministry/pdf/Orders_25022020.pdf.

[5] *Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) (Third Amendment) Regulations*, SEBI, (October 8, 2022), https://www.sebi.gov.in/legal/regulations/oct-2020/securities-and-exchange-board-of-india-listing-obligations-and-disclosure-requirements-third-amendment-regulations-2020_47821.html.

[6] Criminal Procedure Code, 1972, Section 39.

3. Who shall have the obligation to 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 that should conform to the requirements of attorney-client privilege and should set forth the allegations that have been 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. It is important to note here that often corporate internal investigations may serve as a prelude to forthcoming criminal prosecutions and negotiations with the government.[7]

In an internal investigation, it first needs to be recognised who the 'client' is. The client, often the company, or the general counsel or the Board, is the one who 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 to take Before an Internal Investigation

Prior to 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 that specifies the parameters of the probe and helps detect potential problems along the road and keep the investigation on schedule and under budget.

The investigative plan should typically include an evaluation of the firm's operations, people, and jurisdictions that are potentially involved, as well as the primary emphasis of the investigation. It must provide an outline of the documents and data that will be examined, the people who will be questioned, and the financial records that will be the focus of any forensic audit component of the inquiry, etc.[9]

Further, prior to 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

[7] Green & Podger, *supra*, at 73.

[8] Miller & Chevalier, How Can Outside Counsel Sidestep Ethical Pitfalls in Internal Investigations of Antitrust Wrongdoing?, CORPORATE COMPLIANCE INSIGHTS (June 8, 2022), https://www.corporatecomplianceinsights.com/outside-counsel-healthcare-antitrust/.

[9] *Guide to Internal Investigations at Brandon University,* BRANDON UNIVERSITY, https://www.brandonu.ca/diversity/guide-to-internal-investigations-at-brandon-university/.

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 for 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.[10]

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 that may be needed during the course of an investigation. This is because the tasks in the investigation may be intricately complicated and unique, ranging from data gathering and server analysis to accounting irregularities and misstatements. In particular, 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 a target or subject of an investigation, potentially responsive documents cannot be destroyed, regardless of general document retention policies. A clear document retention policy is a critical component of the in-house counsel's investigative toolbox as it enables organisations to perform internal investigations and respond to requests for production readily. Moreover, to preserve documents, the investigative team has to make sure that a hold is in place and every company where there may be pertinent records is notified.

c. Collection of Data and Documents

During an investigation, it is pertinent to conduct a thorough assessment of the entity's business records, financial statements, and observations generated in response to a statutory audit. An assessment of the organisation's internal policies and practices as well as the level of adherence to those policies must be evaluated. 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**"), and it 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.[11] 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 would be a crucial component of any security process and maintains the integrity of

[10] Lorraine Campos, '*Lawyers on the Front Line: Identifying Risk and Managing Internal Investigations*' CROWELL, (DEC. 6, 2017), https://www.crowell.com/NewsEvents/AlertsNewsletters/all/Lawyers-on-the-Front-Lines-Identifying-Risk-and-Managing-Internal-Investigations-1505565.

[11] '*Digital Forensics: A vital component of Internal Investigations*', 4JOURNEY, (JUNE 25, 2020), https://4discovery. com/2020/06/25/digital-forensics-a-vital-component-of-internal-investigations/.

the gathered evidence. The chain of custody is a chronological paper trail that shows who obtained, handled, or otherwise had control over an item of evidence throughout the probe. Additionally, obtaining a consent letter from each custodian attesting to their understanding of, and agreement with, the data gathering procedure is equally important.[12]

Therefore, collection of all necessary data and documents becomes crucial. The assessment of the corporate entities' documents requires a suitable information collection strategy as there are certain crucial aspects in collection of information, which need to be taken into consideration. These aspects are given below:

i. Data Privacy and Protection

In acquiring documents, meeting with internal staff members is the initial stage. Accordingly, the team should find the whereabouts of any hard-copy or electronic documents that may be relevant. However, there are many data privacy concerns surrounding collection of such documents. Currently, there is no explicit legislation protecting data or privacy in India. The Information Technology Act, 2001 ("**IT Act**"), is the main piece of legislation in this area. In addition to this, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data and Information) Rules, 2011 ("**SPDI Rules**"), also control the transmission of personal data.

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

As per the *Puttaswamy* judgment, investigations related to communications and data carriers should be done keeping in mind 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) [proportionality] and the least intrusive method should be used when possible [subsidiarity].

This, in turn, obligates companies to (i) ensure, in instances of sensitive personal data or information or personal information, that there is a legitimate reason to collect and use such data; (ii) provide adequate privacy notice to the affected employees; (iii) obtain prior consent of the affected employees; and (iv) maintain reasonable measures to protect the security and confidentiality of such data.[14]

---

[12] *Guide to Conducting Workplace Investigations*, CORPORATE COMPLIANCE (2008), https://assets.corporatecompliance.org/Portals/1/Users/169/29/60329/Workplace_Investigations_Guide.pdf.

[13] Justice Puttaswamy (Retd) v. Union of India, (2017) 10 SCC 1 (India).

[14] Srijoy Das, Siddharth Seshan and Disha Mohanty, '*India-A Guide to Conducting Internal Investigations in India*', GLOBAL INVESTIGATIONS REVIEW, (MAR. 4, 2016), https://globalinvestigationsreview.com/review/the-asia-pacific-investigations-review/2016/article/india-guide-conducting-internal-investigations-in-india.

