April 2025

The first quarter of 2025 i.e., (January – March 2025) has witnessed notable enforcement actions and judicial developments. In addition to multiple arrests, raids, and investigations undertaken by the law enforcement authorities of India (including the Central Bureau of Investigation ("**CBI**") and the Enforcement Directorate ("**ED**")), this quarter also witnessed key judicial developments surrounding the white collar crimes realm.

Enforcements landscape

Financial Intelligence Unit - India fines Virtual Digital Asset service provider (Bybit Fintech Limited) for violations under the Prevention of Money Laundering Act, 2002 and the rules thereunder

In January 2025, the Financial Intelligence Unit - India ("**FIU-IND**") imposed a monetary penalty of INR 9,27,00,00 (Indian Rupees nine crore twenty-seven lakh) on Bybit Fintech Limited ("**Bybit**"), a Virtual Digital Asset ("**VDA**") service provider. This was in reference to Bybit's violations of its obligations under the Prevention of Money Laundering Act, 2002 ("**PMLA**") read with the corresponding PMLA (Maintenance of Records) Rules, 2005 ("**PMLA Rules**"). As a VDA service provider, Bybit is classified as a 'Reporting Entity' under the PMLA. However, Bybit kept expanding its services in the Indian market without securing the mandatory registration with the FIU-IND. This persistent non-compliance caused the FIU-IND to block their websites to stop operations.

CBI probes INR 9,000 crore (Indian Rupees nine thousand crore) Sports City scam in Noida

In March 2025, the CBI has registered 3 (three) First Information Reports ("**FIRs**") related to alleged irregularities in the allotment, development and sanction of Sports City Projects in Noida ("**Sport City Project**") between 2011 and 2014. This suspected 'scam' is alleged to have caused losses to the tune of INR 9,000 crore (Indian Rupees nine thousand crore).

The FIRs were registered against real estate firms Logix Infra Developers Private Limited, Xanadu Estates Private Limited, and Lotus green Constructions Private Limited, their directors, and some unnamed officials of Noida Authority, based on the orders of the Allahabad High Court. The aim of the Sports City Project was to develop world class sports facilities with residential and commercial areas in Noida. Per media sources, it was alleged that after the allotment of projects, the related conditions were breached multiple times by the allotees in connivance with Noida Authority officials, causing a suspected financial loss to the State at approximately INR 9,000 crore (Indian Rupees nine thousand crore). The CBI alleged that the authorities concerned took no remedial measures even after a Comptroller and Auditor General of India report pointing out irregularities. Acting on these findings, the CBI conducted

searches at several locations in Delhi and Noida, leading to the recovery of incriminating documents. The investigation is ongoing.

CBI arrests Power Grid Corporation of India Limited official for bribery

In March 2025, CBI has arrested 2 (two) accused including senior general manager (public servant) of Power Grid Corporation of India Limited, and deputy general manager of a Mumbai based private company immediately after bribes worth INR 2,40,000 (Indian Rupees two lakh forty thousand) were paid to the public servant by the private company. Reportedly, the bribes were paid for extending undue favours in processing and passing of the bills related to the contracts of the public sector undertaking awarded to the private company.

A case was registered by CBI against 6 (six) accused including senior general manager, other representatives of private company and unknown others. The accused public servant, while acting in connivance with accused representatives of the private company, was facilitating and extending undue favours, in lieu of illegal gratification. Based on the above, CBI had laid a trap and the accused public servant caught red handed, immediately after accepting the bribe amount of INR 2,40,000 (Indian Rupees two lakh forty thousand) from the accused representative of the private company. As part of the ongoing investigation, searches were conducted by CBI at the residential and official premises of accused at Sikar, Jaipur, and Mohali which led to recovery of several incriminating documents and digital devices as well.

Cybercrime enforcements landscape

CBI dismantles transnational cybercrime network in 'OPERATION CHAKRA-IV'

In February 2025, the CBI has, as part of the on-going 'OPERATION CHAKRA-IV' successfully dismantled a sophisticated virtual asset support cybercrime network with part of its operations based in India that had been targeting German nationals since 2021. The operation was executed by the International Operations Division of CBI in close coordination with German authorities pursuant to a case registered under Section 120-B read with sections 420, 467, 468 and 471 of Indian Penal Code, 1860 as well as section 66D of Information Technology Act 2000,

During 2021-2022, the accused individuals allegedly conspired to target the German victims by gaining unauthorised remote access to the victim's computer systems and bank accounts under the pretext of offering tech support services, manipulating victims into transferring Euro 646,032 (Euro six hundred forty-six thousand thirty-two).

