KHAITAN &CO ADVOCATES SINCE 1911

ANTI-FRAUD & WHITE COLLAR CRIME NEWSLETTER

Edition 1

Introduction

2025 has been a watershed year for prosecutions, investigations, and regulatory enforcement in India. Despite geopolitical headwinds, the Indian economy's stability and growth have sustained robust investment activity, a record pace of IPOs, and , consequently, greater detection of fraud and gaps in internal controls.

As the economy expands, the white-collar crime landscape is evolving just as rapidly. Recent months have brought heightened judicial scrutiny, targeted regulatory reforms, and increased cross-border cooperation, all of which underscore the growing complexity and significance of white-collar enforcement in India.

Against this backdrop, we are pleased to present this edition of **Khaitan & Co's Anti-Fraud and White Collar Crime Updates Newsletter**. Curated by the members of our White-Collar Crime Practice, this edition brings together key legal and regulatory developments from across India, along with insights into emerging enforcement trends.

We are also delighted to feature a special viewpoint from **Mr. Naved Ali, General Counsel (Asia Pacific) at Omron,** who shares his perspective on fraud risk management, compliance challenges and risk mitigation.

Through this publication, we aim to keep our clients, colleagues, and stakeholders informed on critical issues shaping the legal landscape and other aspects which may have not made news, but have a significant impact on the white collar crime landscape in India. We welcome your feedback and suggestions, which help us ensure that future editions remain timely, relevant and actionable.

We look forward to continuing these important conversations with you.

In Conversation With...

Naved Alvi
General Counsel - APAC & Oceania
Omron

How does Omron approach fraud risk management across its APAC operations, particularly in high-risk jurisdictions like India?

At Omron, risk management is a critical At Omron, risk management is a critical component of our broader compliance and corporate governance framework across the globe including in APAC region. The legal teams at Omron carry an additional responsibility of risk management and fraud risk management is an essential component of it. In markets such as India where we recognise elevated risk due to regulatory complexity, operational fragmentation and significant reliance on third-party partners, we adopt a comprehensive, proactive approach that integrates preventive controls, continuous monitoring and jurisdiction-specific risk assessments.

Our efforts are deeply collaborative, involving close co-ordination with internal audit, finance and local business leadership to ensure that fraud mitigation is not merely policy-driven but embedded into daily operations. Key measures include the regular conduct of fraud risk assessments, reinforcement of segregation of duties and the enforcement of pre-engagement compliance due diligence for all third-party relationships, particularly in high-risk functions such as procurement, logistics and customs.

Additionally, we actively promote the use of our whistleblower mechanisms, ensuring accessibility, confidentiality and employee awareness. Reports received are followed up with structured investigations conducted with rigor, cultural sensitivity, and procedural fairness, to maintain trust in the process and uphold the integrity of our internal controls. This holistic and risk-informed approach ensures that fraud risk is managed not only as a compliance obligation but as an operational priority aligned with our values and long-term business objectives.

From your vantage point as an APAC GC, what are the most significant compliance challenges you see when implementing global anti-fraud policies in the Indian context?

A key challenge lies in aligning global anti-fraud standards with the operational and cultural realities of India, without compromising the core principles that underpin our compliance framework. For instance, common local practices such as informal documentation, relationship-based dealings and culturally accepted gestures like the exchange of gifts during festive occasions such as Diwali can sometimes conflict with the strict zero-tolerance approach embedded in our global policies. In such cases, we adopt a pragmatic yet principled approach by introducing carefully defined,

> Our efforts are deeply collaborative, involving close coordination with internal audit, finance and local business leadership to ensure that fraud mitigation is not merely policy-driven but embedded into daily operations.

culturally sensitive exceptions that are subject to clear thresholds, documentation and oversight. This allows us to respect local customs while ensuring that such allowances cannot be misused or create ethical ambiguities.

To support this approach, we place strong emphasis on localised compliance training, risk-calibrated procedures and empowering local leadership to serve as champions of our compliance culture. The ability to localise our implementation without diluting our standards is essential to maintaining both effectiveness and credibility.

We consistently reinforce our commitment to Omron's core principles, particularly our belief that ethics must remain at the forefront of all business decisions. In parallel, we continue to provide alternative, ethically sound solutions often drawing on best practices from other jurisdictions to help teams navigate situations where customary practices may not align with our global expectations. This dual focus on principle and practicality has proven vital in achieving sustainable compliance outcomes in complex markets like India.

