SALOT & SHAH ASSOCIATES

NEWSLETTER

APRIL 2025

ABOUT NEWSLETTER

Presenting 8th edition of our newsletter!

We are thrilled to share the latest updates and industry insights.

In this edition, we highlight significant developments and offer practical tips to help companies stay ahead.

Your trust and support inspire us to continually enhance our services and deliver the best possible experience.

CONTACT US

www.salotandshah.com

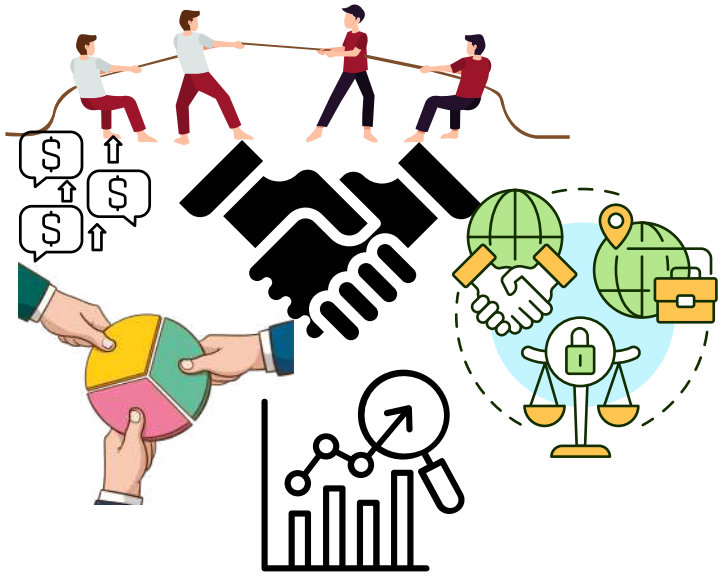
info@salotandshah.com

+91 – 93286 69090

STRENGTHENING MARKET INTEGRITY: CCI PROBES 35 CARTEL CASES ACROSS SECTORS

INTRODUCTION

In India's liberalised and competitive economy, fair market conduct is essential for consumer welfare, economic efficiency, and business integrity. However, cartelisation remains a serious threat. The Competition Commission of India (CCI) recently disclosed investigations into 35 cartel cases over the past five years, highlighting its ongoing efforts to detect and dismantle such arrangements. This reflects the growing strength of anti-cartel enforcement in India, supported by legislative reforms, advanced investigative tools, digital evidence, and economic analysis.



UNDERSTANDING CARTELISATION: LEGAL AND ECONOMIC CONTEXT

Cartelisation involves agreements or understandings between competitors to manipulate market variables such as price, supply, production, or market allocation. These arrangements are typically informal and covert, often facilitated through trade associations, with the aim of reducing competition and maximising profits at the cost of consumers. Under Section 2(c) of the Competition Act, 2002, a cartel is defined as an association of producers, sellers, or service providers who, by agreement, seek to control aspects of trade such as production or pricing. Section 3(3) further presumes such agreements to have an appreciable adverse effect on competition (AAEC), shifting the burden of proof to the parties involved. What sets cartels apart from other anti-competitive practices is the degree of collusion and the serious harm they cause to market integrity. Activities like price-fixing, bid rigging, and market allocation are regarded as "hardcore" violations and are subject to the highest scrutiny and penalties by the Competition Commission.

SECTORAL PATTERNS AND INVESTIGATIVE CHALLENGES

The CCI's recent investigations reveal that cartelisation remains a recurring concern in several key sectors. The cement and steel industries have often been found to be susceptible to collusion due to the relatively small number of major players, standardisation of products, and high entry barriers. In these sectors, instances of coordinated price increases and production restrictions have raised red flags, with several investigations revealing parallel conduct suggestive of tacit or express collusion.

The pharmaceutical distribution sector has also drawn regulatory attention, particularly where trade associations have allegedly imposed restrictive conditions on suppliers and prevented the appointment of new stockists. These practices not only restrict competition but also adversely impact access to essential medicines, thereby implicating public interest.