In February 2025, searches conducted by CBI at 6 (six) locations across Delhi, Kolkata and Siliguri have revealed that this transnational cyber-enabled financial crime network was channeling the proceeds of crime through virtual assets. CBI unearthed an illegal call centre in Darjeeling, West Bengal, finding 24 (twenty-four) hard disks of computer systems used by the accused persons containing incriminating digital evidence.

As part of the investigation CBI has arrested one of the key accused in the case and also recovered key incriminating evidences from the searches conducted at his residential premises. Further investigation on international leads is ongoing in close coordination with the foreign law enforcement agencies.

CBI conducts successful raids in the GainBitcoin scam

In February 2025, the CBI conducted nationwide searches/raids at over 60 (sixty) locations across major cities across India as part of its investigation into the GainBitcoin scam. This scheme, launched in 2015, had promised investors 10% monthly returns on Bitcoin investments for 18 (eighteen) months, following a multi-level marketing structure that enticed investors through lucrative commissions for referral. Initial payouts were made in Bitcoin, although as the scheme collapsed in 2017, payouts were made in an in-house cryptocurrency with significantly lower value, further defrauding investors. Reportedly, during the searches, CBI has seized cryptocurrencies worth INR 23,94,00,000 (Indian Rupees twenty-three crore ninety-four lakh), 121 (one hundred and twenty-one) documents, 34

(thirty-four) laptops and hard disks, and 12 (twelve) mobile phones, along with multiple hardware crypto wallets and email and instant messaging app dumps.

The investigation is currently underway and the seized documents/electronic devices are currently under analysis to uncover further details regarding the misappropriation of funds and potential international transactions linked to the scam.

Infosys agrees to pay USD 17,500,000 (US Dollars seventeen million five hundred thousand) to settle lawsuits over cyber incident in United States of America

In March 2025, Infosys announced that it had reached an agreement with the plaintiffs of lawsuits pending against its subsidiary in United States of America - Infosys McCamish Systems ("**McCamish**") involving the 2023 cyber incident which exposed about 6,500,000 (six million five hundred thousand) individuals' data to unauthorised access and affected some of the customers. Infosys McCamish Systems has agreed to pay USD 17,500,000 (US Dollars seventeen million five hundred thousand) into a fund to settle all the pending class action lawsuits and resolve all allegations made in the incident.

Infosys had first disclosed the cyber incident in a stock exchange filing in November 2023. The company said it was working with a cybersecurity products provider to resolve the issue and had launched an independent investigation to assess its impact.

The proposed terms are subject to confirmation and due diligence by the plaintiffs, finalisation of the terms of the settlement agreement, as well as preliminary and final court approval. Once approved, the settlement will resolve all allegations made in the class action lawsuit without admission of any liability.

Legislative/regulatory developments

Press release on offshore online money gaming firms to curb tax evasion

The Directorate General of Goods and Services Tax Intelligence ("**DGGI**"), as part of its recent Press Release[1] dated March 22, 2025, reported that around 700 (seven hundred) offshore entities involved in the supply of online money gaming/betting/gambling are under DGGI's scanner. It has been noticed that these entities are evading goods and services tax ("**GST**") by failing to register, concealing taxable pay-ins, and bypassing tax obligations. So far**,** 357 (three hundred and fifty-seven) websites/URLs of illegal/non-compliant offshore online money gaming entities have been blocked by the DGGI in coordination with the Ministry of Electronics and Information Technology ("**MeitY**").

In a recent operation against some of the illegal gaming platforms, DGGI targeted and blocked bank accounts that were being used to collect money from participants, attaching nearly 2,000 (two thousand) bank accounts and INR 4,00,00,000 (Indian Rupees four crore), in coordination with the Indian Cybercrime Coordination Centre (I4C) and the National Payments Corporation of India. In another action, 392 (three hundred and ninety-two) bank accounts linked to UPI ids found on websites of some of these offshore entities have been put on debit freeze and sum totalling INR 122,05,00,000 (Indian Rupees one hundred and twenty-two crore five lakh) has been provisionally attached in these accounts.