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 prior to key witness interviews, to ensure that the interviewer is in the best position to examine relevant documents with the witness. To efficiently review documents, the creation of a 'list of key phrases' is of utmost significance. These are the phrases that 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 that have been found are then physically evaluated, with the reviewers individually labelling (or identifying) the emails, documents, and flagging the data that appear to be 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 counsel and its agents to prevent inadvertent waiver of attorney-client privilege. Preferably, a preliminary list of potential 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 technological sophistication of the company and the alleged wrongdoing, but it typically 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 the right information sources such as employee email accounts, business communications, and pertinent files are found, one can quickly load them into a document review platform or use any pre-existing integration with data sources 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.[15] 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. Such forensic reports may be allowed as professional testimony. A forensic expert would fall under the provisions relating to expert evidence and third-party witnesses as per Sections 45 to 51 of the Indian Evidence Act, 1872 ("**Evidence Act**").[16]

[15] Bhasin, M.L. *Forensic Accounting: A New Paradigm for Niche Consulting*. The Chartered Accountant Journal, 1000-1010 (2007).
[16] The Indian Evidence Act, Sections 45-51.

f. Confidentiality Concerns and Client-Attorney Privilege

India has adopted a strict approach toward privileged professional communication between clients and legal advisors. Sections 126 to 129 of the Evidence Act deal with data confidentiality that the client shares with his attorney. It can be essentially said that any communication made for the purpose of seeking legal advice from an attorney 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 Section 126 of the Evidence Act. However, in the Indian legal framework, this protection does not generally extend to an in-house counsel.

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

g. Notice of Mandatory Leave

As a matter of best practice and to preserve the independence, fairness, and sanctity of the investigation, the company may issue a notice of mandatory leave to the employees who are 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 at his or her position and role.

h. Investigation Interviews and Questionnaires

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

[17] Larsen & Toubro Ltd v Prime Displays (P) Ltd., [2003] 114 Comp Cas 141 (Bom).

Interviewees are given an Upjohn warning and are told about the attorney client privileges along with 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 an attorney (in-house or outside counsel) provides a company employee to inform the employee that the attorney represents only the company and not the employee individually.[18] 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.[19]

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 to take after an Investigation

Once the above-mentioned procedures are concluded, the following steps are undertaken to conclude an investigation.

a. Investigation Report

Once an investigation is finished, the investigation team drafts an Investigation Report in order to help the company evaluate the future course of action. Any inquiry should end with a written report that summarises 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 above-mentioned points will be crucial for compiling the entire history of the problem, incident, and situation, and they will serve as the foundation for the investigative report.

b. Legal Obligations and Future Course of Action

After the internal investigation is over, 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.

---

[18] Upjohn Co. v. United States: 449 U.S. 383 (1981).

[19] Sherbir Panag, Tanya Gaunguly & Lavanyaa Chopra, '*The Practitioner's Guide to Global Investigations: India*', GLOBAL INVESTIGATIONS REVIEW, (FEB. 8, 2021), https://globalinvestigationsreview.com/guide/the-practitioners-guide-global-investigations/2021/article/india.

Once an investigation ends, 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 who refuses to cooperate should not be done reflexively, as there can be serious consequences for the company under employment laws.

6. Concerns and Issues in Internal Investigations

There are many concerns surrounding internal investigations that 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 refusing to follow instructions, even if they seem irrational or outside of the course of business.

b. Lack of Integration and Consensus within Corporate Entities

Further, there is lack of integration within the company and the operation of teams. Certain teams within an organisation operate independently, instead of being fully integrated with the processes of the company as a whole. In cases where the team undertakes complicated, highly technical processes (involving convoluted manufacturing, technology systems, etc.), it is likely that the rest of the company may not be familiar with or fully understand these processes, and the team is left to run on its own. Hence, such actions lead to reduced visibility (into their operations) and allow such teams to escape accountability from the rest of the company, and also 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. Often there is hesitation on the part of the management to conduct an investigation due to 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 the company 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.

F

Environmental Social and Governance Compliance and Enforcement in India

1. Introduction

Eighteen 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 world of finance for one has seen an exponential traction for ESG. This growth can be accorded to the shift in thinking of institutional investors.

In the 2016 Paris Agreement, 190 countries came together to agree on Climate Change measures to bolster the role of corporates to improve environmental, social and governance parameters for better sustainable future.[2] There is no denying that to drive sustainable growth, the environment needs to be continuously regulated. The increasing global demand for ESG compliance, especially among multinational corporations, has rendered law firms to dedicate niche advisory services for the same.

With respect to sustainability, it must be noted that sustainability extends beyond environmental issues. 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: https://www.unglobalcompact.org/docs/issues_doc/Financial_markets/who_cares_who_wins.pdf

[2] The Paris Agreement, 2016.

[3] Nidhi Singal, *Why India Inc. Is Excited About ESG*, businesstoday.in (7 July 2022), https://www.businesstoday.in/interactive/longread/why-india-inc-is-excited-about-esg-139-07-07-2022.

