IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Insider Trading In The Digital Era: Algorithmic Trading, Social Media Tipping, And Cryptocurrency Markets

Tuhina Chaturvedi[1], Dr. Neelesh Sharma[2]

[1]Research Scholar, Department of Law, Rabindranath Tagore University, Bhopal, M.P.

[2]Dean, Department of Law, Rabindranath Tagore University, Bhopal, M.P.

Abstract: The rapid evolution of digital financial markets—driven by algorithmic trading, cryptocurrencies, NFTs, and social-media-driven investing—has created profound challenges for traditional insider trading regulations. Legal frameworks such as India's SEBI (Prohibition of Insider Trading) Regulations, 2015 (as amended in December 2024), the U.S. theories of classical and misappropriation insider trading, and the EU/UK Market Abuse Regulation (MAR) were primarily designed for conventional securities markets. These frameworks now face significant stress in addressing new forms of material non-public information (MNPI), including digital data exhaust, algorithmic signals, and influencer-driven financial communication. This paper investigates whether existing PIT/MAR regimes adequately address insider trading risks in these digital contexts and explores the regulatory gaps that emerge when social media "finfluencers," algorithmic pipelines, and alternative data sources blur the line between public and non-public information.

The study makes three key contributions: first, it provides a cross-jurisdictional synthesis of insider trading law in India, the United States, and the European Union; second, it integrates legal analysis with market microstructure insights on algorithmic trading, high-speed data flows, and crypto-asset markets; and third, it develops a compliance blueprint for market participants that balances deterrence, innovation, and fairness. By mapping how digital information becomes "inside information" within algorithmic pipelines, this paper advances a more nuanced understanding of market integrity in the digital age and proposes regulatory strategies that can better safeguard investor trust while enabling technological progress.

Keywords- Insider Trading; Market Abuse Regulation (MAR); SEBI PIT Regulations; Algorithmic Trading;

I. Introduction

Insider trading laws have traditionally included law, economics, and ethics. Insider trading is unfair since it allows select people access to confidential information and profits while normal investors lose[i]. The meaning, acquisition, and abuse of "inside information" have changed in the digital age. The digital microstructure of financial markets nowadays includes algorithmic execution, globalised trading platforms, and lightning-fast data transfer. This development has made it harder for regulators to detect, verify, and punish insider trading employing encrypted chat systems, cryptographic assets, or machine learning models.

The volume and pace of digital market information flows exacerbate these regulatory difficulties. When traditional enforcement methods were devised, press statements or filings were the main way to disclose market-moving information, and brokers or manual trade execution were common. It may be harder to distinguish between legitimate research and illicit MNPI access because algorithms that can sift through satellite images and web traffic can trade in microseconds. New social media influencers called "digital tippees" or "finfluencers" may break securities regulations by disclosing or pushing securities to large audiences. Finally, insiders are exploiting the regulatory hole created by bitcoin markets and NFT platforms, which makes enforcement difficult. Many of these assets do not meet typical security criteria.

Research Questions. Against this backdrop, the present paper addresses several pressing questions:

1. Do existing insider trading frameworks, such as the SEBI (Prohibition of Insider Trading) Regulations, 2015 in India and the Market Abuse Regulation (MAR) in the European Union, adequately cover emerging asset classes such as cryptocurrencies and NFTs?
2. How should regulators conceptualize “inside information” in a digital environment where algorithms, alternative data, and platform listings generate market-moving insights?
3. What legal standards should govern the role of social-media influencers in securities markets, and how should enforcement adapt to the viral, cross-border spread of financial tips?
4. Can compliance frameworks be retooled to address algorithmic governance, social media risks, and digital asset listings without stifling market innovation?

2. Legal and Theoretical Background

2.1 Foundations of Insider Trading Law

Insider trading laws are predicated on the idea that all investors should have equal access to market-changing information. The SEBI (Prohibition of Insider Trading) Regulations, 2015, last revised in December 2024, regulate this field in India. According to these rules, mergers, acquisitions, financial performance, dividends, and capital structure changes are UPSI[ii]. SEBI limits trading-window limits on specified persons, enforces enterprise codes of conduct, and requires structured digital databases (SDDs) to track UPSI access. The Indian system is getting better at spotting WhatsApp groups and Telegram channels as data breaches.