WAY FORWARD

The Competition Commission of India (CCI) is empowered to impose stringent penalties on entities found guilty of cartelisation, including fines of up to ten percent of their average turnover over the past three financial years or three times the profit made from such conduct, whichever is higher. Individuals in key managerial positions may also be held personally liable. Additionally, the Commission may issue cease-and-desist orders, and affected parties may initiate follow-on actions in civil courts based on the Commission's findings. The Competition (Amendment) Act, 2023 has further strengthened the enforcement framework by introducing settlement and commitment mechanisms. The CCI's disclosure of having investigated 35 cartel cases over five years highlights the continued prevalence of collusion in critical sectors. In a rapidly expanding and interconnected economy, regulatory vigilance and proactive compliance by businesses are essential to preserving competitive market conditions.

INDIA'S CRACKDOWN ON CALLER ID SPOOFING: DOT'S DIRECTIVE TO SOCIAL MEDIA PLATFORMS

UNDERSTANDING CALLER ID SPOOFING

Caller ID spoofing is defined as a technique in which the caller tampers with the mechanism of passing the identity so that it does not appear to him and is displayed wrongfully on the caller ID. For example, when you receive a call from someone whose identity indicates that the call was made from your bank or your child's school, it may actually be from a scammer sitting halfway across the country–or even the world. This is actually used for committing a fraud or impersonation of a trusted institution for extraction of sensitive information or for tricking into payments or malicious application downloads.

WHY THE URGENCY?

With the appearance on various websites, video streaming platforms, and app marketplaces of videos and online tutorials that demonstrate or promote spoofing tools, the advisory from the Department of Telecommunications is well-timed. The pros offered by these tools, often merely called harmless call apps, are spoof phone calls or prank calls. Some put it down to playful activity or privacy measures, but they often find this very means for committing awful crimes. The government therefore recognizes this gap and is now busy plugging it rigorously and legally. The crackdown by the government aims to protect consumers like us from rising levels of fraud. Scammers have become ever so sophisticated; and ever so personal, that even a simple call can turn into a threat. A call appearing to originate from a long-trusted credit card company contact—yet in reality, placed by a fraudster—demonstrates the alarming effectiveness of caller ID spoofing. That's how convincing caller ID spoofing can be. By getting rid of the tools to practice it, the government puts the onus on social media platforms and draws the line on what is acceptable in the digital communications space.

THE DOT'S ADVISORY AND ITS IMPLICATIONS

The DoT's advisory comes in the wake of incidents where social media influencers demonstrated methods to alter Calling Line Identification, effectively promoting tools that enable such tampering. Recognizing the potential for misuse, the DoT has underscored that any application or content facilitating the alteration of telecom identifiers—be it Calling Line Identification, IP addresses, or International Mobile Equipment Identity numbers—constitutes a violation of the Telecommunications Act, 2023.

Under the Telecommunications Act, 2023, particularly Section 42, any act of tampering with telecom identifiers is illegal. This includes manipulation of Calling Line Identification which is the phone number that shows up on your screen, International Mobile Equipment Identity number which is a unique identifier of mobile phones and IP addresses which is used for internet communication Here's what the law says about the consequences:

- Such offenses are cognizable and non-bailable.
- Offenders can face up to 3 years of imprisonment, a fine of up to ₹50 lakh, or both.

Responsibilities of Platforms: Social Media and hosting application platforms must immediately take down any content and applications that promote or facilitate tampering with telecom identifiers. Also, inaction shall attract legal liability upon the platform itself as it amounts to abetment of perpetration of the crime.

Deadline for Compliance: The date by which compliance report needs to be sent by platforms to the DoT shall be February 28, 2025 confirming removal of such content and applications.

INDUSTRY REACTIONS

The advisory has given rise to forceful reactions in the tech ecosystem:

- For some cybersecurity experts, this represents a long-awaited measure to deter fraud.
- Others think it could lead to overreach while privacy advocates say: Transparent and equitable content moderation is in order.
- Tech platforms are caught in a bind-they must balance enabling user expression and complying with legal frameworks.