Another operation against a few Indian nationals, who were running Online Money Gaming Platforms from outside India, was conducted by DGGI. It revealed that these individuals were facilitating online money gaming to Indian customers through various such online platforms including Satguru Online Money Gaming Platform, Mahakaal Online Money Gaming Platform and Abhi247 Online Money Gaming Platform and are using mule bank accounts to collect money from Indian customers. DGGI has so far blocked 166 (one hundred sixty-six) mule accounts linked with these platforms. Till now, 3 (three) such persons have been arrested and investigation against more such individuals is under progress.

[1] Available at: https://pib.gov.in/PressReleasePage.aspx?PRID=2113991

Non-compliance by foreign entities distorts fair competition, harms local businesses, and skews the market. These unscrupulous foreign entities circumvent restrictions by creating new web addresses. Investigations also revealed that these companies operated through 'mule' bank accounts to process transactions. Funds collected through mule accounts leave the potential to be funneled into illicit activities which may also be dangerous for the national security point of view.

DGGI remains committed to proactively tackle the menace of illegal offshore gaming entities and has intensified its enforcement actions against offshore online gaming entities. The online money gaming industry comprises both domestic and foreign operators.

Security gaps in Indian Council of Medical Research system as per Indian Computer Emergency response team report

The seventh report issued by the parliamentary standing committee on communication and information technology, highlights that it was informed by the MeitY about multiple security gaps (including insecure application design and inadequate security controls) of Indian Council of Medical Research ("**ICMR**") on January 7, 2025. Further, as per media sources, the Indian Computer Emergency response Team ("**CERT-In**") had discovered threat intelligence reports about the sale of personal data from the ICMR in October 2023 as well.

Pursuant to the above, CERT-In had recommended that ICMR should, among other things, have a clear and documented security policy, adopt a risk-based approach to security, conduct regular risk assessments, ensure security by design for application development and operations, and conduct a security audit of the entire ICMR ecosystem.

The committee's report (as part of its recommendations) also requests upon MeitY to highlight the practices adopted at its end to ensure 'fool-proof security measures during the entire data life cycle and steps taken for its effective monitoring and enforcement'.

Advisory on cybersecurity threats and best practices for satellite communications

On February 4, 2025, the Indian Computer Emergency Response Team ("**CERT-In**") under the MeitY issued an advisory on cyber security threats and best practices for satellite communications. This advisory has been issued owing to the increased risk of cyber-attacks on satellite communications infrastructure. With the integration of satellite communication in essential daily operations, any disruption in the same could lead to widespread repercussions. The following risks have been highlighted as cyber security threats by CERT-In in the advisory: (a) unauthorised access to links connected to satellite in ground station can allow attackers to redirect or disable satellite functions, interrupting critical services, or even destroying the satellite for malicious purposes; and (b) data transmitted between earth and satellites are required to be secure to ensure accuracy and confidentiality to avoid compromise in data.

Judicial discourse

Judgments by the Supreme Court of India

In ***Sanjay Dutt vs. State of Haryana***[2], the Supreme Court of India ("**Supreme Court**") reiterated that directors of a company are not automatically vicariously liable for the criminal offences committed by the company. The court specifically held that "*mere authorization of an act at the behest of the company or the exercise of a supervisory role over certain actions or activities of the company is not enough to render a director vicariously liable*", and that what is required is some 'personal involvement' of such director outside his 'routine corporate duties'. The observations provide

[2] 2025 SCC OnLine SC 32

further clarity on the necessary allegations that must be particularised in order to maintain a criminal prosecution against officers of an accused company.

In ***State of Punjab vs. Hari Kesh***,[3] the Supreme Court restored a prosecution under the Prevention of Corruption Act, 1988 ("**PC Act**") while reinforcing the legal position that whether or not the sanction for prosecution was passed by the competent authority would not be a matter for quashing but would be a matter of evidence to be proved by the prosecution during the course of trial.

