BEHAVIORAL SHIFT: RETHINKING THE "INSIDER"

Shalini Saxena, PhD Scholar at Sushant University, Gurgaon

Dr. Divya Sharma, Assistant Professor, School of Law, Sushant University

Dr Treena, Assistant Professor, School of Law, G.D Goenka University

ABSTRACT

The concept of insider trading is based on white-collar crime which was initially based on access to privileged and precise information and positions of trust within various companies and organisations. The rapid spread of digital invention in Fintech industry in India and globally consists of behavioral shifts in rethinking capacity of an individual. This paper shall focus on legal and compliance framework including Securities Exchange Board of India (SEBI) insider trading probes, banking frauds and examination of frameworks under SEBI (Prohibition of Insider Trading) Regulations 2015 (as amended), Companies Act 2013, Prevention of Money Laundering Act (PMLA) 2002, and Reserve Bank of India (RBI) guidelines on white-collar crimes and Fintech industry, exploring behavioral aspects and dynamics of same based on technological affordances, psychological pressures, organizational cultures, and economic incentives.

Two prominent frameworks of Edwin Sutherland and Petter Gottschalk, explain how social learning, organizational environments, and perceived opportunities contribute to white-collar criminal behavior. When complemented by insights from behavioral economics, particularly prospect theory and its application to high-status offenders, these frameworks move beyond narrow legal and regulatory definitions of insider misconduct to provide a more comprehensive behavioral understanding of why insiders engage in financial crime. Fintech industry involves not only the employees or companies but also involves algorithmic systems, third-party vendors, and hybrid human-AI entities exploiting unpublished price-sensitive information (UPSI), data asymmetries, and regulatory arbitrage.

This paper has focused on jurisdictional challenges in domestic as well as cross-border financial services industry. Further, it will reveal outdated notions being followed and attempt to show how these can be remedied or updated, based on automated trading.

The paper has also focused on algorithmic trading, data usage and misuse, identity fraud and lastly paper has made recommendations on or for behavioral risk management, AI driven detection, protection for whistleblower, legislative reforms and gaps, corporate criminal liability. This behavioral rethinking is aimed to bridge compliance gap(s), enhance

deterrence, and foster ethical innovation in India's fintech ecosystem, contributing to broader economic integrity.

I. INTRODUCTION

Insider trading, has been for a long time been regarded as a quintessential white-collar crime; traditionally understood through the lens of privileged access to material non-public information and breach of fiduciary duties or position of trust within corporations. Rooted in classical notions of confidentiality and market fairness, the offence hinges on exploitation of *unpublished price-sensitive information*, referred to a UPSI, by those deemed "insiders" such as directors, key officers, key employees, or other connected persons. In India, this framework finds expression in SEBI (Prohibition of Insider Trading) Regulations, 2015[1] (as amended), alongside overlapping provisions in the Companies Act, 2013[2], the Prevention of Money Laundering Act (PMLA)[3], 2002, and RBI guidelines and notifications, governing banking and financial institutions.

However, rapid digitalisation of financial markets, particularly within ever-growing Fintech industry, has fundamentally disrupted these traditional boundaries. India's Fintech ecosystem valued for its explosive growth in digital lending, payments, algorithmic trading, Robo-advisory, and data-driven investment platform has accelerated flow of information across borders, devices, and entities[4]. What once required physical proximity or formal employment now occurs through cloud infrastructure, APIs, algorithmic systems, third-party vendors, and hybrid human-AI decision-making processes. This technological affordance has precipitated a behavioral shift in very conception of "insider," moving beyond static legal definitions to dynamic, behavior-centric models that account for data asymmetries, regulatory arbitrage, and automated exploitation of UPSI[5].

Recent issues and related enforcement actions underscore urgency of need to rethink the definition. In FY 2024-25, SEBI investigated 287 cases of alleged insider trading, up significantly from previous years, now involving banking executives, consulting firms (such as PwC and EY), and global players like Bank of America, involved in block deals and share

[1] SEBI (Prohibition of Insider Trading) Regulations, 2015.
[2] Companies Act, 2013.
[3] Prevention of Money Laundering Act (PMLA).
[4] AZB & Partners, White-collar crime 2023, https://www.azbpartners.com/bank/white-collar-crime-2023-law-and-practice/ accessed on 10th July, 2026 at 10:00 AM.
[5] *ibid*.

offerings[6]. These cases revealed not only classical breaches but also novel vectors involving algorithmic trading, data misuse, identity fraud, and cross-border coordination challenges that expose limitations of outdated regulatory paradigms designed for a pre-digital era.