US insider trading law is based on judicial doctrine. Classical theory holds that trading equities based on MNPI violates shareholder fiduciary duty (Cirella v. United States, 445 U.S. 222 (1980)). Taking confidential information without authorisation can make outside parties responsible under the misappropriation principle, established in United States v. O'Hagan, 521 U.S. 642 (1997). These concepts allow U.S. regulators to prosecute many insider trading crimes. SEC v. Wahi (2023-2024), a cryptocurrency listing case, applies these theories.

The EU's Market Abuse Regulation (MAR) prohibits trading based on unlawful disclosure, market manipulation, and inside information. Because MAR applies to all asset classes and trading venues, ESMA can dynamically interpret responsibilities. The EU has strengthened its system with sectoral laws like REMIT II (2024/1106) for wholesale energy markets to address algorithmic threats.

2.2 Material Non-Public Information in Digital Settings

Digital MNPI definition is harder. UPSI in India used to handle financial data and business announcements, but geolocation pings, web-scraping outputs, and metadata about upcoming product releases are also market-moving[iii]. American courts are likewise scrutinising whether complex analytics data is "non-public". Separating authentic market research from leaked or stolen material is difficult. Even algorithmic models based on secret data can reveal digital market insider information. MNPI could include algorithmic predictions by a trading company with early order-book depth via privileged exchange links. Insider information about upcoming token listings or exchange integrations can be valuable even though cryptocurrency regulations are still developing.

2.3 Market Integrity and Information Asymmetry Theories

Three primary justifications underlie insider trading prohibitions:

Market Efficiency: Allowing insiders to trade erodes trust in market pricing, leading to distortions in liquidity and capital allocation.

Fairness: Investors expect a level playing field; insiders exploiting confidential information undermine public confidence in financial markets.

Deterrence and Enforcement: Strong insider trading rules deter misconduct, reduce information asymmetry, and uphold market reputation.

These assumptions are still valid in the digital era, but we should reconsider. Retail investors influenced by social media "finfluencers" are now part of the fairness conversation, and algorithmic order routing and bot strategy collaboration are part of efficiency.

3. ALGORITHMIC AND HIGH-SPEED TRADING

3.1 Where Algorithms Intersect with Insider Rules

Algorithmic trading—computer algorithms executing orders—now facilitates most securities transactions. Algorithms can process metadata and structured data in milliseconds and find arbitrage possibilities. Insider trading regulations apply to algorithms that use confidential information. A trading company with access to non-public exchange data streams and predictive models could make profitable trades using unfair advantages.

To prevent purposeful or inadvertent insider trading, algorithms need pre-trade risk controls. Companies must have algorithm development control, regularly check their data sources, and include "kill-switches" to stop anomalous activity. Without these safeguards, algorithms may use manipulative or insider-influenced methods.

3.2 EU Developments: REMIT II and ESMA Guidance

The EU is proactive about algorithmic dangers. REMIT II (Regulation (EU) 2024/1106) requires market parties to report suspicious orders and transactions, including algorithm-generated ones[iv]. High-frequency trading, especially with stacked or swiftly cancelled orders, can disguise insider-driven strategies, prompting this modification.

In addition, ESMA plans to publish algorithmic pre-trade control requirements in 2025 as part of MiFID II. The goals are algorithmic developer governance, automatic alert system standardisation, and maximum order-to-trade ratios. Adding insider-risk factors to algorithmic trading's design marks a shift from reactive enforcement to preventive monitoring.

3.3 Risk Scenarios in Algorithmic Trading

Several risk scenarios highlight the complexity of insider trading in algorithmic environments:

Data Leakage into Models: Algorithms trained on datasets that include confidential information—whether intentionally or inadvertently—may generate trading signals that constitute insider trading.

Alternative Data Exploitation: Use of unconventional datasets, such as satellite imagery of retail parking lots or web-scraped supplier information, raises questions about whether such data qualifies as non-public and material. While often lawful, it risks straying into the realm of UPSI if obtained through illicit means.

Collusive Botnets: Multiple algorithms programmed to share information or trade in coordination can mimic collusive behavior, amplifying insider advantages.

Dark Pools and Venue Information: Privileged access to dark-pool order flows or venue-specific latency advantages can constitute non-public information, creating an uneven playing field for market participants.

4. Social Media Tipping and "Finfluencers"

4.1 Conceptual Map: Tipping, Touting, and Conflicts of Interest

New market manipulation, insider trading, and tipping have developed since financial communication went digital. Popular people on Twitter (now X), YouTube, Instagram, and Telegram can share financial ideas and essential information with a large audience[v]. Unlike traditional financial analysts, many finfluencers work internationally, are unregulated, and make money from their audience through concealed sponsorships and affiliate links.