Have you faced situations where cultural or operational differences impacted the outcome or perception of an investigation? How do you mitigate that risk?

Yes, cultural context plays a significant role in shaping both the perception and execution of internal investigations. Across different jurisdictions, we observe varying employee preferences when it comes to raising concerns. For instance, in my experience, employees in India are generally more inclined to voice concerns in person, whereas employees in countries like Vietnam or Indonesia tend to favor anonymous reporting channels, such as whistleblower hotlines. Levels of trust in the investigative process also differ by culture. In some environments, individuals may be reluctant to disclose information due to concerns about retaliation, loss of face, or reputational consequences. In others, interviewees may hesitate to engage if they perceive the process to be adversarial or punitive in nature.

To mitigate these risks, we ensure that all investigations are conducted with a high degree of cultural sensitivity, legal fairness and procedural integrity. We routinely involve local HR and legal teams and, where appropriate, engage external investigators who are familiar with the local context. We also address potential language barriers by involving internal or external personnel fluent in the relevant local language, thereby minimising the risk of miscommunication or misinterpretation.

Fundamentally, building trust in the investigative process requires consistency, transparency and time. While we emphasise our policies on confidentiality and non-retaliation, we recognise that employee confidence is shaped more by observed behavior and past experiences than by formal assurances alone. Accordingly, we take a sustained, relationship-based approach to reinforce credibility in our processes.

What are some practical steps you've taken to build fraud awareness and prevention mechanisms into the operational fabric of your India business units?

At Omron, our objective is to integrate compliance into the day-to-day fabric of business operations, rather than treating it as a standalone or peripheral function. To achieve this, we have implemented a number of practical, locally relevant initiatives within our India operations. These include in-person fraud and ethics training conducted by members of the legal and compliance team at each of our Indian offices, ensuring that employees engage directly with the subject matter in a contextualised and relatable manner. We have also launched a "Holistic Risk Management" campaign, which features anonymised real-world case studies drawn not only from India but also from global operations. This initiative is designed to foster proactive awareness and enhance analytical thinking around risk identification and mitigation.

In addition, we have taken firm disciplinary action in substantiated compliance breaches, thereby reinforcing a strong and visible message of zero tolerance toward misconduct. Line managers and finance controllers are empowered to act as first-line compliance ambassadors, reinforcing the message that integrity and accountability are shared responsibilities. We have also embedded fraud awareness into onboarding processes and regular business reviews, including quarterly meetings, to ensure continuous reinforcement across employee lifecycles. Furthermore, we dedicate an entire month each year to focused activities on compliance, ethics, and anti-fraud awareness, reinforcing these values through targeted communications, workshops, and leadership engagement. Through these efforts, we aim to cultivate a culture in which fraud prevention is embraced not merely as a compliance requirement, but as a core part of our organisational ethos.

Regulatory Updates

Income Tax Act, 2025

The Income Tax Act, 2025, has officially been enacted, introducing a major reform of the country's direct tax system. Set to come into force on April 1, 2026, the new law supersedes the Income-tax Act of 1961, which had shaped India's tax framework for more than sixty years.

Notable features and proposed reforms include:

a. Wider ambit of undisclosed income - The Act expands the definition of "undisclosed income" in search and seizure cases to now include "virtual digital assets", in addition to cash, bullion, jewellery, and other tangible valuables. Crypto tokens, NFTs will also face increased scrutiny as a result of the same.

b. No new criminal offences and penalties largely unchanged - The Act does not introduce any new prosecution sections or increase punishment for existing offences.

c. Decriminalisation of Section 276CCC - Under the erstwhile Income Tax Act, prosecution for failing to file an ITR after a search operation could proceed without any sanction. The new Act reclassifies this offence as non-cognisable, meaning arrests cannot be made without judicial approval. Further, prosecution can only be initiated with prior sanction from a senior tax official.

d. Access to digital assets and platforms under search and seizure provisions - The Act allows tax authorities to forcibly access individuals' digital platforms, including social media and private email accounts, during search and seizure operations. Under the law, if a person possesses or controls books of accounts or other information stored digitally, whether on computers or electronic storage systems, they are required to provide the income tax officer with reasonable technical assistance, including access credentials, to allow inspection of any data, records, or communications stored therein. Moreover, if such access credentials are unavailable, the officer is authorised to override them to gain entry into the relevant computer systems or "virtual digital spaces". These "virtual digital spaces" are broadly defined to include social media accounts, online investment and trading platforms, bank accounts, remote or cloud servers and other digital application platforms.