This research paper examines paradigm shift necessitated by these developments. It analyses legal and compliance frameworks governing insider trading and related white-collar crimes in India's Fintech industry, while integrating behavioral and criminological perspectives[7]. Drawing upon Edwin Sutherland's *differential association theory* (which explains criminal behavior through learned interactions within intimate groups) and Petter Gottschalk's *theory of convenience* (positing that white-collar crime occurs when financial motives align with organisational opportunities and personal willingness for deviance), against insights from behavioral economics including adaptation of prospect theory for high-status offenders; this study highlights how psychological pressures, organisational cultures, economic incentives, and technological enablers shape deviant conduct[8] especially with respect to "insider".

In the fintech context, complicates traditional insider definition. Algorithmic systems, machine learning models trained on proprietary datasets, third-party data aggregators, and hybrid entities can now access and act upon sensitive information at speed and scale unattainable by human actor by himself/herself. The use of AI helps an individual to dive deep into already available information of an individual or company and then use it according to the need of the topic which in a way hampers privacy of personal information of the individuals. Jurisdictional complexities arising from domestic operations intertwined with global platforms, cloud providers, and cross-border data flows further strain existing enforcement mechanisms[9]. Outdated notions of "connected persons" and manual compliance controls prove inadequate against automated trading, real-time data exploitation, and sophisticated identity fraud schemes.

This paper proceeds by first mapping evolving legal landscape under regulations of SEBI, RBI, and other statutory and allied laws. It then explores behavioral dynamics through

[6] Ira Duggal & Jaishree P. Upadhyay, India watchdog presses banks, other regulators for stricter insider trading enforcement, Reuters, https://www.reuters.com/sustainability/boards-policy-regulation/india-watchdog-presses-banks-other-regulators-stricter-insider-trading-2026-03-02/ accessed on 10th July, 2026 at 5:00 PM.
[7] Suraj Prakash & Dr. Tavleen Kaur Khurana, Securities Fraud in India: A criminological examination of insider trading in India, Journal of Informatics Education and Research, https://jier.org/index.php/journal/article/view/1534/1285 accessed on 11th July, 2026 at 11:00 AM.
[8] *ibid*.
[9] *supra* n.6.

aforementioned theoretical lenses, followed by an examination of specific challenges in algorithmic trading, data governance, and cross-border Fintech. Finally, it offers actionable recommendations for behavioral risk management frameworks, AI-driven detection tools (involving advantages and disadvantages in proper usage of AI) strengthened whistleblower protections, legislative reforms to address regulatory gaps, and enhanced models of corporate criminal liability.

By bridging compliance gaps through a behavioral rethinking of *who is an* insider, this study seeks to strengthen deterrence, promote ethical innovation, and safeguard integrity of India's Fintech-driven financial ecosystem in an era of unprecedented technological convergence. In doing so, it contributes to both academic discourse on white-collar crime and practical policymaking for emerging market regulators confronting realities of digital finance.

II. STATEMENT OF PROBLEM

The rapid increase in proliferation of fintech industry in India and abroad has mainly redeveloped and transformed financial landscape,

Widespread growth in and of fintech industry in India has transformed financial landscape, offering unprecedented access to credit, payments, investments, and wealth management. However, this digital disruption has simultaneously amplified incidence and sophistication of white-collar crimes. Central to this challenge is evolving nature of "insider" -traditionally understood as an individual with positional access to unpublished price sensitive information (UPSI) or privileged data. In the contemporary fintech ecosystem, this archetype is undergoing a profound behavioral shift that current legal and compliance frameworks are ill-equipped to address.

Despite robust statutes such as the SEBI (Prohibition of Insider Trading) Regulations, 2015, the Companies Act, 2013, the Prevention of Money Laundering Act, 2002, and various RBI guidelines, significant gaps persist in conceptualizing, detecting, preventing, and prosecuting insider-driven white-collar offenses in fintech. Regulators and organizations continue to rely on static, position-based definitions of insiders, while behavioral realities driven by intense performance pressures, ethical disengagement, technological affordances (e.g., algorithmic trading, API integrations, cloud data flows), organizational cultures of "move fast and break things," and emergence of hybrid human-AI actors have rendered these definitions increasingly obsolete.

This misalignment or inability or delay in evolving alongside, creates a fertile environment for misconduct. Employees, vendors, contractors, and even autonomous systems can exploit data asymmetries, circumvent controls through subtle behavioral patterns, and engage in acts ranging from data exfiltration and synthetic identity fraud to algorithmic front-running and market manipulation. High-profile incidents and rising regulatory probes underscore problem: SEBI has investigated hundreds of insider trading cases in recent years, yet conviction rates remain low, enforcement is protracted, and Fintech-specific vulnerabilities are inadequately covered.