In ***Nirankar Nath Pandey vs. State of Uttar Pradesh***,[4] the Supreme Court held that in prosecutions for disproportionate assets under the PC Act where the check period spans many years, the assessment of income and assets should be adjusted for inflation, appreciation of property values and broader economic changes that have taken place in such long period of time.

In a significant case of ***Satender Kumar Antil vs. CBI***[5], the Supreme Court has directed that service of notices by the police, such as for appearance of accused under Section 41A of the Code of Criminal Procedure, 1973 ("**CrPC**")/Section 35 of the Bharatiya Nagarik Suraksha Sanhita, 2023 ("**BNSS**") or for appearance of witness under Section 160 of the CrPC/Section 179 of the BNSS, when done through WhatsApp or other electronic modes, is invalid. The Supreme Court held that the same is no alternative or substitute to the mode of service recognised and prescribed under the CrPC and BNSS, i.e. service in person, or by registered post, or by pasting at a prominent place. The directions came in the continuing supervision of bail and arrest procedures across the country in the said case. The Supreme Court relied on and approved previous decisions of the Delhi High Court[6] and Supreme Court[7] referring to the aspect of service.

The Supreme Court in ***Radhika Agarwal vs. Union of India***[8] held that provisions of the CrPC/BNSS relating to arrest would apply to the Customs Act, 1962 ("**Customs Act**") and the GST Act, 2017 ("**GST Act**" and collectively "**Acts**") as well. Though challenges to the constitutional validity of various provisions in these statutes were rejected, the Supreme Court observed that wherever the Acts do not expressly exclude the provisions of the CrPC relating to search, seizure and arrest, such CrPC provisions would apply. For example, customs or GST officers making arrests should bear clear identification, as per Section 41-B of the CrPC. Further, Section 41-D of the CrPC is applicable, thus entitling a person arrested by a customs or GST officer to meet an advocate of his choice during interrogation (though not throughout interrogation). Section 50A of the CrPC, which obligates the arresting officer to inform the relatives or friends of the arrestee of the place where the arrestee is being held, was also held applicable to arrests under the Customs Act or the GST Act. 'Reasons to believe' in the arrestee's guilt must be furnished to the arrestee, since Section 104 of the Customs Act is to be interpreted the same way as Section 19(1) of the PMLA. However, the court also cautioned that judicial review of arrests would not entail examining the sufficiency of such 'reasons to believe' for the arresting officer under these statutes, but only an examination of whether there were extraneous or *mala fide* circumstances, absence of authority, contravention of statutory provisions, etc.

In ***R. Madhavan Pillai vs. Rajendran Unnithan***,[9] the Supreme Court set aside a direction that had been passed by the Kerala High Court[10] to the ED to register an Enforcement Case Information Report, reasoning that it would be drastic to pass such a direction simply because the Kerala High Court felt that a predicate offence of criminal breach of trust was made out.

The Supreme Court in ***Pradeep Nirankarnath Sharma vs. ED***[11] held that even if a predicate offence was committed prior to the enactment of the PMLA, the accused would still be liable for the offence of money laundering since the said offence is a continuing one so long as the proceeds of crime are concealed, used or projected as untainted property.

[3] 2025 SCC OnLine SC 49
[4] Criminal Appeal No. 5009/2024

[8] 2025 SCC OnLine SC 449
[9] Civil Appeal No. 3530-3531 of 2025 decided on March 3, 2025
[10] *Rajendran Unnithan S. vs. Registrar of Coop. Societies*, 2024 SCC OnLine Ker 7156
[11] 2025 SCC OnLine SC 560

International developments

Trump administrations initiates pause on the enforcement under the Foreign Corrupt Practices Act

On February 10, 2025, the President of the United States of America, Donald Trump signed an executive order instructing the Attorney General of the United States of America to pause enforcement of the Foreign Corrupt Practices Act ("**FCPA**") and issue updated guidelines for enforcing the statute.

President Trump's order provides Attorney General Bondi 180 (one hundred and eighty) days to: (a) review in detail all existing FCPA investigations or enforcement actions and take appropriate action with respect to such matters to restore proper bounds on FCPA enforcement and preserve Presidential foreign policy prerogatives; and (b) issue updated guidelines or policies, as appropriate, to adequately promote the President's Article II authority to conduct foreign affairs and prioritise American interests, American economic competitiveness regarding other nations, and the efficient use of Federal law enforcement resources.

