World Economics & Finance Bulletin (WEFB)
Available Online at: https://www.scholarexpress.net
Vol. 54, January, 2026
ISSN: 2749-3628,

DETECTION AND PREVENTION OF MARKET MANIPULATION AND INSIDER TRADING IN STOCK MARKETS: RISK INDICATORS AND CONTROL MODELS

Boysunov Jamshid Baxriddin ugʻli
Senior Lecturer at the Department of Corporate Finance and Securities
Tashkent State University of Economics

Article history:

Received: 30th November 2025
Accepted: 30th December 2025

Abstract:

The integrity of global financial markets is perpetually challenged by evolving methods of manipulation and the illicit exploitation of private information. As trading mechanisms transition from human-centric exchanges to high-frequency, algorithmic ecosystems, the nature of market abuse has shifted towards complex, microsecond-level anomalies and obscured network-based collusion. This research report provides an exhaustive examination of the theoretical and practical frameworks used to detect and prevent market manipulation and insider trading. Grounded in market microstructure theory, the analysis explores the efficacy of risk indicators such as Kyle's Lambda and the Volume-Synchronized Probability of Informed Trading (VPIN) in quantifying order flow toxicity. It further scrutinizes the evolution of surveillance models, contrasting traditional rule-based logic with state-of-the-art Deep Learning architectures, including Transformers for Limit Order Book (LOB) forecasting and Graph Neural Networks (GNNs) for identifying non-linear insider networks. A comparative legal analysis of the United States and European Union regulatory regimes highlights the divergence in enforcement philosophies and pre-trade risk controls. By synthesizing empirical data, algorithmic methodologies, and regulatory statutes, this report offers a roadmap for the next generation of market surveillance, emphasizing the necessity of adaptive, context-aware artificial intelligence in preserving market fairness.

Keywords: Market Manipulation, Insider Trading, Market Microstructure, Limit Order Book (LOB), Artificial Intelligence, Graph Neural Networks, VPIN, Financial Regulation, Algorithmic Surveillance, High-Frequency Trading.

The fundamental premise of a capital market is the efficient allocation of resources, a function that relies entirely on the integrity of price formation. Prices must reflect the aggregation of available public information and the genuine interplay of supply and demand. When this mechanism is distorted by manipulation—the artificial inflation or deflation of prices—or by insider trading—the exploitation of non-public information—the cost of capital rises, liquidity evaporates, and investor confidence is eroded. The detection of such abuses has historically been a reactive discipline, dependent on manual audits and whistleblower reports. However, the digitization of finance has necessitated a paradigm shift toward proactive, algorithmic surveillance.

In the contemporary landscape, the volume of data generated by financial markets is staggering. A single trading session on a major exchange can generate billions of data points, including order submissions, cancellations, and executions. Within this torrent of data, manipulative behaviors are often camouflaged as legitimate liquidity provision or hedging strategies. The rise of High-Frequency Trading (HFT) has further complicated the surveillance mandate, introducing manipulative tactics like "spoofing" and "layering" that exist for mere milliseconds—far below the threshold of human perception. Consequently, financial institutions and regulators are increasingly turning to Artificial Intelligence (AI) and Machine Learning (ML) to police these markets. A 2024 survey by the UK Financial Conduct Authority (FCA) revealed that 75% of financial services firms have integrated AI into their market abuse detection frameworks, a significant increase from 58% just two years prior. Similarly, 99% of leading derivatives firms reported deploying AI in some capacity by 2023, underscoring the ubiquity of these technologies in modern risk management.