The problem is compounded by several interconnected factors:

- Conceptual Lag: Legal definitions fail to capture behavioral motivations (e.g., prospect theory-driven risk-seeking among high-status actors) or non-human insiders.
- Regulatory Fragmentation: Overlapping yet soiled oversight by SEBI, RBI, MeitY, and SFIO leads to jurisdictional ambiguities and coordination failures.
- Technological Obsolescence: Compliance tools and regulations predate widespread adoption of AI/ML, behavioral analytics, and decentralized Fintech architectures.
- Enforcement and Deterrence Deficits: Resource constraints, evidentiary challenges in digital environments, weak whistleblower protections, and inadequate corporate accountability mechanisms undermine effective response.
- Societal and Economic Impact: White-collar crimes in Fintech erode investor confidence, destabilize financial inclusion gains, impose massive economic costs, and undermine trust in India's digital public infrastructure (e.g., UPI, Account Aggregator).

Existing literature on white-collar crime in India adequately documents traditional frauds but falls short in integrating behavioral criminology with Fintech-specific regulatory analysis. There is a critical need to rethink insider through a behavioral lens - shifting from rule-based, perimeter-focused compliance to dynamic, motivation-sensitive, and technology-augmented models.

III. LITERATURE REVIEW

Secil Tastan (2019) focused upon multidisciplinary review of white-collar crimes, criminality

and its understanding based upon psychological, organisational and situational motives behind happening of such crimes. The paper analysis the environmental, psychological and situational factors based upon white-collar crimes which are engaged in crimes in the organisations and companies. The paper further analysed organisation based situational word variables which are behind white-collar crimes, including ethical climate and opportunities for role by bending among antecedents of white-collar crime. It focuses on organisational behaviour, code of conduct and ethical climate. Lastly, paper has analysed implications of such practices and importance of developing business ethic codes, prevention issues and creating strong, ethical climate[10].

Joost H. R. van Onna (2020) this paper focuses on white-collar crime on personal level. In this paper, 26 offenders convicted of white-collar crime were interviewed. The theory and research was based on white collar criminology, life course criminal and moral psychology. The findings and circumstances have shown social bonds and adjusted moral ideas of offenders behind such white-collar crimes. Further, the paper has focused upon evolving of long running processes which dwell social bonds or ideas being adjusted, influencing decision to engage offender into white collar offence. At lastly, the paper has found out directions which can be used for future research purposes in relation to white collar crime and its psychological effect[11].

Benson Michael L., Madensen Tamara D. & Eck John E. (2021) focused on the white collar crime from opportunity perspective stating that importance of white collar crime is no longer an important aspect to be argued. There are devastating financial and physical reasons behind same. Now it is important to focus on ways which are necessary to control and prevent white collar crimes. In this paper, the author has focused on reduction of white collar crime and specific opportunities structures associated with criminal offences related to white-collar crime. It has also identified features of crime and how it takes place. It has also relied upon theories which can help in identification of white-collar crime, including routine activity, theory, criminal pattern theory and situational crime prevention theory. Furthermore, the author has also analysed opportunities which are prevalent in environment and has helped to discover and evaluate potential offenders. The white-collar crime has been important to know that how

[10] Secil Tastan, White-Collar Criminals and Organizational Criminology: Theoretical Perspectives, https://www.researchgate.net/publication/345559549_White-Collar_Criminals_and_Organizational_Criminology_Theoretical_Perspectives, accessed on 13th July, 2026 at 7:00 PM.

[11] Joost H. R. van Onna, From the Avalanche to the Game: White-Collar Offenders on Crime, Bonds and Morality, https://link.springer.com/article/10.1007/s10611-020-09899-x accessed on 13th July, 2026 at 02:00 PM.

they have been committed and structural analysis has been drawn at the end of paper[12].

Manfred F. R. Kets de Vries (2022) stated that white-collar crimes in India are generally based upon corporate crimes. He analyses the stockbrokers and information perceived by them. He focused on the white-collar crime terminology and its effect starting from year 1939 till the present time. He stated that fraud is a triangle which is based upon three major forces. According to the auditor it is based upon individual decisions, how to commit a fraud including pressure, opportunity, and realisation. He analyses people's equation is related to dance between the situation and personality dynamics. Further, he focused on the prevention of white collar crimes in India with respect to corporate culture, leadership, development, entry and exit, control systems, responsibility of business schools, etc[13].

Soni Priyanka, Singh Rajat, Piplani Riddhi, Gautam Anjali (2025) focused on the white-collar offences, including fraud, embezzlement, malfeasance, which are genuinely based upon psychological influences, which are guided by offender's risk-taking capacity, ethical decision-making and many other behavioral aspects. This paper generally examines white-collar crime, which is based upon psychological theories, including risk perception, disengagement, and personality characteristics like narcissism, psychopathy. It has also analysed fear of sanctions, high self-efficacy and cognitive realisations, which indulge person into happening of white-collar crime. The paper has also focused upon the cognitive dissonance theory which generally is based upon personal values and diluting guilt and fear of individual. It has also analysed psychological processes which a person indulges into while committing such offence and prevention of fraud practices. At the end, paper has discussed psychological understandings and criminal logically effect of white-collar crimes. The paper has helped to understand behaviour which can result in greater detection of mechanisms and legal frameworks behind such happening of white collar, crime and cultural ethical responsibility in dealing corporate settings[14].