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. The Indian government has recently formulated four consolidated labour codes – governing wages, industrial relations, social security and working conditions – in a bid to address contemporaneous concerns in the workforce. Under the Factories Act 1948, the working conditions and terms of employment of certain categories of workmen are regulated. Some other acts that regulate the labourers include:

i. **Ensure fair and equitable pay:** Payment of Wages Act, 1936, Minimum Wages Act, 1948, and Equal Remuneration Act, 1976.

ii. **Regulation of employment of contract labour and prohibition of child labour:** Contract Labour (Regulation and Abolition) Act, 1970, and Child and Adolescent Labour (Prohibition and Regulation) Act, 1986.

iii. **Provides for registration and the rights/ liabilities of a registered trade union:** Trade Unions Act, 1926.

iv. **Benefit of workforce and for their overall well-being:** Employees State Insurance Act, 1948, Employees Provident Fund and Miscellaneous Provision Act, 1952, Payment of Gratuity Act, 1972, and Maternity Benefit Act, 1961.

Furthermore, under the Companies Act, 2013 ("**Companies Act**"), the board of directors must act *bona fide* in promoting the objects of the company 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 towards the environment.[4] 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 financial, operational and government matters are required to be filed with the registrar of companies as they form part of routine filings.

[4] M.K Ranjitsinh v. Union of India (Writ Petition (Civil) No. 838 of 2019).

3. ESG Policies in India

The Ministry of Corporate Affairs ("**MCA**"), in an attempt to ensure responsible business conduct by companies, 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**").[5] In March 2019, the NVG was further revised into the National Guidelines on Responsible Business Conduct ("**NGRBC**").[6]

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**") as part of their annual report so that the relevant listed entities could describe the initiatives taken by them from an ESG perspective.[7] In 2015, this number was extended to 500 companies[8] and, subsequently, in 2019, it was extended to the top 1,000 companies by market capitalisation.[9]

In 2021, the Business Responsibility and Sustainability Report ("**BRSR**") replaced the BRR to make the reporting framework more comprehensive, focussing on measurable key performance indicators across all principles of NGRBCs.[10] The top 1,000 listed companies by market capitalisation have to mandatorily furnish this report from financial year 2022-23. Furthermore, through the 'Report of the Committee on Business Responsibility Reporting'[11], 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 set up a 'Sustainable Finance Group' ("**SFG**"), with an objective of suggesting strategies and introducing a regulatory framework for banks that could propagate sustainable practices and mitigate climate related risks.[12] SFG was thus set up as a medium to co-ordinate with other national and international agencies to deal with climate change.

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 devoted towards setting up an ESG disclosure regime on a uniform basis and 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. The increase in disclosure norms will shift the discretionary conduct of ESG to that of a mandatory conduct.

---

[5] National Voluntary Guidelines on Social, Environment and Economic Responsibilities of Business' issued by the Ministry of Corporate Affair, (July 2011), https://www.mca.gov.in/Ministry/latestnews/National_Voluntary_Guidelines_2011_12jul2011.pdf

[6] National Guidelines on Responsible Business Conduct' published by the MCA, (March 15, 2019), https://www.mca.gov.in/Ministry/pdf/NationalGuildeline_15032019.pdf

[7] Securities and Exchange Board of India Notification, (September 2, 2015), 1441284401427.pdf (sebi.gov.in).

[8] *Id.*

[9] Report of the Committee on Business Responsibility Reporting (May 8, 2020) published by the MCA, https://www.mca.gov.in/Ministry/pdf/BRR_11082020.pdf.

[10] Circular on 'Business responsibility and sustainability reporting by listed entities' published by the SEBI, (May 10, 2021), https://www.sebi.gov.in/legal/circulars/may-2021/business-responsibility-and-sustainability-reporting-by-listed-entities_50096.html.

[11] Report of the Committee on Business Responsibility Reporting (May 8, 2020) published by the MCA, https://www.mca.gov.in/Ministry/pdf/BRR_11082020.pdf

[12] Reserve Bank of India Publications (28 December 2021), https://m.rbi.org.in/scripts/PublicationsView.aspx?id=20941.

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.[13] 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:

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

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

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

iv. 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 provision of relief to victims of polluting activities.

5. ESG and Investors

ESG investing can be understood as an investment made not only on the basis of financial factors, but also non-financial environmental, social and governance (or ESG) factors. In today's time, investors are heavily relying on ESG as an important metric to guide their investment decisions. Greenwashing is looked at poorly by investors internationally.[14] 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 the 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.

---

[13] *'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 5, 2016), https://pib.gov.in/newsite/printrelease.aspx?relid=137373

[14] Deena Robinson, What is Greenwashing, earth.org (November 13, 2022), https://earth.org/what-is-greenwashing/

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

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

ii. Establishing dedicated committees for the furtherance of ESG goals.

iii. Appointing a compliance officer to oversee reporting obligations under the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 ("**LODR**")[15], 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.[16] 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 increasingly being driven by investor and shareholder interest, who are now widely acknowledged as the ultimate owners of a company, 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.[17] 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.

As a result of this, 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.[18]

7. Issues in Implementation and Monitoring of ESG

i. **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

[15] SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 (September 2, 2015), https://www.sebi.gov.in/sebi_data/attachdocs/1441284401427.pdf.

[16] Kenneth Squire, *Activist ESG investing — the Goldilocks of responsible investing*, CNBC (October 8, 2022), https://www.cnbc.com/2022/10/08/activist-esg-investing-the-goldilocks-of-responsible-investing.html

[17] 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), https://corpgov.law.harvard.edu/2023/01/05/2022-u-s-shareholder-activism-and-activist-settlement-agreements/.