The deliberate or inadvertent release of private or sensitive information online is called "tipping". "Touting" is aggressively promoting a security for unknown income, whereas "pump-and-dump" is a social media operation that urges normal investors to buy inflated positions before insiders sell for a profit. The frequency of undeclared conflicts of interest in influencer culture raises severe regulatory concerns. Influencers may hold securities they recommend, earn promotional prizes, or benefit from sponsored trading platforms. These approaches erode market integrity and blur the boundary between authorised financial education and illicit manipulation.

4.2 UK/FCA: FG24/1 and Crackdown on Social Media Promotions

UK's financial watchdog, the FCA, is addressing social media marketing issues. In 2024, the FCA released FG24/1, its final rules for applying the UK financial promotional framework to social media. The letter stressed that financial promotions must be honest, straightforward, and not misleading regardless of media. Importantly, the suggestions warned against "click-bait" like jokes and short films that simplify investing products.

In late 2024 and early 2025, the Financial Conduct Authority (FCA) warned greater fines and enforcement against content producers and finfluencer employers[vi]. The Financial Times reported on Parliament's growing worry over influencers promoting high-risk products like crypto-assets and CFDs. In 2025, the FCA initiated coordinated enforcement sweeps that warned TikTok and Instagram users that creating fals e or misleading claims might result in criminal or civil charges.

Instead of banning financial information on social media, authorities should hold investment promoters to professional standards. The FCA wants to establish this regulatory structure. This aligns the influencer economy with financial advisors, but with the added element of viral communication.

4.3 India/SEBI: Scrutiny of Finfluencers and Enforcement Climate

The scenario in India is similar. As millions of individual traders join the stock and derivatives markets via cheap internet platforms, social media commentators' influence has expanded. After understanding the risks, the Securities and Exchange Board of India (SEBI) began investigating influencers' duties in 2024–2025, especially when promotional content was tied to concealed broker arrangements or sponsored partnerships[vii]. The Economic Times said that SEBI aims to regulate this market by enhancing transparency, demanding disclosures, and exploring ways for influencers and financial intermediaries to share responsibility.

SEBI now relies on the 2015 Prohibition of Insider Trading (PIT) Regulations and research analyst and registered investment adviser advertising laws. Most finfluencers don't follow this paradigm, hence there are enforcement loopholes. SEBI is considering registering or disclosing financial ad influencers like investment advisers. SEBI has tightened enforcement to show it is willing to apply insider-trading principles to digital platforms. Trading restrictions and fines have resulted from Telegram stock-promotion groups.

4.4 Compliance: Templates, Platforms, and KOL Vetting

Several organised approaches could lessen influencer economy concerns from a compliance perspective. Influencers should use standard disclosure templates first. This would show when they own securities or receive pay for promotional content. Second, platform duties matter. Like consumer advertising content censors, social media corporations can

Table 1 : Comparative Obligations for Social-Media Investment Content

Regime	Scope	Key Obligations	Penalties
FCA FG24/1 (UK, 2024)	All social media promotions	Must be fair, clear, not misleading; risk disclosures required	Civil/criminal liability; fines
SEBI PIT + advertising code (India)	Registered advisers, analysts, influencers under review	UPSI prohibition; disclosure of holdings/compensation; no misleading claims	Monetary penalties; trading bans
SEC (U.S.) Rules	Investment advisers, promoters, influencers	Mandatory disclosure of compensation (Securities Act §§ 17(b)); prohibition on fraud/touting	SEC enforcement; DOJ prosecutions

5. Cryptocurrency and NFTs

5.1 Doctrinal Tension: Securities vs. Commodities

Insider trading regulations face new challenges with cryptocurrencies and NFTs due to their unclear legal classification. The CFTC considers some tokens commodities in the US, but the SEC says many meet the Howey test for securities. Tokens may not be securities, therefore securities insider trading laws may not apply, generating confusion. To avoid defining insider trading, regulators have used wire fraud theories and broad anti-fraud rules to seek comparable penalties.

This tension has major enforcement and compliance implications. Since market participants can't predict if an NFT or token will be regulated, they face ex post liability[viii]. Due to this uncertainty, defendants may unfairly argue that the law was not clear when the action happened.

5.2 Key U.S. Cases

Two recent U.S. cases illustrate the frontier of insider trading enforcement in digital assets.