[12] Benson Michael L., Madensen Tamara D. & Eck John E., White Collar Crime from an opportunity perspective, https://link.springer.com/chapter/10.1007/978-0-387-09502-8_9 accessed on 14th July, 2026 at 10:00 AM.
[13] Manfred F. R. Kets de Vries. Into the Mind of White-Collar Criminals, https://knowledge.insead.edu/leadership-organisations/mind-white-collar-criminals accessed on 14th July, 2026 at 12:00 noon.
[14] Soni Priyanka, Singh Rajat, Piplani Riddhi, Gautam Anjali, Psychological Perspective of white-collar crimes, https://www.researchgate.net/publication/391565988_Psychological_Perspective_of_White-Collar_Crimes accessed on 13th July, 2026 at 8:00 PM.

IV. RESEARCH OBJECTIVES

1. To analyze the behavioral drivers and evolving typology of "insiders" in the Fintech context.
2. To critically evaluate the Indian legal and regulatory framework for white-collar crimes, identifying enforcement and conceptual shortcomings.
3. To examine behavioral shifts and framework failures.
4. To propose behaviorally informed policy, technological, and institutional recommendations for robust compliance.

V. RESEARCH QUESTIONS

1. How have behavioral drivers (psychological, organizational, and technological) contributed to a shift in the nature and manifestation of insider threats in Indian Fintech?
2. What are the primary gaps in the existing legal and compliance frameworks (SEBI, RBI, Companies Act, PMLA, etc.) in addressing these behaviorally evolved insider risks?
3. What are the gaps in current regulatory mechanisms, which fail to incorporate behavioral analytics and adaptive compliance strategies?
4. What are recommendations to ensure better behavioral aspect behind happening of white-collar crime?

VI. RESEARCH METHODOLOGY

This paper has adopted the qualitative, doctrinal and analytical approach for research to deeply examine and analyse behavioral shift in rethinking the "insider" within the context of white-collar crime in Indian Fintech. This methodology has been adopted keeping in mind research questions and research objectives. Further, this paper attempts to identify the gap between the already persisting research and further focuses on bridging the gap in legal and compliance area.

The research will be based on descriptive-analytical design following the doctrinal analysis which will be based on secondary resources. The secondary sources shall include relevant

statutes, regulations, judicial pronouncements, scholarly literature reviews, internet sources and reports which will help to analyse existing law and gaps in law. The analytical components will help to deeply analyse and evaluate adequacy of frameworks against behavioral realities in present day Fintech.

This type of analysis and design is generally adopted wherein there are issues related to white-collar crimes, involving technique and technology, enforcement practices, individual and organisational behaviour. The secondary sources shall include: -

Secondary Sources:

- Statutes and Regulations: SEBI (Prohibition of Insider Trading) Regulations, 2015 (as amended up to 2025), Companies Act, 2013, Prevention of Money Laundering Act, 2002, Information Technology Act, 2000, Bharatiya Nyaya Sanhita (relevant fraud/cheating provisions), RBI Master Directions on Fintech, outsourcing, and cyber security.

- Judicial Decisions: Key Supreme Court and High Court judgments on insider trading (e.g., interpretations of UPSI), corporate fraud, and regulatory enforcement.

- Official Reports: SEBI Annual Reports, RBI Financial Stability Reports, SFIO publications, Enforcement Directorate data, and government policy documents on Fintech regulation.

- Scholarly articles, books, and Ph.D. theses on white-collar crime, behavioral criminology, and Fintech regulation.

- Reports from think tanks (e.g., Kearney, Protiviti on insider threats), international bodies (FATF, IOSCO), and industry analyses.

- Media-reported case studies and empirical data on Fintech fraud trends (used cautiously for triangulation).

VII. UNDERSTANDING THE BEHAVIORAL SHIFT: RETHINKING THE INSIDER IN FINTECH

7.1 TRADITIONAL CONCEPT OF INSIDER

The traditional concept of insider is based upon the regulations involving SEBI Regulations,

2015, which in was connected persons, including directors, officers, employees, or any contractual relationships who possess unpublished price sensitive information. Under this concept, white-collar crime is generally based upon the breach of trust by an individual regarding organisational boundaries. It involves, the key characteristics of traditional model. i.e formal affiliation based upon employment, board membership of professional advisory rules[15]. Here the human agency focuses upon the individuals in position which holds trust and duty and material information involving PSI. It relies on compliance via confidentiality agreements and periodic disclosure[16].

7.2 DRIVERS OF BEHAVIORAL SHIFT

The drivers of behavioral shift involve the technological preferences, digital information, spread, economic incentives, and organisational structures, regulatory, arbitrary opportunities, psychological and social factors.