[18] *Prepare for ESG activism:* Parekh, THE TIMES OF INDIA (December 20, 2021); https://timesofindia.indiatimes.com/business/india-business/prepare-for-esg-activism-parekh/articleshow/88379085.

allocation, etc. Simply training employees is not enough and this shortage poses an issue in ESG implementation.

ii. **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.

Challenges to Be Addressed:

ESG reporting presently lacks a standardised scheme. There are multiple ways of reporting, which require legislative harmonisation of the 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.

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 at their end, must align their portfolios toward 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, however, incorporation of social and social justice related concepts into activism strategies would be a further bonus to ESG themed activism.

G

Cryptocurrency Regulation and White-Collar Crimes Enforcement

1. Introduction

The last decade saw 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 asset 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 and combating terror financing. Given the highly speculative character and the absence of detailed regulations, cryptocurrencies are vulnerable to frauds and price volatility.[1]

According to Chainalysis, money laundering activity in the crypto market has spiked nearly 30% between 2020 and 2021. In India, the Enforcement Directorate ("**ED**") has unearthed more than INR 4,000 crore of illegal transactions in 2021 alone. Recently, the ED froze assets worth INR 64.67 crore of a cryptocurrency exchange platform in August 2022, while investigating a money laundering case.[2] The ED stated that the cryptocurrency exchange platform had complete details of transactions relating to the crypto assets purchased from the proceeds of crime in the Instant Loan App fraud, however, it did not share the information with the authorities. In response, the cryptocurrency platform stated that though it had no legal obligation to carry out Know Your Customer/ Anti-Money Laundering ("**KYC/AML**") checks, it would carry out the checks subsequent to the investigation. The incident highlights the lacunae in KYC compliance by cryptocurrency platforms as per the Prevention of Money Laundering Act, 2002 ("**PMLA**").[3] The limited application of KYC/ AML provisions, together with transaction anonymity, exposes cryptocurrency markets to illegal activities and market manipulation, posing financial stability concerns.[4] Therefore, it is important to trace the current regulatory framework for cryptocurrencies in India and analyse the lacunae in it in order to ensure risk-proof compliance by companies.

---

[1] *Chapter 1: Macrofinancial risks,* RESERVE BANK OF INDIA (Dec 29, 2021), https://rbi.org.in/scripts/PublicationReportDetails.aspx?ID=1195

[2] *ED freezes WazirX's bank assets worth ₹64.67 crore in money laundering case*, HINDUSTAN TIMES (Aug 5, 2022), https://www.hindustantimes.com/india-news/ed-freezes-wazirx-s-bank-assets-worth-rs-64-67-crore-in-money-laundering-case-101659712179763.html

[3] *WazirX says ED has unfrozen bank accounts, allowing it to continue ops*, BUSINESS STANDARD (Sept 12, 2022), https://www.hindustantimes.com/india-news/ed-freezes-wazirx-s-bank-assets-worth-rs-64-67-crore-in-money-laundering-case-101659712179763.html

[4] GUIDANCE FOR A RISK-BASED APPROACH TO VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS, FATF (Oct 2021).

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,[5] thus eliminating the need for a central entity to validate the transactions. The first application of blockchain technology was to design and develop the cryptocurrency, Bitcoin, in 2009.

b. Cryptocurrency

While cryptocurrencies are not legally defined in India[6], the defining characteristics of cryptocurrencies are:

- *"... 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."*

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 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.[7]

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,[8] 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.

---

[5] MINISTRY OF ELECTRONICS & INFORMATION TECHNOLOGY, NATIONAL STRATEGY ON BLOCKCHAIN: TOWARDS EN ABLING TRUSTED DIGITAL PLATFORMS (Dec 2021).

[6] *Cryptocurrencies- An Assessment: Keynote address delivered by Shri T Rabi Sankar, Deputy Governor, Reserve Bank of India*, RBI (Feb 14, 2022), https://rbi.org.in/Scripts/BS_SpeechesView.aspx?Id=1196

[7] *Chapter 1: Macrofinancial risks*, RESERVE BANK OF INDIA (Dec 29, 2021), https://rbi.org.in/Scripts/BS_SpeechesView.aspx?Id=1196

[8] *Prohibition on dealing in Virtual Currencies (VCs)*, RBI (Apr 6, 2018), https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11243

From a regulatory perspective, the measure was borne out of safety concerns – the need to prevent potential misuse due to ambiguities and related to 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.[9] 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.[10] The Hon'ble Supreme Court held as follows:

> *"It is clear from the above that the governments and money market regulators 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*".[11] 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. More recently, in July 2022, the Finance Minister remarked that effective regulation of cryptocurrencies requires international collaboration to prevent regulatory arbitrage.[12]

---

[9] Internet and Mobile Association of India v. RBI, (2020) 10 SCC 274.

[10] *The Legality of Cryptocurrency in India*, LEGAL500 (Apr 19, 2021), https://www.legal500.com/developments/ thought-leadership/ the-legality-of-cryptocurrency-in-india/

[11] *Ministry of Finance, Lok Sabha Unstarred Question No. 2138*, GOVERNMENT OF INDIA, LOK SABHA (Aug 2, 2021), http://164.100.24.220/loksabhaquestions/annex/176/AU2138.pdf

[12] *Cryptocurrency: RBI seeks ban, but India needs global support to regulate it, says FM Nirmala Sitharaman* LIVEMINT (Dec 14, 2022), https://www.livemint.com/news/india/cryptocurrency-rbi-seeks-ban-but-india-needs-global-support-to-regulate-it-says-fm-nirmala-sitharaman-11658129082511.html

3. Legal Framework in India

a. Anti-money laundering regulations

Currently, there is no particular 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, which is currently in effect, allows Regulated Entities to deal in VDAs such as cryptocurrencies so long as they comply with the existing KYC, AML and countering the financing of terrorism ("**CFT**") requirements.[13]

On April 28, 2022, the Indian Computer Emergency Response Team ("**CERT-In**") issued directions under Section 70B of the Information Technology Act, 2000,[14] for the purpose of KYC for business entities, documents mentioned in the Customer Due Diligence process prescribed in RBI's KYC Master Direction of 2016, as updated from time to time must be used and maintained.