   This section has attracted widespread criticism. Its implications also warrant examination in light of existing guidelines that allow the Income Tax Department to share information with other law-enforcement agencies and regulators, given the potentially far-reaching impact of this provision.

e. Conditional Relief for TDS/TCS Defaults - The Act introduces a significant relief measure for failure to deposit TDS, i.e., if the tax is deposited before the prescribed due date for filing the TDS return, prosecution will not be initiated. This provision allows taxpayers an opportunity to rectify non-compliance within the statutory timeline, thereby limiting the risk of automatic criminal prosecution.

RBI amends FEMA Compounding Guidelines for certain offences

In April 2025, the Reserve Bank of India (RBI) introduced significant amendments to the compounding framework under the Foreign Exchange Management Act (FEMA), 1999 via the "Master Directions on Compounding of Contraventions" . These Directions were issued in alignment with the Foreign Exchange (Compounding Proceedings) Rules, 2024 (FECP Rules), which replaced the erstwhile FECP Rules, 2000. These changes aim to streamline procedures, enhance transparency, and provide relief for minor contraventions, making the framework more efficient and business friendly.

The RBI has introduced a cap on the compounding amount for certain contraventions. A new penalty cap of INR 2 lacs has been introduced for technical violations. These include contraventions on violations around end-use restrictions of foreign exchange, receiving investment from ineligible foreign investors and making payments to non-residents without approvals. The cap is granted as per the discretion of the compounding authority, based on the facts and circumstances of the case, nature of the contravention and wide public interest.

Previously, the compounding framework required a 50% penalty enhancement for applicants who had been subject to an earlier compounding order but failed to pay the compounding amount and subsequently reapplied for compounding. Pursuant to the amendment, this linkage to earlier orders has been eliminated. Each reapplication will now be considered independently. This change aims to ensure fairness and consistency in the compounding process.

When to consider compounding:

- Tech or reporting misses (e.g., delays in FC-GPR/FC-TRS, ODI/ECB filings, LO/BO filings) - First check if the issue can be regularised via Late Submission Fee (LSF). If LSF is available, use it; compounding is not required.

- Substantive FEMA breaches (beyond mere late reporting), or items outside LSF - Compounding is the right recourse (voluntary, for admitted contraventions). RBI must dispose of a complete application within 180 days; payment of the compounding amount is due within 15 days of the compounding order (if the applicant fails to pay the prescribed amount within 15 days of the order, the compounding is effectively undone).

RBI vs ED: who compounds what?

- RBI compounds all contraventions under Section 13 of FEMA (which includes non-reporting or delay in reporting foreign transactions, exceeding or breaching forex limits, not repatriating foreign exchange earnings, etc.) except Section 3(a), which is done by the ED.

- Directorate of Enforcement (ED) compounds Section 3(a) cases (which includes dealing in forex outside authorised channels, Hawala transactions, etc.).

Likelihood of compounding:

- **High** chances of compounding where:
  - The breach is technical/first-time
  - Fully remedied
  - Clearly quantifiable
  - No ED angle (where facts don't suggest serious misconduct).

- RBI's process is designed to "minimise transaction costs" for admitted contraventions.

- RBI looks at undue gains or economic benefit, loss to exchequer, repetitiveness and track record, and candour during hearing to decide the amount. As mentioned above, RBI has capped certain miscellaneous reporting contraventions at INR 2 lacs per contravention.

RBI and SEBI measures to prevent financial frauds through phone calls and SMS

In January 2025, the RBI released a notification titled "Prevention of Financial Frauds Perpetrated Using Voice Calls and SMS – Regulatory Prescriptions and Institutional Safeguards", with an aim to curb the surge of digital fraud through customers' personal mobile numbers. The notification directs regulated entities of RBI, including banks, NBFCs, payment aggregators, and co-operative banks, to verify customer care numbers and use the Department of Telecommunications' Mobile Number Revocation List to monitor and clean their consumer database. Regulated entities are expected to develop SOPs for fraud prevention and enhanced monitoring of accounts linked to revoked numbers to prevent misuse in cyber frauds or as money laundering. The notification has further stated the use of specified numbering series for communication for service-related (1600xx numbering series) and promotional calls (140xx numbering series). It further reiterated the requirement to additionally comply with the Telecom Regulatory Authority of India's guidelines on commercial communications.