- **Technological Affordances-** It involves the publication of data, analysis of the real time, cloud computing, and other markets involving information where in past data basis and infer PI are used to form patterns, eroding tradition, traditional barriers.
- **Digital information spread-** It involves technical platforms where there is cross border sharing of data between third parties and devices. It extends to alternative data providers, social trading apps and other information beyond known organisation perimeters.
- **Economic incentives and organisational cultures-** It involves high growth of industry and crime based upon performance, matrix, innovation, and other areas where sensitive information is being used as aggressive data, for exploitation and means to put pressure on individuals in a psychological manner.
- **Regulatory arbitrage opportunities-** It is based upon hybrid work and oversight of domestic and cross powdered jurisdictions, which are used to exploit gaps between the rules and evolving technologies between countries and regions.
- **Psychological and social factors-** It involves hybrid work, involving economic participation and virtual network, which weaken the bond between companies and

[15] Atul Harit, White Collar Crime International Prospective With Reference To India, & UK, Internationa Journal of Creative Research Thoughts, https://ijcrt.org/papers/IJCRT2409559.pdf accessed on 14th July, 2026 at 6:00 PM.
[16] S. Umapathi, Changing patterns of white collar crime, cyber crime and justice.. An over view, https://mcrhrdi.gov.in/splfc2-2022/week5/Investigation%20Economic%20Offences%20review%20-%20Copy%20-%20Umapathi%20IPS.pdf accessed on 13th July, 2026 at 10:00 AM.

organisations.

7.3 EMERGING TYPOLOGY OF INSIDERS (HUMAN, HYBRID, ALGORITHMIC)

The emerging type of insider(s) is based upon the human insider involving employees, executives, and consultants who exploit UPI systems to indulge in insider trading in fintech industry and also to exploit transfer of data from one person to another using unfair means[17]. Furthermore, the hybrid sides are also present where there are technological augmentation and human judgement, which involves exploitation both from human discretion and machine efficiency and complicating attribution further with the content and liability[18]. Further, the algorithmic and systematic insider modules, non-human entities and high frequency trading algorithms, machine learning models, and other auto trading bots are responsible and help to detect a criminal act based upon the human intentions[19].

7.4 BEHAVIORAL THEORIES APPLIED (CONVENIENCE THEORY, PROSPECT THEORY, ETC.)

The behaviour authorities are generally based upon the Sutherland differential association theory which involves insider trading and criminal behaviour behind it. It generally analyses what was criminal intent of the offence. Further, the theory is based on the Gottschalk's Convenience Theory as per which white-collar crime spreads into three dimensions, involving financial motive, organisational opportunity and personal willingness. He thinks that all these three elements should or need to be present in order to commit a white-collar crime[20].

VIII. LEGAL AND REGULATORY FRAMEWORK GOVERNING WHITE-COLLAR CRIME IN INDIAN FINTECH

8.1 KEY LEGISLATIONS (SEBI PIT REGULATIONS, COMPANIES ACT, PMLA, IT ACT, RBI GUIDELINES)

This section provides a detailed examination of existing legal architecture governing insider trading and related offences in India, relevant to the Fintech industry. While these frameworks

[17] *ibid*.
[18] *ibid*.
[19] Shrutika Jejurkar, Smruti Patil, Paridhi Taneja, Eshaan Advani, Samarth Jain, Dissertation of White-Collar Crimes in India, International Journal of Novel Research and Development, https://www.ijnrd.org/papers/IJNRD2404422.pdf accessed on 14th July, 2026 at 12:00 noon.
[20] *ibid*.

have evolved to address market integrity, they exhibit structural limitations when applied to digital, algorithmic, and cross-border environments, as highlighted in behavioral shift detailed above.

8.1 KEY LEGISLATIONS

SEBI (PROHIBITION OF INSIDER TRADING) REGULATIONS, 2015 (AS AMENDED)

The cornerstone of insider trading regulation in India, these regulations prohibit trading in securities while in possession of UPSI and impose obligations on listed companies and intermediaries to maintain confidentiality and structured digital databases (SDD). Key amendments have strengthened disclosure requirements, introduced the role of compliance officers, and expanded definition of connected persons. However, the regulations remain primarily human-centric and struggle when put to test against algorithmic trading, where trades occur at sub-second intervals without any direct human intervention[21]. Recent enforcement actions against banks, consulting firms, and global intermediaries illustrate both heightened scrutiny and persistent challenges in proving intent in such automated scenarios.

COMPANIES ACT, 2013

Sections 195 and related provisions, criminalise insider trading by directors, key managerial personnel, and other officers. The Act addresses corporate governance, fiduciary duties, and corporate criminal liability. In context to Fintech industry, it applies to startups and NBFCs but falls short in addressing liability for algorithmic systems or third-party vendors. Its provisions on oppression and mismanagement, offers limited recourse in cases of data misuse or information asymmetry.