Interestingly, the Securities and Exchange Commission ("**SEC**") is not subject to this order and does not appear to be prohibited from continued enforcement of the FCPA. The SEC has civil FCPA enforcement authority over American issuers, which includes enforcing the requirement to have reasonable accounting controls as well as accurate books and records.

New international Anti-Corruption Prosecutorial Task Force Announced

The UK, France and Switzerland have announced a new anti-corruption taskforce, aimed at strengthening collective efforts to tackle the significant 'complex and international' threat of bribery and corruption.

On March 20, 2025, the UK's Serious Fraud Office ("**SFO**"), France's Parquet National Financier and the Office of the Attorney General of Switzerland announced the creation of the International Anti-Corruption Prosecutorial Taskforce to strengthen efforts to address bribery and corruption. The taskforce is intended to create formal structures to promote the sharing of expertise, insight and strategy and to seize opportunities for operational collaboration to tackle international bribery and corruption.

The taskforce will create formal structures to allow for increased cooperation at both strategic and operational levels, including a Leaders' Group to allow for the regular exchange of insights and strategy and a Working Group to devise proposals for co-operation on individual cases.

U.S. Department of Justice intensifies crackdown on cartels and transnational criminal organizations

The U.S. Department of Justice has intensified efforts to dismantle transnational criminal organizations. In line with Attorney General Pam Bondi's February 5, 2025, memorandum titled 'Total Elimination Of Cartels And Transnational Criminal Organizations' the Eastern District of New York established a dedicated Strike Force. This unit focuses on investigating and prosecuting cartels, targeting their leadership and disrupting activities like drug trafficking and human smuggling. Recent actions include the indictment of 6 (six) leaders of a maritime drug trafficking network responsible for distributing over 5,000 (five thousand) kilograms of cocaine.

Anti-Corruption, White Collar Crimes & Investigations (AWCCI) Practice

JSA has a well-established and extensive White-Collar Crimes and Investigations practice which assists clients in dealing with diverse issues, matters and investigations arising in relation to fraud, white collar crimes and violation of internal codes of conduct. We represent and advise domestic and multinationals corporates in India and across the globe. The AWCCI practice also complements our other practice areas which provide legal advice to corporates on diverse matters, including representation before other regulators such as the Reserve Bank of India (RBI), the Ministry of Corporate Affairs (MCA), the Department of Industry Policy and Promotion (DIPP) and the Securities & Exchange Board of India (SEBI) and the Directorate of Enforcement (ED) under the (Indian) Prevention of Money Laundering Act, 2002 (PMLA).

Our white-collar crimes litigation team routinely represent clients from across industries and sectors in different fora including all courts, tribunals and judicial bodies in India, along with arbitrations and other forms of dispute resolution.

This Newsletter has been prepared by:

Rupinder Malik
Partner

Kumar Kislay
Partner

Vibhor Jain
Principal Associate

Archit Sehgal
Senior Associate

18 Practices and
41 Ranked Lawyers

7 Ranked Practices,
21 Ranked Lawyers

14 Practices and
12 Ranked Lawyers

12 Practices and 50 Ranked Lawyers

20 Practices and
22 Ranked Lawyers

8 Practices and
10 Ranked Lawyers
Highly Recommended in 5 Cities

Recognised in World's 100 best competition practices of 2025

Among Best Overall
Law Firms in India and
14 Ranked Practices
---
9 winning Deals in
IBLJ Deals of the Year
---
11 A List Lawyers in
IBLJ A-List - 2025

Asia M&A Ranking 2024 – Tier 1

Employer of Choice 2024

Energy and Resources Law Firm of the Year 2024

Litigation Law Firm
of the Year 2024

Innovative Technologies Law Firm of the Year 2023

Banking & Financial Services
Law Firm of the Year 2022

Ranked Among Top 5 Law Firms in India for ESG Practice

2022

Ranked #1
Best Law Firms to Work

Top 10 Best Law Firms for Women

For more details, please contact km@jsalaw.com

www.jsalaw.com

Ahmedabad | Bengaluru | Chennai | Gurugram | Hyderabad | Mumbai | New Delhi