Similarly in April 2025, SEBI introduced a new directive aimed at curbing fraud and strengthening investor protection in the securities market. The directive mandates that all registered and regulated entities must exclusively use phone numbers beginning with the "1600" series for service and transactional voice calls to existing customers. This measure is intended to help investors easily recognise legitimate calls from SEBI-regulated entities, thereby reducing the risk of fraudulent or deceptive communications.

FIU's directions to cryptocurrency exchanges for KYC updates and verification of accounts

In April 2025, the Financial Intelligence Unit–India (FIU-IND) directed cryptocurrency exchanges to strengthen their Know Your Customer (KYC) procedures by June 30, 2025, in line with the provisions of the Prevention of Money Laundering Act (PMLA).

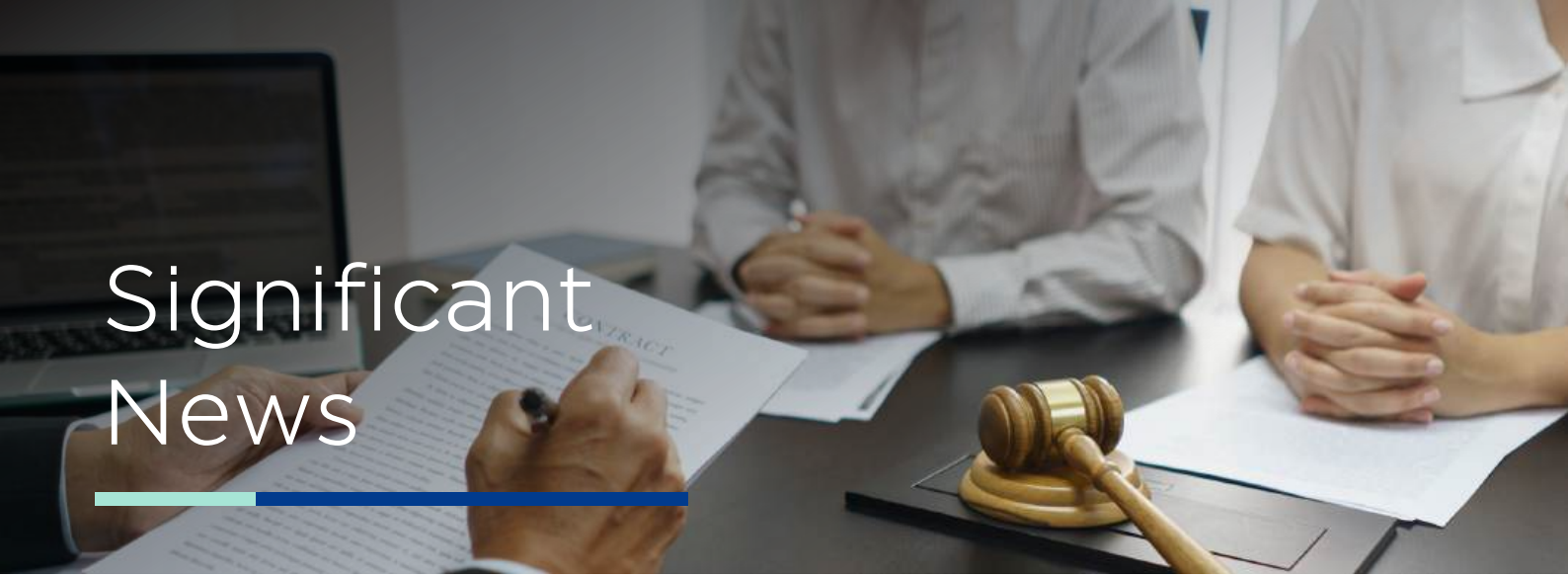
This directive is aimed at enhancing compliance with anti-money laundering (AML) regulations and bolstering the security of cryptocurrency transactions. Under the enhanced KYC framework, exchanges are required to:

Update user details: Ensure all user information is accurate and up to date.

Re-KYC older accounts: Conduct fresh KYC verification for accounts that have not been updated in 18 months or more.

Apply enhanced due diligence for high-risk accounts: Gather additional documentation and information for accounts flagged as high risk.

This move forms part of the Indian government's broader strategy to regulate the cryptocurrency sector and mitigate financial crime risks.