PREVENTION OF MONEY LAUNDERING ACT (PMLA), 2002

PMLA serves as a critical tool for tracing proceeds of insider trading and other predicate offences. Scheduled offences include violations under SEBI regulations, enabling attachment of properties and stringent bail conditions. In Fintech, PMLA is increasingly invoked for

[21] Harpreet Singh, White Collar Crimes in India: Regulatory Mechanism and enforcement challenges, Journal of Advance and Future Research, https://rjwave.org/jaafr/papers/JAAFR2605355.pdf accessed on 14th July, 2026 at 5:00 PM.

layering schemes involving digital wallets, crypto assets, and cross-border transfers[22]. However, the Act focus on predicate offences, creates an enforcement gap when it comes to insider advantages diffused through complex algorithmic or hybrid entities.

INFORMATION TECHNOLOGY ACT, 2000 (AS AMENDED)

The IT Act, more particularly with respect to sections dealing with data protection, cyber security, and unauthorised access (e.g., Section 43, 66), compliments the law on securities by addressing data breaches and identity fraud that facilitate insider trading. With the Digital Personal Data Protection Act, 2023, the aim is to further strengthen consent and processing norms[23]. Yet, challenges persist in attributing liability for AI-generated insights or data inferred from aggregated sources, which fail even with the latest legislation, making it a regulatory grey zone.

RBI GUIDELINES AND RELATED FRAMEWORKS

The Reserve Bank of India issues guidelines on outsourcing, information security, customer data protection, and fraud reporting applicable to banks and Fintech partnerships (e.g., under the Payment and Settlement Systems Act)[24]. Guidelines on algorithmic lending, digital lending, and co-lending address some risks but lack specific integration with SEBI's insider trading rules. RBI's focus on systemic stability often intersects with market abuse concerns in unified payment interfaces (UPI) and account aggregators, yet identification, coordination and penalizing mechanisms remain fragmented[25].

Collectively, these legislations provide a multi-layered but soiled framework that has not fully adapted to the involvement of algorithmic systems, third-party vendors, and hybrid human-AI entities exploiting UPSI and data asymmetries.

8.2 COMPLIANCE MECHANISMS AND INSTITUTIONAL ARCHITECTURE CORE COMPLIANCE MECHANISMS

- **Structured Digital Databases (SDD) and Chinese Walls**: Mandatory maintenance of SDDs to track UPSI access is a key preventive tool, yet implementation is often

[22] *ibid*.
[23] *ibid*.
[24] Pranita Dhara, Examine the laws and regulations governing White collar crime in India, Naya Legal, https://www.nayalegal.com/examine-the-laws-and-regulations-governing-white-collar-crime-in-india accessed on 13th July, 2026 at 7:00 PM.
[25] *ibid*.

superficial, as evidenced by settlement orders.

- **Code of Conduct and Disclosures**: Companies must formulate insider trading codes, conduct periodic training, and ensure pre-clearance of trades. Fintech companies are required to implement robust internal controls[26].
- **Whistleblower Mechanisms**: Protected under the Companies Act, 2013 and SEBI Regulations, 2015 these are vital but under utilised due to fear of retaliation.
- **Surveillance and Monitoring**: Stock exchanges and SEBI employ market surveillance systems, but these are still catching up with high-frequency and algorithmic patterns.

Institutional Architecture

- **SEBI**: Primary regulator for securities markets, with dedicated investigation and enforcement departments. It collaborates with stock exchanges (NSE, BSE) for real-time monitoring.
- **RBI**: Oversees banking and payment systems, focusing on prudential norms and cyber security.
- **Enforcement Directorate (ED) and Central Bureau of Investigation (CBI)**: Handle serious fraud and money laundering offenses.
- **Ministry of Corporate Affairs (MCA) and Serious Fraud Investigation Office (SFIO)**: Address corporate governance framework and consequent failures.
- **Inter-Regulatory Coordination**: Bodies like the Financial Stability and Development Council (FSDC) aim to bridge gaps, but overlapping jurisdictions of multiple fragmented authorities, frequently cause delays in Fintech-related probes.

IX. IDENTIFICATION AND ANALYSIS OF GAPS IN THE LEGAL AND COMPLIANCE FRAMEWORK

9.1 CONCEPTUAL AND DEFINITION GAPS

Conceptual and definition level gaps involve the narrow insider definition, static versus

[26] *ibid*.

dynamic information, outdated notion of trust and position. The following are being discussed:

1) **Narrow insider definition-** Generally based upon the narrow definition of 'insider'; which is based in AI systems that are also limited in what it they covering largely third-party data vendor and/or algorithmic trading platforms that maybe involved. The AI model have to be trained and expanded to understand and relate to more definitions such as UPSI without relying only upon the traditional connected persons or any insider person.

2) **Static versus dynamic information-** Its source is based upon the conceptualised information wherein fintech industry generally uses the data asymmetric from a continuous, aggregated or machine generated learning where binary codes are used from public and unpublished source which are or become obsolete over time. On the contrary behavioral models show that trading systems are vulnerable to reacting or acting based on past behavior they also hence share material information without human actor being aware of the same. It is hence imperative that data be secured and encrypted to avoid potential misuse and impersonation.