For the purpose of KYC, the Securities and Exchange Board of India ("**SEBI**") circular dated April 24, 2020,[15] mandated that procedures as amended from time to time must be referred to.[16] 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 directly impacts the cryptocurrency industry, as all "*attacks or malicious/ suspicious activities affecting systems/ servers/ networks/ software/applications related to ... Blockchain, virtual assets, virtual asset exchanges ...*" have to be mandatorily reported 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. Taxation Regulations

The Finance Act, 2022, and guidelines framed by the CBDT have brought VDAs under the tax regime.

---

[13] *Customer Due Diligence for transactions in Virtual Currencies (VC)*, RBI (May 31, 2021), https://rbi.org.in/Scripts/NotificationUser.aspx?Id=12103

[14] Nishchal Anand et al., *Blockchain & Cryptocurrency Laws and Regulations*, GLOBAL LEGAL INSIGHTS (2022), https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/india#_ednref6

[15] *Clarification on Know Your Client (KYC) Process and Use of Technology for KYC*, SEBI (Apr 24, 2020), https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/india#_ednref6

[16] *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), https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf

i. Definition of VDAs: Section 2(47A) of the Finance Bill defines VDAs as:

> *"any information or code or number or token (not being Indian currency or foreign currency), generated through cryptographic means or otherwise, by whatever name called, providing a digital representation of value exchanged with or without consideration, with the promise or representation of having inherent value, or functions as a store of value or a unit of account including its use in any financial transaction or investment, but not limited to investment scheme; and can be transferred, stored or traded electronically."*

It also includes non-fungible tokens and other assets that may be notified by the government from time to time.

ii. Tax on income from cryptocurrencies: Section 115BBH has been inserted into the Income Tax Act, 1961, pursuant to which a 30% tax is now imposed on income derived from the transfer of a VDA.[17] The Finance Secretary mentioned that "*this is not only for crypto, but for all speculative income. For example, if I take horse racing, that also attracts 30% tax. There is already a 30% tax on any speculative transaction. Crypto is a speculative transaction, so we are taxing it at a 30% rate*".[18]

No deduction other than the VDA's acquisition cost is allowed. Infrastructure costs incurred in mining of VDAs will not be treated as acquisition cost, as the same will be in the nature of capital expenditure, which is not allowable as deduction under the Act. Even losses from such trading will not be allowed to be set off against income arising from transfer of another VDA.

iii. Payment on transfer of cryptocurrencies: The Act also proposes to include Section 194S into the Income Tax Act. This will enable a withholding tax of 1% of the consideration amount to be withheld and deposited by the buyer of cryptocurrency worth more than INR 10,000. When the consideration is in kind, whether fully or partially, it must be taxed in full before the consideration can be released.

iv. VDAs as gift: Receipt of VDAs by an individual for no consideration or for a price that is at least INR 50,000 less than fair market value will be taxable under Section 56(2)(x) as "income from other sources" in the hands of the recipient. This amendment is proposed to come into effect from April 1, 2023.

From the above discussion, it is evident that the government is not in support of trading in virtual digital assets. Furthermore, the introduction of tax deduction at source in relation to transfer of virtual digital assets will enable the Government to regulate collection of taxes on such transactions.[19]

---

[17] *Cyril Shroff et al., Anti Money Laundering Laws and Regulations India*, ICLG (2022), https://iclg.com/practice-areas/anti-money-laundering-laws-and-regulations/india

[18] *Is cryptocurrency legal tender in India? What we know so far. 10 points,* LIVEMINT (Feb 2, 2022), https://www.livemint.com/news/india/is-cryptocurrency-legal-tender-in-india-what-we-know-so-far-10-points-11643806115501.html

[19] *Union Budget 2022-23 Analysis,* PRS India (February 1, 2022), https://prsindia.org/budgets/parliament/union-budget-2022-23-analysis.

c. 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 decentralized applications, therefore, they may be classified as current account transactions under Foreign Exchange Management Act, 1999 ("**FEMA**").[20]

When an Indian resident pays in cryptocurrencies for services rendered and goods sold by a non-resident, such transaction is classified as an 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 process facilitated through a bank, which leads to a situation where a cross-border barter would not be permitted. Therefore, a cross-border transfer by Indian residents involving cryptocurrency without any fiat currency through an authorised banking channel violates Export Regulation.

d. 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 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,[21] defines the term '*prepaid payment instruments' as "payment instruments that facilitate 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.[22] 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.[23] However, industry is of

[20] Vipul Kharbanda, Aman Nair, *Crypto-Assets: A Challenge To India's Strong Exchange Control Laws*, MEDIANAMA (January 10, 2022), https://www.medianama.com/2022/01/223-crypto-assets-challenge-india-foreign-exchange-laws/