Significant News

NSEL-related settlements announced

SEBI proposed the NSEL Settlement Scheme 2025 for brokers against whom SEBI has passed adjudication orders or imposed fines for trading or facilitating trades on the now-defunct National Spot Exchange Ltd (NSEL) platform. The scheme is intended exclusively to settle violations of securities laws and applies to such orders in the NSEL matter where appeals are currently pending before the Securities Appellate Tribunal (SAT) or other Courts.

The scheme is open from August 25, 2025, to February 25, 2026 (inclusive). However, eligibility is restricted to brokers who:

- Have not been charge-sheeted by investigative agencies such as the Economic Offences Wing (EOW), Directorate of Enforcement (ED), Ministry of Corporate Affairs (MCA), Serious Fraud Investigation Office (SFIO) or any other law enforcement agency in the NSEL matter.
- Who are not classified as defaulters on any stock exchange as of the date of application.

Further, if any law enforcement agency files a chargesheet in the future against a broker under the Scheme for NSEL-related violations, the settlement with such broker shall be void.

This initiative is part of SEBI's ongoing efforts to address regulatory fallout from the NSEL payments crisis, which began in July 2013 when the exchange defaulted on obligations of INR 5600 crores to approximately 13,000 investors. While partial payments have been made over the years, many investors, particularly larger ones, continue to await full resolution.

Further, a significant breakthrough may be underway in the broader NSEL matter. A proposed INR 1950 crores one-time settlement between NSEL and its creditors has received overwhelming support from affected traders. About 92.81% of traders by number (5682 traders) and 91.35% by claim value voted in favour of the resolution plan, which is awaiting approval of the National Company Law Tribunal (NCLT), Mumbai.

Significant Rulings

Review of Vijay Madanlal Choudhary judgement[1]

A bench of Hon'ble Supreme Court Justices Surya Kant, Justice Ujjal Bhuyan and Justice N. Kotiswar Singh will be hearing review petitions filed against the judgement, Vijay Madanlal Choudhary v. Union of India, which upheld the constitutional validity of certain provisions of the PMLA, 2002. This landmark ruling affirmed broad powers for the ED in money laundering investigations but drew sharp criticism for diluting accused persons' safeguards.

The review is limited to two questions:

1. Is the ED obligated to provide the accused with the Enforcement Case Information Report (ECIR) filed against them?

2. Is the reversal of the presumption of innocence constitutionally valid?

The Supreme Court in Vijay Madanlal had concluded that ED enquiries are different from criminal investigations, and thus the procedural requirements under the Code of Criminal Procedure (CrPC) or Bharatiya Nagrik Suraksha Sanhita (BNSS) are inapplicable. It also upheld the twin conditions of bail under Section 45, whereby the accused must prima facie prove that they are not guilty and satisfy the court that they will not commit any offence. It also upheld Section 50 of the PMLA, holding that confessions made to ED officers, including self-incriminating ones, are admissible in evidence.

Currently, the matter is at the stage of formulation of issues. If the Supreme Court modifies or overturns key aspects of Vijay Madanlal Choudhary, the ripple effects on ED's ongoing and upcoming actions will be profound. Both individuals and corporate entities entangled in PMLA matters would see significant changes in how cases proceed:

- **Reduced Coercive Leverage:** A noteworthy impact of potential overturn of the judgement is the reduction of ED's coercive leverage. Under the current law, the threat of prolonged jail without bail and use of one's own statements as evidence creates enormous pressure on the accused to cooperate or even confess under duress. If bail standards are liberalised (twin conditions struck or read down) and if statements to ED officers are deemed inadmissible unless given voluntarily (should the Court reconsider the Section 50 issue in the future), the ED loses two major pressure tactics.

- **Potentially more rigorous preliminary investigation by the ED :** If the Court mandates that an ECIR be supplied at the time of arrest, the ED can no longer rely on secret "internal" records to initiate action. Investigators would have to ensure that by the time of arrest, they have a well-documented basis for the money laundering charge that can withstand scrutiny.

- **Burden of proof reversal:** If the Supreme Court overturns the reverse burden (Section 24), the ED will carry the burden to prove the 'tainted' nature of assets in attachment proceedings and

[1] *Vijay Madanlal Choudhary v. Union of India, (2023) 12 SCC 1*

at trial. This could significantly aid corporates and banks facing PMLA probes as they would no longer have to prove a negative (i.e. that their funds are clean) without knowing the full case.