3) **Outdated notion of trust and position-** The integration of Artificial Intelligence has made traditional, binary models of trust, where a system is viewed as either completely reliable or untrustworthy, both are obsolete. In the AI era, trust is no longer about blind reliance; it is a spectrum of rectified trust that requires constant verification, transparency, and human oversight

9.2 ENFORCEMENT AND IMPLEMENTATION GAPS

Based on existing SEBI's enforcement activity, the gaps range from: resource and technological constraints, compliance burden and superficial adherence, fragmented agency coordination and deterrence deficiency. These are addressed as below:

1) **Resource and technological constraints: -** They are based upon the regulatory bodies, which lack forensic tools and knowledge to detect algorithmic manipulation or chain, required to investigate into complex data related matters. Then, investigation related to private information is difficult to be accessed by the whistleblower, leading to delay or incomplete prosecutions or even incorrect or inadequate decisions.

2) **Compliance burden and superficial adherence-** While it involves mandatory requirement to be adhered or complied with based upon structure, digital data basis it's a mere check the box exercise. In fact, it helps to illustrate how entities get away with penalties while systems remain is weak and incompetent to address systemic issues.

3) **Fragmented interagency coordination-** Involving varied economic incentives, there is an overlap between SEBI, RBI, other authorities, resulting in delay across many elements such as information sharing or triggering of relevant framework decision being taking, as an example a case which should be decided under of the Prevention of Money Laundering Act in case of fintech industries, result in loss of time and evidence in this overlap ambiguity.

4) **Deterrence deficiency-** Reduced capacity of legal frameworks to deter from using technology to commit sophisticated financial crimes. This deficiency emerges since use of say AI lowers the risk, cost, and probability of punishment for offenders.

9.3 TECHNOLOGICAL AND BEHAVIORAL GAPS

The technological and behavioral gaps, involve the algorithmic trading and automation, data usage and misuse, behavioral dynamics, explained to some extent below:

1) **Algorithmic trading and automation-** Based upon the high frequency in AI driven areas which are used by the fintech industry and faster technology system in say UPSI which are being misused.

2) **Data usage and misuse-** Based upon the ecosystem of API's and third-party aggregators, which may facilitate misuse or leak of information resulting in identity theft, systematic identities, and deep fake social engineering identities which further exploits the psychological pressure of performance, incentives and organisational cultures.

3) **Behavioral dynamics-** Sutherland's *differential association theory* under which behavioral dynamics amongst employees is generally ignored and necessary steps are not implemented from time to time preempting and preventing such crimes or situations enabling such crimes.

9.4 INSTITUTIONAL AND JURISDICTIONAL GAPS

The institutional gaps range across core domestic challenges, cross border complexities, institutional capacity and are addressed below:

1) **Domestic challenge-** Foundational weaknesses in enforcing regulations, protecting whistleblowers, and insulating law enforcement from political influence.

2) **Cross border complexities-** Means necessary involvement of global fintech platforms which is difficult given fragmented international laws, bureaucratic and slow extradition processes that sophisticated financial criminals exploit through regulatory arbitrage.

3) **Institutional capacity-** Gaps in skill in say forensic, outdated digital infrastructure, accountability and checks on companies to act in a systematic way leading to creation of opportunity for criminal liability and failures in the fintech governance.

X. RECOMMENDATIONS AND CONCLUSION

To address the behavioral shift in the insider trading ecosystem, this paper has attempted to focus on the compliance gaps, incorporate behavioral insights and legal frameworks based upon SEBI, Companies Act, PMLA and RBI Guidelines.

The recommendations involve behavioral risk management framework, that is to integrate continuous monitoring of behavioral pattern, communication network and detection of the behavioral analytics. It also highlights that individual behaviour should align with long-term market integrity rather than focusing upon short-term information advantages. Additionally, the paper has provided a recommendation with respect to AI driven detection and technological upgradation. Based upon the UPSI system in use across, both hybrid and aromatic insiders, the related models should be built based on relevant regulations, rules and law, such as RBI 7 sutras in AI development. Further, there is a need to strengthen protection accorded to a whistle blower, especially in cases related to white-collar crimes in the fintech industry. Similarly, legislative reforms should be taken regarding amendment of relevant SEBI Regulation(s) and further strengthen the position into related elements under the Companies Act and PMLA. Further, cross-border data sharing and mutual legal assistance protocol should be adopted to strengthen the global fintech corporation which impact or related to cross border aspects. There

should be an enhanced corporate criminal liability check system for the organisations where there are systemic failures being sighted, and lastly there should be an introduction a system to check and prevent offences in the global models, thereby safeguarding organic businesses and the organisations.