SEC v. Wahi et al. (2023–2024): This lawsuit involved former Coinbase product manager Ishan Wahi, who told his brother and a friend about upcoming cryptocurrency listings. The SEC charged the defendants for insider trading "crypto asset securities." In 2023, the SEC settled with Ishan and Nikhil Wahi, while in 2024, Ramani, the third defendant, defaulted. This case was the first SEC insider trading case involving crypto asset securities, setting a precedent for crypto securities regulation.

U.S. v. Chastain (OpenSea/NFTs): In 2023, former OpenSea product manager Nathaniel Chastain was found guilty of money laundering and wire fraud for selling NFTs he knew would be shown on the homepage[ix]. Due to flaws in jury instructions about "property" and "commercial value," the Second Circuit overturned the conviction on July 31, 2025. This verdict has major implications for how insider trading theories are used to NFTs and if NFT listings' private company information is fraud "property".

Together, these cases underscore both the creativity of regulators and the doctrinal fragility of insider trading enforcement in digital asset markets.

5.3 Regulatory Trajectory

Aft er the Chastain judgment, authorities will have to reconsider their prosecution strategies, including jury training and whether NFTs are securities or other regulated assets. Clear legal standards that treat token listing information as confidential, regardless of securities status, could be implemented. The dependence on platform-based laws requires exchanges to regulate the trading and secrecy of staff and contractors with listing pipeline access.

Geofenced tokens also complicate cross-border transactions by permitting some nations to supply assets and others not. When a token is a security in one jurisdiction but not another, enforcement may be uneven. International regulator coordination is needed to prevent regulatory arbitrage, where insiders use inconsistent definitions.

Step 1: Is the token a security under Howey/MAR? → If yes, apply securities insider trading rules.

Step 2: If not, is there confidential property information (listing pipelines, business plans)? → If yes, prosecute under wire-fraud/ML statutes.

Step 3: If neither, consider bespoke crypto regulation.

6. India Focus: SEBI's Evolving PIT Regime

6.1 SEBI (PIT) Regulations 2015 and 2024 Amendments

India's central insider trading law is the SEBI (Prohibition of Insider Trading) Regulations, 2015, last revised in December 2024. The amendments expanded the use of Unpublished Price Sensitive Information (UPSI), tightened SDD maintenance requirements, and increased controls over directors, workers, and associated intermediaries[x]. Companies must now arrange blackout periods if they do not have financial results or major events to disclose within the defined timeframe.

Enterprises must monitor and document UPSI access through digital communication channels under the 2024 revisions. A fundamental innovation. SEBI acknowledges that WhatsApp leaks and Telegram recommendations have made insider trading in India common.

6.2 Digital-Era Challenges

SEB I still has to improve the PIT framework for internet markets notwithstanding these modifications. First, regulators must use metadata, screenshots, or voluntary disclosures to piece together encrypted chat system evidence, making data collection harder. Second, social media tip groups raise collective action problems. In these organizations, numerous people send UPSI pieces to avoid detection. Third, robo-advisers and AI-driven trading proposals add ambiguity. An algorithm analyzing UPSI without human intent ambiguously defines lability.

Indian retail investors are increasingly adopting offshore cryptocurrency platforms, which puts them at risk of insider trading in unregulated countries. SEBI lacks extensive jurisdiction to regulate offshore digital asset trade, despite its warnings.

6.3 Enforcement Themes and Gaps

SEBI's enforcement activities have recently shared themes. Systematic evidence gathering is becoming more important, such as the requirement that firms preserve digital audit trails of UPSI access. Still, connecting in an encrypted environment is difficult. Lack of cross-border cooperation is another concern[xi]. Foreign authorities like the SEC or FCA must oversee insider trading schemes involving crypto exchanges, offshore corporations, or cross-listed securities.

Finally, SEBI must decide whether to explicitly require digital asset traders and influencers to assume PIT duties. Despite advances in 2024, a comprehensive law reform may be needed to cover social media tipping, algorithmic trading, and crypto exposure.

7. Comparative Framework & Case-Law Matrix

Comparing India, the US, and the UK/EU insider trading laws shows similarities and contrasts. According to SEBI's PIT Regulations, 2015 (as revised in 2024), UPSI includes financial outcomes, dividends, capital structure changes, mergers, and important events. The Securities Exchange Act of 1934 (Section 10(b)) and Rule 10b-5 highlight misappropriation or breaches of fiduciary duty involving critical, non-public information, which inspired the US SEC/DOJ framework. The EU Market Abuse Regulation (MAR, 2016), which was in force in the UK before Brexit and is mirrored in FCA recommendations, defines inside information as accurate, non-public knowledge that could significantly affect price. Energy market REMIT II uses MAR reasoning for commodity standards.