This report aims to deconstruct the technological and theoretical arsenal employed in the

World Economics & Finance Bulletin (WEFB)
Available Online at: https://www.scholarexpress.net
Vol. 54, January, 2026
ISSN: 2749-3628,

fight against market abuse. It begins by establishing the market microstructure foundations that define "informed trading" and "toxicity." It then categorizes the spectrum of manipulative behaviors, from blunt trade-based schemes to sophisticated order-book algorithms. The core of the analysis focuses on the transition from static, parameter-based risk indicators to dynamic Deep Learning models capable of unsupervised anomaly detection. Specifically, it examines how Convolutional Neural Networks (CNNs) and Transformers are used to decipher the visual and temporal language of the Limit Order Book (LOB), and how Graph Neural Networks (GNNs) are revolutionizing the detection of insider trading by mapping the invisible social and transactional edges between market participants. Finally, the report contrasts the regulatory approaches of the United States and the European Union, positing that technology must be paired with robust legal frameworks to effectively deter market malfeasance.

To effectively detect manipulation, one must first understand the physics of the market, a discipline known as market microstructure. This field analyzes how specific trading mechanisms, rules, and participant interactions affect price formation and liquidity. The central challenge in microstructure is distinguishing between "uninformed" order flow—generated by liquidity needs or portfolio rebalancing—and "informed" order flow—generated by traders possessing private information or manipulative intent.

The theoretical basis for detecting informed trading is heavily influenced by the work of Albert Kyle (1985) and subsequent models by Glosten and Milgrom. These models conceptualize the market as an interaction between three distinct agents: the informed trader (who knows the true future value of the asset), the noise trader (who trades randomly), and the market maker (who sets prices to clear the market).

In this ecosystem, the market maker faces an adverse selection problem. If they trade with an informed trader, they will lose money, as the informed trader only buys when the asset is undervalued and sells when it is overvalued. To compensate for this risk, the market maker adjusts prices based on the order flow imbalance. The sensitivity of price to order flow is quantified by **Kyle's Lambda (λ)**, a critical metric in surveillance.

The relationship is expressed linearly:

$$P_t = P_{t-1} + \lambda * Q_t + \varepsilon_t$$

Where P_t is the price change, Q_t is the net order flow (signed volume), and λ represents the **price impact** or illiquidity of the asset.

- **Interpretation:** A high λ indicates that a small amount of volume is moving the price significantly. This suggests that the market maker suspects a high concentration of informed trading (or manipulation) and is withdrawing liquidity (widening spreads and reducing depth) to protect themselves.
- **Surveillance Application:** By monitoring real-time fluctuations in λ, surveillance algorithms can detect periods of "toxic" order flow. If λ spikes without a corresponding public news event, it acts as a strong risk indicator of insider trading or a "pump and dump" operation in progress.

However, empirical research notes that λ is not static. In modern automated markets, price impact is dynamic and path-dependent. The "memory" of the order book means that the impact of a trade can decay over time, a phenomenon that advanced stochastic models attempt to capture. Research indicates that while aggregate noise trading volatility might be unpredictable (a martingale), the market depth (inverse of λ) tends to adjust in equilibrium, making λ a submartingale that generally increases during periods of informational asymmetry.

Traditional asset pricing models often relied on execution data (Level 1 data: price and volume of completed trades). However, modern detection requires a granular view of the **Limit Order Book (LOB)**. The LOB is the central queue of all outstanding buy and sell orders at every price level.

- **Level 1:** Best Bid and Best Ask.
- **Level 2:** The top N price levels (e.g., best 10 bids and asks).
- **Level 3:** Full message traffic, encompassing every submission, cancellation, and modification.

Manipulators frequently operate in the LOB without executing trades, using strategies that create a false appearance of supply or demand. Therefore, a robust surveillance model must reconstruct the LOB from raw message data (like NASDAQ's ITCH feed) to visualize the "shape" of the market. This allows for the detection of anomalies such as order imbalances deep in the book, which would be invisible to a system monitoring only execution prices. The shift to LOB-centric analysis has driven the adoption of computer vision techniques

World Economics & Finance Bulletin (WEFB)
Available Online at: https://www.scholarexpress.net
Vol. 54, January, 2026
ISSN: 2749-3628,

in finance, where the LOB is treated as a dynamic image rather than a simple time series.

Market abuse is not a monolithic entity but a diverse taxonomy of behaviors, each requiring distinct detection methodologies. Regulatory bodies and academics generally classify these into three categories: Trade-based, Order-based (Action-based), and Information-based manipulation.