The paper concludes that in evolved and evolving arena of digitalisation in fintech, the existing concept of insider has become obsolete. They are white collar crimes which have been precipitated by first involving oneself personally into the organisation and then building position of trust and gaining access into complex matters and identifying behavioral phenomena leading to human acts, monitoring algorithmic systems, and third-party vendors and hybrid entities, which are exploiting the data information leading to regulatory gaps and then commit the crime.

India being a developing country is vulnerable and the fintech ecosystem, critical to wellbeing of any country and its citizens, can see the behavioral shift from the regulatory philosophy rigid, position-based rules to a gap to catch up and be ready for the new insider role and disguise. The paper has demonstrated the framework and legal position under SEBI Regulations, 2015, Companies Act and PMLA. Furthermore, the Sutherland Differential Association theory, Gottschalk's Convenience theory, reveal the psychological pressure, organisational, cultural, and economic incentives, which are now behind the automated trading with data usage and insider trading.

Therefore, this new and evolving behavioral lens offers a different path to identify between wrong and right intent of the person who is indulging in the offence. It has analysed the compliance caps and regulatory gaps, in the legal diaspora, which should be strengthened or amended, to better manage such offences and identify who is the "insider" today.

REFERENCES

ACTS

- Companies Act, 2013.
- Prevention of Money Laundering Act (PMLA).
- SEBI (Prohibition of Insider Trading) Regulations, 2015.

WESITES/ARTICLES/RESEARCH PAPERS

- Atul Harit, White Collar Crime International Prospective With Reference To India, & UK, Internationa Journal of Creative Research Thoughts, https://ijcrt.org/papers/IJCRT2409559.pdf accessed on 14th July, 2026 at 6:00 PM.
- AZB & Partners, White-collar crime 2023, https://www.azbpartners.com/bank/white-collar-crime-2023-law-and-practice/ accessed on 10th July, 2026 at 10:00 AM.
- Benson Michael L., Madensen Tamara D. & Eck John E., White Collar Crime from an opportunity perspective, https://link.springer.com/chapter/10.1007/978-0-387-09502-8_9 accessed on 14th July, 2026 at 10:00 AM.
- Harpreet Singh, White Collar Crimes in India: Regulatory Mechanism and enforcement challenges, Journal of Advance and Future Research, https://rjwave.org/jaafr/papers/JAAFR2605355.pdf accessed on 14th July, 2026 at 5:00 PM.
- Ira Duggal & Jaishree P. Upadhyay, India watchdog presses banks, other regulators for stricter insider trading enforcement, Reuters, https://www.reuters.com/sustainability/boards-policy-regulation/india-watchdog-presses-banks-other-regulators-stricter-insider-trading-2026-03-02/ accessed on 10th July, 2026 at 5:00 PM.
- Joost H. R. van Onna, From the Avalanche to the Game: White-Collar Offenders on Crime, Bonds and Morality, https://link.springer.com/article/10.1007/s10611-020-09899-x accessed on 13th July, 2026 at 02:00 PM.
- Manfred F. R. Kets de Vries. Into the Mind of White-Collar Criminals, https://knowledge.insead.edu/leadership-organisations/mind-white-collar-criminals accessed on 14th July, 2026 at 12:00 noon.
- Pranita Dhara, Examine the laws and regulations governing white-collar crime in India, Naya Legal, https://www.nayalegal.com/examine-the-laws-and-regulations-

governing-white-collar-crime-in-india accessed on 13th July, 2026 at 7:00 PM.

- S. Umapathi, Changing patterns of white collar crime, cyber crime and justice.. An over view, https://mcrhrdi.gov.in/splfc2-2022/week5/Investigation%20Economic%20Offences%20review%20-%20Copy%20-%20Umapathi%20IPS.pdf accessed on 13th July, 2026 at 10:00 AM.
- Secil Tastan, White-Collar Criminals and Organizational Criminology: Theoretical Perspectives, https://www.researchgate.net/publication/345559549_White-Collar_Criminals_and_Organizational_Criminology_Theoretical_Perspectives, accessed on 13th July, 2026 at 7:00 PM.
- Shrutika Jejurkar, Smruti Patil, Paridhi Taneja, Eshaan Advani, Samarth Jain, Dissertation of White-Collar Crimes in India, International Journal of Novel Research and Development, https://www.ijnrd.org/papers/IJNRD2404422.pdf accessed on 14th July, 2026 at 12:00 noon.
- Soni Priyanka, Singh Rajat, Piplani Riddhi, Gautam Anjali, Psychological Perspective of white-collar crimes, https://www.researchgate.net/publication/391565988_Psychological_Perspective_of_White-Collar_Crimes accessed on 13th July, 2026 at 8:00 PM.
- Suraj Prakash & Dr. Tavleen Kaur Khurana, Securities Fraud in India: A criminological examination of insider trading in India, Journal of Informatics Education and Research, https://jier.org/index.php/journal/article/view/1534/1285 accessed on 11th July, 2026 at 11:00 AM.