[21] *Master Direction on Issuance and Operation of Prepaid Payment Instruments*, RBI (Nov 17, 2020), https://m.rbi.org.in/scripts/BS_ViewMasDirections.aspx?id=11142

[22] Meenal Garg, *A Regulatory Approach to Cross-Border Transactions through Cryptocurrency in India*, SCC ONLINE BLOG (November 23, 2021), https://www.scconline.com/blog/post/2021/11/23/cryptocurrency-3/

[23] *List of Commodities Notified under* SCRA, SEBI (Sept 28, 2016), https://www.sebi.gov.in/legal/circulars/sep-2016/list-of-commodities-notified-under-scra_33359.html

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.[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, and/ or a store of value*"[29] and has issued tax guidance accordingly. Tax has been imposed on exchange, use,

---

[24] *Crypto exchanges say Sebi or a new entity, not RBI, should regulate the sector*, MONEYCONTROL (May 18, 2021), https://www.moneycontrol.com/news/business/markets/cryptocurrency-exchanges-say-sebi-or-a-new-entity-not-rbi-should-regulate-the-sector-report-6906961.html

[25] *Budget 2022-23: Speech of Nirmala Sitharaman, Minister of Finance*, GOVERNMENT OF INDIA: UNION BUDGET (Feb 1, 2022), budget_speech.pdf (indiabudget.gov.in)

[26] *Summary of Union Budget 2022-23*, PRESS INFORMATION BUREAU (Feb 1, 2022), https://pib.gov.in/PressReleasePage.aspx?PRID=1794167#:~:text=Smt%20Nirmala%20Sitharaman%20also%20announced,been%20communicated%20in%202021%2D22.

[27] *Concept Note on Central Bank Digital Currency, RBI (Oct 7, 2022)*, https://rbi.org.in/Scripts/PublicationReportDetails.aspx?UrlPage=&ID=1218#:~:text=Reserve%20Bank%20broadly%20defines%20CBDC,a%20safe%20store%20of%20value.

[28] Harshit Rakheja, *What does the road ahead for cryptocurrencies look like in India?* BUSINESS TODAY (December 23, 2021), https://www.business-standard.com/podcast/finance/what-does-the-road-ahead-for-cryptocurrencies-look-like-in-india-121122300050_1.html

[29] *Cryptocurrency Regulations by Country*, THOMSON REUTERS (2022), https://www.thomsonreuters.com/en-us/posts/wp-content/uploads/sites/20/2022/04/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 (Dec 18, 2020), https://home.treasury.gov/news/press-releases/sm1216

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 for longer than one 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.

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.

Compared to India, the US indeed possesses a more robust regulatory regime. However, it is marked by a variety of different legislations approaching cryptocurrencies in multiple ways that make compliance more taxing and confusing. Like India, the US does not recognise cryptocurrencies as legal tender, however, the crypto exchanges are legal and regulated by each state independently.[34] The US Government is likely to pass a uniform federal law to eliminate any confusion on tax and AML rules soon.

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.*"[35]

---

[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 (Dec 18, 2020), https://home.treasury.gov/news/press-releases/sm1216

[31] Alexander Lee et al., *Tokens and accounts in the context of digital currencies*, BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM (Dec 23, 2020), https://www.federalreserve.gov/econres/notes/feds-notes/tokens-and-accounts-in-the-context-of-digital-currencies-122320.htm.

[32] CFTC *Staff Issues Advisory on Virtual Currency for Futures Commission Merchants*, CFTC (Oct 21, 2020), https://www.cftc.gov/PressRoom/PressReleases/8291-20

[33] Brett Wolf, *US law enforcers partner with cryptocurrency tracking firm to fight financial crime*, REUTERS (Dec. 23, 2020), https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/cryptocurrency-financial-crime/

[34] Lindsey Choo & Benjamin Pimentel, Crypto's *European win is just the beginning of a global regulatory fight*, PROTOCOL (Mar 15, 2022), https://www.protocol.com/fintech/global-crypto-regulation

[35] Aryan Gupta, *Cryptocurrency in Financial Statements - A Comparative Analysis*, CENTRE FOR INTERNET & SOCIETY (June 14, 2021), Cryptocurrency in financial statements (cis-india.org)

While cryptocurrency exchanges and other businesses offering such services are supposed to be registered with the Financial Conduct Authority ("**FCA**"),[36] like the US, the UK also 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.[37]

The United Kingdom considers cryptocurrencies as capital assets, thus imposing capital gains tax on the basis of the existing tax slabs with respect to exchange, payment for goods/ services and giving away cryptocurrencies.[38] 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 result in cryptocurrency exchanges and custodian wallet providers' activities being within the scope of AML laws.

This Regulation details the CDD and KYC requirements as is applicable for other businesses and is also similar to the regulatory regime in India. Further, VDAs are also not understood as other securities like in India. Similar to the US, the UK finds crypto exchanges to be legal and they are regulated by the FCA. However, cryptocurrency is not a 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

Cryptocurrency regulations vary globally, and thus far, the Indian regulatory and legislative approach has largely remained conservative.

Where transactions involving cryptocurrency surpass specified thresholds, the operators must record or report the same to FIU-IND. Regular external auditing is crucial to maintain accurate records. Importantly, true identification of the holders of cryptocurrency accounts from which funds are being sent and received will enable the operators and regulators to appropriately apply transaction monitoring controls.