LOOKING BEYOND: THE WIDER CONTEXT

The DoT's advice is general and not isolated for just one application or video; it is part of the much bigger change in India's digital safety and accountability policy. India is currently building the legal backbone for a more secure, transparent, and trustworthy communication ecosystem with the introduction of the Telecommunication Act, 2023, which reflects India's proactive stance toward the ever-evolving nature of covetous cyber threats and digital fraud.

In the past, calls like caller ID spoofing or IP manipulation might have been viewed as technical violation or user-level pranks, but now such injustice is being termed national security crimes with financial implications. The state is in fact teaching that national priority should be paid to cyber fraud and it is no longer a low-priority issue. It is a national-level threat that needs serious attention and strong enforcement.

SEBI AMENDS INVESTMENT ADVISER REGULATIONS TO ADDRESS AI-RELATED RISKS: A LEGAL PERSPECTIVE

INTRODUCTION

In the growing and fast learning world, where Artificial Intelligence (AI) is increasingly getting involved financial services, our country's Securities and Exchange Board (SEBI) has taken a huge step by amending the Investment Adviser Regulations to mitigate the emerging risks posed by AI-driven investment advisory. This move is necessary, reflecting the regulator's awareness of evolving technologies and its commitment to investor protection in a digital economy.

AI has brought unprecedented capabilities to investment advisory services. From robo advisors that offer portfolio balancing to predictive analytics tools that forecast market trends, the use of AI has become pervasive. Startups and legacy firms alike are leaning on algorithms to offer scalable, customized financial advice. While these developments enhance efficiency, they also pose unique risks ranging from algorithmic bias to lack of transparency, and from data misuse to systemic errors.

Unlike human advisors who can be held directly accountable, algorithms lack judgment and empathy. Their opaque functioning; often described as "black box" decision-making creates challenges in assessing their reliability and compliance. SEBI's recent amendments acknowledge these challenges and attempt to lay down a more robust framework to govern the responsible deployment of AI in investment advisory.

OVERVIEW OF THE AMENDMENTS

The new amendments to the SEBI (Investment Advisers) Regulations primarily focus on four broad areas:

1. Disclosure Obligations Regarding AI Use
2. Accountability and Oversight
3. Data Privacy and Algorithmic Transparency
4. Grievance Redressal and Risk Management

These changes seek to strike a balance between encouraging innovation and safeguarding investors from potential harm.

MANDATORY DISCLOSURE OF AI TOOLS AND THEIR ROLE

One of the central features of the amendment is the requirement for registered Investment Advisers (IAs) to disclose the use of AI or machine learning tools in their advisory process. This includes clearly informing clients whether the advice is fully or partially automated, and explaining the nature and limitations of such advice.

This move enhances transparency and enables clients to make informed decisions about the source and reliability of their financial advice. More importantly, it allows SEBI to monitor the spread and impact of AI tools in the investment ecosystem, thus laying the groundwork for future policy refinements.

INCREASED ACCOUNTABILITY FOR ALGORITHM-DRIVEN ADVICE

The amendments place the onus on IAs to ensure that AI tools used in advisory services are compliant with SEBI's broader regulatory objectives. The "responsibility cannot be outsourced" principle has been reinforced—meaning that even if an algorithm provides the advice, the registered IA is accountable for the outcomes.

This has far-reaching implications. Investment advisers must now implement regular audits and validation checks of their AI tools. They also need to have qualified personnel who understand the algorithmic models and can intervene if anomalies arise. This raises the bar for operational preparedness and technological due diligence within advisory firms.