- **Enhanced protection of personal liberty:** If the judgement is overturned, procedural lapses by the ED may start resulting in tangible relief for individuals, incentivising the agency to follow due process to the letter. Should the ECIR become a required disclosure, individuals will, at minimum, know what predicate offense and transactions they are being linked to. This knowledge enables them to seek prompt legal redress if the allegations appear baseless or outside PMLA's scope.

NCDRC holds that virtual digital assets cannot be treated to be a subject matter of consumer services and dealt with under the Consumer Protection Act, 2019

The National Consumer Disputes Redressal Commission (NCDRC) in Gurmeet Singh v. Zenmai Labs & Ors[2]. declined to exercise jurisdiction over consumer complaints related to WazirX. NCDRC held that claims involving cryptocurrency and any alleged deceptive conduct arising therefrom are not the subject of any express recognition or declaration by the legislature or by any judicial authority. The NCDRC found that the current regulatory framework surrounding cryptocurrencies, like those offered by WazirX, is unclear and not well-defined. It said that when it comes to fraud and investigation of crypto platforms which largely remain unregulated, the legal remedy is either a criminal complaint in a regular court or a civil complaint before the civil courts.

The implication of the NCDRC judgment for the victims of the WazirX scam who were the complainants before NCDRC is that they have to pursue remedies to recover their dues through civil courts and/or criminal courts.

Supreme Court affirms the need to protect foreign investments while ensuring fair trial for accused; overturns quashing of criminal proceedings against Daechang CFO

In Hyeoksoo Son[3], Moon June Seo , the Supreme Court set aside the Karnataka High Court's order quashing criminal proceedings against the former CFO of Daechang Seat Automotive Ltd., the Indian subsidiary of South Korea based Daechang Seats, a supplier of car seats for Kia Motors.

The case involves allegations of private sector corruption. In 2022, the CFO allegedly diverted company funds amounting to INR 9.73 crores to the company's Chartered Accountant firm under the pretext of GST payments. Investigations revealed that the funds were misappropriated, with the CFO receiving a cash kickback of INR 1.8 crores from the CA firm during May and June 2022. Based on these findings, the company filed a criminal complaint against the CFO, employees of the accounts department, and the CA firm.

While the Karnataka High Court had quashed

[2]*Consumer Complaint No. 7 of 2025, National Consumer Disputes Redressal Commission, Order dated 13th March, 2025*
[3]*2025 SCC OnLine SC 759*

the complaint under Section 482 of the CrPC, the Supreme Court reversed this decision and directed that criminal proceedings against the CFO should continue.

The case demonstrates the judiciary's stance that foreign investors' funds require robust legal protection. It also underlines that corruption within the private sector, particularly involving internal finance officers, can attract penal sections such as criminal breach of trust, even if not public servant, so long as fiduciary capacity and misappropriation claims exist. Further, the judgment essentially lowers the bar for criminal proceedings involving foreign investment or large sums, encouraging full adjudication rather than premature disposal. From a defense vantage point, the focus will shift to trial readiness.

PMLA accused is entitled to documents not relied upon by ED during prosecution

In the case of Sarla Gupta and Anr. v. Directorate of Enforcement[4], the Supreme Court ruled that an accused is entitled to receive a list of documen ts and statements collected by the ED during an investigation under the provisions of PMLA, even if these materials are not ultimately relied upon in the prosecution complaint, reinforcing the procedural safeguards available to the accused under the PMLA.

The Supreme Court extended this right to bail hearings as well. It held that during the bail stage in proceedings under PMLA, an accused may seek non-relied-upon documents under Section 91 CrPC, but the ED can resist disclosure if it shows that doing so may prejudice an ongoing investigation. However, once the investigation is complete, the ED cannot withhold such documents on that ground.

This ruling came in an appeal challenging a Delhi High Court order from 2019, holding that the prosecution is obligated to supply only those documents referred to and relied upon in the complaint or chargesheet. The accused sought access to "unrelied upon" documents to facilitate their defense.

The Supreme Court emphasised that for a fair trial, the accused must have knowledge of all evidence, including those that the prosecution chooses not to use, to prepare an effective defense.