The lack of a robust legal framework places crypto exchanges in a vulnerable position as they do not know what procedures they should adopt to best disassociate themselves from the proceeds of crime, as seen with WazirX in 2022. Moreover, specific regulations for unique virtual currencies and assets are imperative.

---

[36] FCA *establishes Temporary Registration Regime for cryptoasset businesses*, FINANCIAL CONDUCT AUTHORITY, UNITED KINGDOM (Dec. 16, 2020), https://www.fca.org.uk/news/press-releases/fca-establishestemporary-registration-regime-cryptoasset-businesses.

[37] *Cryptocurrency regulation around the world & how India compares*, LIVEMINT (Nov 8, 2021), https://www.livemint.com/brand-stories/cryptocurrency-regulation-around-the-world-how-india-compares-11636355438835.html

[38] Katherine Lemire, *Cryptocurrency and anti-money laundering enforcement*, REUTEURS (Sept 26, 2022), https://www.reuters.com/info-pages/supported-browsers/

H

Legal Privilege and Investigations

1. Introduction

The legal privilege or 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 legal advice seeking client.

Due to the privilege protection clause, a professional legal advisor, i.e. a solicitor, barrister or an attorney cannot divulge details of any communication without the express permission of the client. The privilege of protection is of the client and not that of the attorney. Legal privilege protects 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 disclosing 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, where in the case of *Berd vs. Lovelace*[1], the court 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 Indian Evidence Act, 1872 ("**Evidence Act**"), any professional and confidential communication with the legal advisor is protected. Sections 126 to 129 of the Evidence Act codify the common law principles of privileged professional communication between an attorney and the client. It can be essentially summarised to say that any communication made for the purpose of seeking legal advice to an attorney would be protected. In India, any person who seeks an advice from a practicing advocate, registered under the Advocates Act, 1961, would have the benefit of the legal privilege and his/her communication would be protected under Section 126 of the Evidence Act. The Bombay High Court, in *Cecilia Fernandes v. State*[3], held that the right to personal liberty given under Article 22(1) of the Constitution can be meaningfully exercised only in confidence. The interpretation of the term 'legal privilege' in India is severely diluted, especially in terms of enforcement investigation wherein investigative agencies have accessed documents.

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

[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.

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

However, the privilege is subject to limitations, and the shall no longer apply where 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 fact by or on behalf of the client.

Section 127 of the Evidence Act expands the scope of privilege provided under Section 126 by imposing a similar duty on interpreters, clerks and servants of the legal adviser. Section 128 of the Evidence Act provides that the attorney cannot disclose any information which is deemed privileged under Section 126 unless the client calls upon the legal adviser as a witness and questions him on the same. Furthermore, Section 129 of the Evidence Act lays down that no one shall 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 this case, the attorney may be compelled to disclose any communication as deemed necessary by the court to explain any evidence so provided by the attorney, but no other. The Calcutta High Court, in *Sudha Sindhu v. Emperor*[4], 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 126 of the Evidence Act, a communication by a party to his/her pleader must be of a confidential nature.[5] However, privilege does not apply to communications made before the creation of a relationship of a pleader and client.[6]

Further, in India, the work product doctrine, 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.*[7], while deciding a petition for winding up 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 126 and 129 of the Evidence Act. 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 often includes materials prepared by persons other than the

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

attorney, as long as they were prepared for ongoing or potential litigation.[8] This goes on to show that attorney work product doctrine covers a more comprehensive track than the legal privilege.

In addition to the provisions under the Evidence Act, 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, under Rule 17, Chapter II, Part VI, stipulate 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 the client and states 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.[9] A 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*[10], 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 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*[11], 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."*

---

[8] Woolley v North London Railway, (1868-1869) LR 4 CP 602.

[9] The Bar Council of India, Rules on Professional Standards, Rule 7 and Rule 15, http://www.barcouncilof¬india.org/about/professional-standards/rules-on-professional-standards/.

[10] Satish Kumar Sharma v. Bar Council of Himachal Pradesh, AIR 2001 SC 509.

[11] Municipal Corporation of Greater Bombay v. Vijay Metal Works, AIR 1982 Bom 6.

Thus, in India, in order to qualify as privileged, the communications between clients and in-house attorneys would have to be tested on the basis of whether the inhouse counsel is an employee[12] or retained in order to provide legal advice to the company. Further, the issue of whether the advice sought is in legal or executive capacity would also be a key distinguishing factor.

3. Privilege during Internal Investigations

Internal investigations pose a great challenge in terms of preserving legal privilege due to their 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. In terms of investigation, maintaining privilege is crucial and it is important to structure and conduct the internal investigation in a manner that maximises the legal privilege available in a particular jurisdiction. It is imperative to note that legal privilege in many jurisdictions across the globe may not recognise communications with an in-house counsel, as 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 recommended to create and preserve written records demonstrating the purpose of the investigation and the legal advice sought in connection with anticipated litigation, if any. The records must reflect that key decision-makers at the company are within the client group so that there is no ambiguity in relation to applicability of privilege to the communication 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 inadvertent waiver by ensuring the investigation and any related documents or reports are treated as confidential and not disclosed outside the investigation team.