U.S. enforcement has classed Coinbase token listing data as "crypto asset securities" UPSI (SEC v. Wahi), and SEBI has lately prioritized structured digital databases to capture listing pipelines as UPSI. Listing information treatment is uncertain. European MAR standards treat listing information as inside knowledge if it significantly affects price.

The FCA's FG24/1 directly regulates finfluencers under the financial promotions regime, while SEBI is working on required disclosure requirements. Different from how the FCA promotes on social media. Under Securities Act §17(b), the U.S. SEC enforces "touting" requirements that require compensation disclosure. While US courts are exploring fraud and property (e.g., U.S. v. Chastain), SEBI has issued investor alerts about cryptocurrency, while the FCA only prohibits the advertising of illicit crypto-assets. There are several penalties. SEBI has the authority to prohibit trading, impose fines up to INR 25 crore (≈USD 3 million), or quadruple earnings. The SEC and DOJ apply criminal, civil, and disgorgement penalties for wire fraud, with the maximum penalty being 20 years in jail. EU MAR administrative fines can reach €15 million, or 15% of a company's annual revenue[xii]. The two organizations also offer different whistleblower protections. The 2019 SEBI Informant Mechanism offers financial incentives but is less used than the SEC's powerful program that compensates whistleblowers with up to 30% of sanctions.

Table 2 : Comparative Obligations & Penalties

Dimension	India (SEBI)	US (SEC/DOJ)	UK/EU (FCA/MAR)
Definition of inside info	UPSI (Reg. 2015, amended 2024)	Material, non-public info (case law)	Precise, price-sensitive (MAR)
Listing data	Explicitly included (2024 SDD reforms)	Coinbase/Wahi precedent	MAR treats as inside info
Social media	PIT + finfluencer scrutiny	§17(b) touting rules	FG24/1 binding guidance
NFTs/DAOs	No statutory coverage	Chastain (vacated conviction, 2025)	Crypto promotions banned
Penalties	Up to INR 25 cr/3x gains	20 yrs prison; civil & disgorgement	€15m or 15% turnover
Whistleblowing	Informant Mechanism	SEC Whistleblower Program	Limited MAR protection

8. Compliance & Governance Playbook

For future-proof compliance, corporate governance, platform-level security, individual responsibility, and technology infrastructure must align. Companies still value current insider lists[xiii]. These directories should be current and include all UPSI-accessible consultants, auditors, and digital contractors. Businesses must record trading algorithm design, testing, and permission to avoid using large non-public datasets. Model-risk governance is necessary as algorithmic trading grows more prevalent in financial markets. Kill switches for trading algorithms allow organizations to stop activity if abuse is suspected, and audit trails should document all UPSI access, whether through emails, digital databases, or ephemeral messaging apps. Surveillance systems should notify firms to unusual pricing or volume spikes caused by abrupt social media activity to assist them understand and prevent manipulation.

Platforms and exchanges have the largest insider-trading risk from listing pipeline control. Digital asset exchanges should require personnel to sign confidentiality agreements, prohibit trading in securities before announcement, and enforce employee trading policies. The Wahi scandal taught Coinbase the importance of preventing pre-announcement trade leaks. Exchanges must also check suspicious asset trades before announcements.

Regulators say individuals and influencers will need disclosure, training, and record-keeping. Influencers should follow authorities' forms and disclose their assets and compensation. Companies with social media-active employees or contractors should implement UPSI do-not-post policies, conflict of interest training, and punishments for wrongdoing. Keeping drafts of posts or promotional contracts can help defeat enforcement inquiries.

Finally, technology is more crucial to compliance. Example: SEBI-mandated Structured Digital Database (SDD): centralised, immutable, timestamped, encrypted UPSI visitor records. Effective governance requires rules for alerting on anomalous communications or agreements, integration with trade monitoring systems, and mechanisms to keep ephemeral messages (WhatsApp, Telegram, Signal). Global organizations must create retention policies that comply with the GDPR, Indian IT rules, and SEC paperwork requirements.

9. Policy Recommendations

Discrepancies in doctrine and enforcement among jurisdictions require policy reforms. Digital asset regulators should first standardize "inside information" for these assets. Misclassification of tokens as securities and commodities creates uncertainty. A unified method would consider all asset classes inside knowledge for confidential listing, protocol update, and platform governance details. Platforms must evaluate and manage insider-risk controls before launching tokens or NFTs. Exchanges should certify audit procedures, staff trading constraints, and confidentiality safeguards before trade, like issuers certified prospectuses.