The judgment will usher in transparency and accountability, reducing opacity in investigations and limiting surprise evidence. To withstand court scrutiny, ED must compile and submit a more detailed and legible set of documents upfront. It will lead to enhanced access to information for the accused, and opportunity to the accused to challenge procedural omissions (failure by ED to provide these materials can form grounds for motions to quash or discharge).

Stamp Vendors are "Public Servants" under the Prevention of Corruption Act, 1988

In the case of Aman Bhatia v. State (NCT of Delhi) [5], the Supreme Court held that a stamp vendor falls within the definition of "public servant" under the Prevention of Corruption Act, 1988. The Court reiterated well-established principles that the

[4] *2025 SCC OnLine SC 1063*
[5] *2025 SCC OnLine SC 1013*

nature of the duty discharged, rather than a fixed employment status, is paramount in determining "public servant" status. It observed that stamp vendors perform an important public duty by facilitating government revenue collection through stamp duty and receive remuneration through discounts on stamp paper procurement. This remuneration, governed by government rules, qualifies them as "remunerated by the government" for the purposes of Section 2(c)(i) of PCA, thus extending the ambit of anti-corruption legislation.

The Court also reaffirmed another key principle, i.e., a conviction for bribery cannot rest solely on recovery of tainted money or positive phenolphthalein tests. What is indispensable is an active demand for gratification by the public servant, proven beyond reasonable doubt. In this case, the prosecution's failure to establish a demand led to the acquittal of the stamp vendor.

This decision sets a dual precedent - it widens the ambit of the Prevention of Corruption Act by including regulated public-facing roles; and it underscores stringent proof standards, particularly the necessity of proving bribery demand. For legal practitioners, the implications will be twofold: enforcement agencies may broaden their target base, while defense counsel must reinforce demand-related defenses and exploit evidentiary deficiencies to secure acquittal or dismissal.

Supreme Court upholds bank's liability for fraudulent transactions from customer's bank account

IIn SBI v. Pallabh Bhowmik[6], the Supreme Court underscored the crucial responsibility of banks to protect a customer's bank account from fraudulent and unauthorised transactions. The Court upheld the bank's liability in a case where a customer experienced fraudulent activity in his bank account with SBI.

In 2021, a customer downloaded an app to process a refund which resulted in three unauthorised online transactions in the customer's SBI account. On the same day, the customer reported the matter to the customer care. However, the bank did not take steps to stop the transfer. The customer also filed complaints with the Assam Police and the National Cybercrime Reporting Portal and eventually approached the Ombudsman under the RBI Integrated Ombudsman Scheme, 2021. The Ombudsman came to a finding that the bank was not liable to compensate the customer for the fraud. The customer challenged the Ombudsman's decision before the High Court of Gauhati and a Single Judge of the Gauhati High Court set aside the Ombudsman's decision and directed SBI to deposit the amount fraudulently transferred to the customer's bank account. SBI challenged the Single Judge's order before a Division Bench of the Gauhati High Court who dismissed the appeal. SBI filed a second appeal before the Supreme Court which upheld Gauhati High Court's order.

The Supreme Court relied on RBI's July 2017 Circular titled "Customer Protection- Limiting Liability of Customers in Unauthorised Electronic Banking Transactions" which states that in case of unauthorised electronic banking transactions occurring due to third party breaches i.e., where the deficiency neither lies with the customer or the bank, the customer liability will be "zero" if the fraudulent transaction is reported within three working days from the date on which the customer receives the communication.

This is a landmark judgment affirming that banks bear full liability for fraudulent and unauthorised electronic withdrawals in specific circumstances. The ruling highlights that even if a customer's actions might have inadvertently contributed to the fraud, the bank's inherent responsibility to ensure transaction security remains paramount, particularly when the fraud is reported by a customer to the bank promptly. Consumers now have clearer grounds to demand restitution swiftly if fraud occurs and is timely reported.

[6]*Special Leave to Appeal (C) No. 30677/2024, Supreme Court of India, judgement dated 3rd January, 2025*[5]*2025 SCC OnLine SC 1013*

ABOUT KHAITAN & CO

Khaitan & Co is a top tier and full-service law firm with over 1300+ legal professionals, including 300+ leaders and presence in India and Singapore. With more than a century of experience in practicing law, we offer end-to-end legal solutions in diverse practice areas to our clients across the world. We have a team of highly motivated and dynamic professionals delivering outstanding client service and expert legal advice across a wide gamut of sectors and industries.

To know more, visit www.khaitanco.com