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

i. **Investigative powers under Prevention of Money Laundering Act:** Under the Prevention of Money Laundering Act 2002 ("**PMLA**"), the Directorate of Enforcement ("**ED**") has been given wide powers to conduct searches and seizures when it suspects someone has engaged in

[12] Rule 49, Section VII, Chapter II, Part VI of BCI Rules.

any act constituting money laundering activity or is in possession of records, property, or proceeds of crime connected to money laundering.[13] An application or complaint must be made to the Adjudicating Authority, which has been established to exercise the 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. As per Section 8 of the PMLA the Adjudicating Authority has the authority to serve a notice, if it has reason to believe that any person has engaged in money laundering or is in possession of proceeds of crime, requesting that the person specify the sources of their income, earnings, or assets out of which or by which they acquired the property that has been seized, attached, or frozen as well as the evidence on which the person relies.

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**"), including, 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.

ii. **Investigative powers under the Prevention of Corruption Act:** Section 9 of the Prevention of Corruption Act 1988 ("**PCA**") states that if a commercial organisation gives or promises to give a public servant an undue advantage in exchange for obtaining/retaining a business or a business advantage, the person in charge of the organisation under whose authorisation the undue advantage is being given shall be punishable with an imprisonment of three years that may extend to seven years with fines.

iii. **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 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, asking them to reveal information they have on debt-ridden Infrastructure Leasing and Financial Services ("**IL&FS**"), and refusing to comply with which would result in consequences under Section 217(8) of the Companies Act.[14] 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 as it was stated that the Code of Criminal Procedure 1973 ("**CrPC**") has adequate safeguards in place with respect to search and seizure.[15] Therefore, it may be inferred that legal privilege has limited application in the face of search and seizure warrants by enforcement agencies.

---

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

[14] *SFIO sends notices to top law firms, consultants to reveal all information* related to IL&FS, ET Now (October 9, 2019), https://www.timesnownews.com/business-economy/companies/article/sfio-sends-notices-to-top-law-firms-consultants-to-reveal-all-info-related-to-debt-laden-ilfs/501593.

[15] Akshita Saxena, *No Adverse Presumption Against Investigation Agency: Delhi High Court Dismisses Plea To Regulate Search & Seizure Operations On Advocates' Premises* (October 6, 2021), https://www.livelaw.in/news-updates/delhi-high-court-dismisses-plea-to-regulate-search-seizure-operations-on-advocates-premises-183223?infinitescroll=1

iv. **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 attorney in anticipation of litigation will qualify as privileged communication.[16]

Depending on the facts and circumstances, privilege may be attached to some aspects of internal investigations. Privilege will generally attach to legal advice sought or given with respect to the investigation, lawyers' notes taken during an investigation and communications or documents which are prepared for the dominant purpose of litigation, where litigation is ongoing or reasonably anticipated.

Legal privilege, however, shall not extend to letters written by one employee to another regarding information that could potentially become useful to their attorney,[17] or for statements made by an employee regarding the subject matter of certain suit proceedings that were not to be submitted to their attorney.[18] 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 the organisation can take advantage of privilege and protect itself from making unnecessary or damaging disclosures, before embarking on the search for documents and evidence.

While in civil cases, a party may object to production of certain documents on the 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 91 of the CrPC. Section 126 does not place any restrictions on the ability to issue notices under Section 91 of the CrPC.

5. Preserving and Protecting Privilege: Best Practices

Privilege applies only to communications where an attorney's role was primarily for the purpose of rendering 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; and

[16] Larsen & Toubro Limited v. Prime Displays Pvt. Ltd., Abiz Business Pvt. Ltd. and Everest Media Ltd (2003) 105(1) BomLR 189.
[17] Bipro Doss Dey v Secretary of State for India in Council (1885) ILR 11 Cal 655.
[18] The Central India Spinning Weaving and Manufacturing Co Ltd v G I P Railway Co, AIR 1927 Bom 367.

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

v. Best practices in the age of zoom

Furthermore, to determine legal professional privilege between in-house counsel and corporate employees, 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 also 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.[19] Simply put, for legal advice privilege to apply, the dominant purpose of a 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 the 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 purpose of the said communication is to seek or provide legal advice.

iv. Where the client is a large organisation or company with 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 of such communication only to those legal and non-legal team members with a direct connection to the legal matter at issue.

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

It is highly recommended that companies while conducting internal investigations should strive to protect the privilege at the outset so as to retain the flexibility to decide later whether and

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

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.

While there is a legal duty to produce inquiry findings during litigation, it can be protected by properly asserting and preserving a privilege over all or some portions of an 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 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 in order to maintain privilege, without flouting the principles established in case law. It is important to correctly identify and mark documents as privileged and confidential.

Notes

Notes

Notes

Contributors

Faraz Alam Sagar
Partner
faraz.sagar@cyrilshroff.com

Sara Sundaram
Principal Associate
sara.sundaram@cyrilshroff.com

Pragati Sharma
Principal Associate
pragati.sharma@cyrilshroff.com

Anjali Kumari
Associate
anjali.kumari@cyrilshroff.com

Sreeja Sengupta
Associate
sreeja.sengupta@cyrilshroff.com

Offices of
Cyril Amarchand Mangaldas

Mumbai

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

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

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

GIFT City

Cyril Amarchand Mangaldas – OFC,
415, Pragya Tower, GIFT City,
Gandhinagar - 382 355, Gujarat, India
T +91 79 4903 9900 F +91 79 4903 9999
E cam.giftcity@cyrilshroff.com

Singapore

61 Robinson Road,
#11-03, Singapore - 068893
T +65 63292260
E cam.singapore@cyrilshroff.com
(CAM Singapore Pte Ltd., UEN: 202137213R)

presence also in hyderabad and chennai


INVESTIGATION


RULES
REGULATIONS