Third, social media safe havens may balance investment protection with free speech. Platforms that fail to oversee covert marketing may be liable, while influencers who follow disclosure templates—which state their roles, compensation, and risk warnings—may be protected. This f ollows SEBI's finfluencer discussions and FCA's FG24/1 guidelines.

To clarify this fourth issue, authorities should publish data-science standards defining algorithmic model outputs as inside information. UPSI could be an AI trading model's forecasts based on secret listing or non-public corporate data. Clearing such criteria is crucial in this age of machine learning-driven trading.

10. Methodology & Limitations

Doctrinal analysis and comparative regulatory scan are employed in this work. Statutes, regulations, and court decisions (such as SEC v. Wahi and U.S. v. Chastain) are the main legal resources. For doctrinal research, a mini-dataset of 2022-2025 enforcement activities in India, the US, and the UK/EU was analyzed. The data collection highlighted digital insider trading themes.

The ever-changing environment limits. Case law changes frequently, making NFT enforcement uncertain. This uncertainty in judicial interpretation is shown by the July 2025 Second Circuit Chastain opinion. Conflicts between the SEC and CFTC over token classification continue. Due to encrypted conversations and offshore platforms, authorities have limited investigation ability, and financial media generally rely secondary reporting instead of original information. Thus, the results are provisional and reflect August 2025 legislation and practice.

11. Conclusion

The paper explores the evolution of insider trading in the digital era, focusing on algorithmic trading, social-media tipping, and cryptocurrency markets. It highlights shared concerns and divergent enforcement strategies across jurisdictions. The U.S. courts, FCA, and SEBI are shaping crypto-asset insider trading, while the Chastain appellate ruling highlights the fragility of applying insider trading theories to digital assets. The policy imperative is to harmonize global definitions of inside information and expand compliance architectures to encompass digital platforms, influencers, and algorithms.

References

[i] Garno Z. Insider Trading Challenges in the Digital Era: Legal and Ethical Considerations for US Financial Market Regulation. Journal of Next-Generation Research 5.0. 2025 Mar 25.

[ii] Langenbucher K. Insider trading in Europe: from financial instruments to crypto-assets. InResearch Handbook on Insider Trading 2025 Jan 7 (pp. 301-326). Edward Elgar Publishing.

[iii] Bizzi L, Labban A. The double-edged impact of social media on online trading: Opportunities, threats, and recommendations for organizations. Business Horizons. 2019 Jul 1;62(4):509-19.

[iv] Dell'Erba M. Crypto-Trading Platforms as Exchanges. Mich. St. L. Rev.. 2024:1.

[v] Verstein A. Crypto Assets and Insider Trading Law's Domain. Iowa L. Rev.. 2019;105:1.

[vi] Wright DC. Digital Manipulation: An Exploration of Kripkean Dogmatism and Dark Triad Traits in Cryptocurrency Social Media Communities. Available at SSRN 5343449. 2024 Apr 24.

[vii] Mesioye O. The nexus between insider trading and organized crime: Challenges in enforcing ethical market practices. Int J Res Public Rev. 2025;6(1):1817-31.

[viii] La Morgia M, Mei A, Sassi F, Stefa J. The doge of wall street: Analysis and detection of pump and dump cryptocurrency manipulations. ACM Transactions on Internet Technology. 2023 Feb 23;23(1):1-28.

[ix] Patel V, Putniņš TJ. How much insider trading happens in stock markets?. InAmerican Finance Association (AFA) Annual Meeting 2020.

[x] Krause D. Beyond the Milei $ LIBRA Scandal: Unmasking the Unfair Meme Coin Ecosystem and Its Exploitation by Insiders. Available at SSRN 5149323. 2025 Feb 22.

[xi] Aravind G, Vijayakuaran A. Error 5XX: A Critique on Application of Insider Trading Regulations to Cryptocurrencies in India. RGNUL Fin. & Mercantile L. Rev.. 2021;8:228.

[xii] Krishnan S, Shashidhar N, Varol C, Islam AR. A novel text mining approach to securities and financial fraud detection of case suspects. International Journal of Artificial Intelligence and Expert Systems. 2022;10(3).

[xiii] Teall JL. Financial trading and investing. Academic Press; 2022 Jul 9.