DATA PRIVACY AND ALGORITHMIC GOVERNANCE

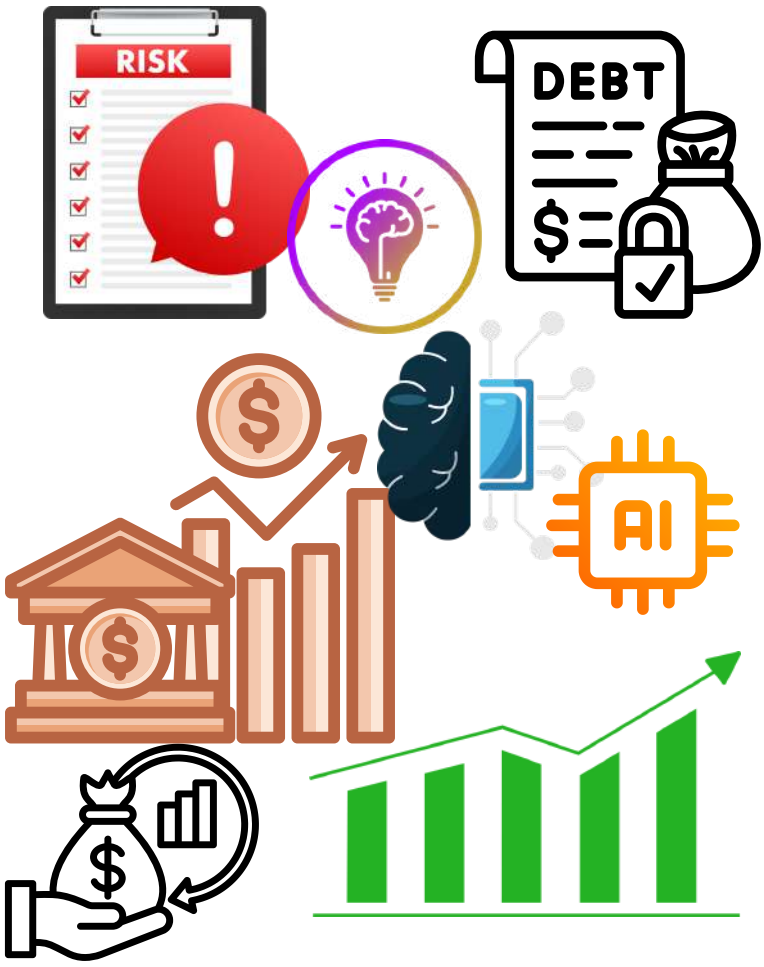
SEBI's amendment also touches upon the delicate issue of data protection. Since AI tools rely heavily on client data; often sensitive and personal; SEBI mandates that IAs put in place robust data governance frameworks. This includes securing client data from breaches, ensuring data is collected with consent, and not misused for purposes beyond the advisory scope.

Furthermore, firms are expected to develop a "model governance framework" to track and document algorithmic behavior. This may encompass decision tree logs, the reasoning behind advice generation, and mechanisms for real-time monitoring of model drift (i.e., changes in AI model performance over time). Although these technical elements may be unfamiliar to many financial advisors, SEBI's initiative is steering the industry toward more responsible and transparent use of AI.

RISK MANAGEMENT AND GRIEVANCE REDRESSAL

To complement the above measures, SEBI has insisted that IAs establish comprehensive risk management frameworks for AI use. These should cover risk identification, mitigation protocols, fallback mechanisms in case of AI failure, and contingency plans to ensure service continuity.

Importantly, a separate channel for AI-related grievance redressal must be maintained. Clients should have recourse to human intervention when they face problems arising from automated advice. This ensures that technology does not alienate investors but rather serves them effectively and ethically.



IMPLICATIONS FOR THE INDUSTRY

The regulatory change signals a shift in SEBI's approach from passive observation to active governance of AI in finance. While some may view this as a compliance burden, it is, in fact, a much-needed foundation for sustainable innovation. It prevents the misuse of AI under the guise of automation and levels the playing field for firms that genuinely invest in responsible technology deployment.

For legal professionals and compliance officers, this amendment demands a proactive approach. Internal policies must be updated, third-party vendor contracts revisited (especially those involving AI tools), and data protection practices realigned with both SEBI guidelines and the evolving data protection framework in India.

CONCLUSIVE THOUGHTS

SEBI's amendments are a welcome move in anchoring technological advancements to legal accountability. As AI becomes integral to financial decision-making, regulatory oversight must evolve in parallel. By mandating transparency, governance, and accountability in AI-led investment advisory, SEBI has taken a decisive step toward future-proofing investor protection.

This also sets a precedent for other regulatory bodies across domains demonstrating that innovation and regulation can, and must, coexist. In the long run, such balanced regulatory frameworks will strengthen trust in AI systems and promote their ethical adoption in India's financial sector.