Type of Manipulation	Description	Mechanism of Action	Primary Detection Signal
Wash Trading	Simultaneous buying and selling of the same asset by the same entity (or colluding entities).	Creates artificial volume to lure momentum traders or inflate exchange rankings. No change in beneficial ownership.	Self-Match Prevention (SMP) logs; Closed-loop cycles in trader graphs.
Painting the Tape	A group of traders buying a security among themselves to create a price trend.	Manipulates the "Last Traded Price" to trigger technical indicators or attract outsiders (Pump & Dump).	Anomalous price/volume correlation; Graph analysis of trader clusters.
Marking the Close	Executing orders at the very end of the trading session.	Influences the closing price, which is often used for valuing derivatives or mutual funds.	Volume spikes at exactly 15:59:59; Deviation from VWAP (Volume Weighted Average Price).
Cornering the Market	Securing a dominant position in a tradable asset or its underlying commodity.	Forces short sellers to cover their positions at inflated prices due to lack of available supply.	Concentration of Open Interest; Inventory analysis.

The speed of HFT has given rise to order-based manipulations that rely on deception rather than execution.

- **Spoofing:** This involves placing a large order on one side of the book (e.g., a buy order) with the explicit intent to cancel it before execution. The spoofer's goal is to create a visual impression of high demand (a "buy wall"). Other algorithms, detecting this imbalance, react by buying, which pushes the price up. The spoofer then cancels their buy order and executes a sell order against the artificially inflated price. This entire cycle can occur in milliseconds. Effective detection requires analyzing the **Order-to-Trade Ratio (OTR)** and the **cancellation latency** (time between placement and cancellation).
- **Layering:** A variant of spoofing where the manipulator places multiple limit orders at different price levels (layers) on one side of the book. This creates a false slope in the supply/demand curve, misleading sophisticated liquidity-seeking algorithms. Layering is harder to detect than simple spoofing because the volume is distributed, requiring models that analyze the aggregate shape of the LOB.
- **Quote Stuffing:** This tactic involves flooding the exchange with a massive number of order updates (submissions and cancellations) in a short burst. The objective is often not to trade, but to generate **latency**. By clogging the exchange's matching engine or the data feeds of competitors, the "stuffer" creates a momentary information lag, which they can exploit for arbitrage. Detection involves monitoring message rates and identifying bursts of activity that lack economic rationale (e.g., 5,000 updates in a second with zero executions).
- **Momentum Ignition:** The manipulator executes a series of aggressive trades to trigger stop-loss orders or other automated responses from passive algorithms, causing a rapid, cascading price movement. Once the price moves, the manipulator reverses their position to profit from the rebound.

To automate surveillance, theoretical concepts must be translated into computable features—

World Economics & Finance Bulletin (WEFB)
Available Online at: https://www.scholarexpress.net
Vol. 54, January, 2026
ISSN: 2749-3628,

quantitative risk indicators that can be monitored in real-time.

One of the most significant advancements in measuring order flow toxicity is the **VPIN** metric (Volume-Synchronized Probability of Informed Trading), developed by Easley, López de Prado, and O'Hara. Traditional time-based sampling (e.g., 1-minute bars) is flawed because information flow in markets is not constant; it arrives in bursts. VPIN solves this by operating in **Volume Time**.

The VPIN Algorithm:

1. **Volume Buckets:** Data is sampled not by time, but by volume. A "bucket" is defined as a fixed number of shares traded (e.g., every 10,000 shares). During high activity, buckets fill rapidly; during lulls, they fill slowly. This aligns the sampling rate with the information arrival rate.
2. **Bulk Volume Classification (BVC):** Since the aggressor side of a trade isn't always explicitly tagged in public data, BVC estimates the buy (V^B) and sell (V^S) volume within each bucket using price changes. The formula relies on the standardized normal distribution (Z) of price returns:

$$V_T^B = V_{bucket} * Z\left(\frac{P_T - P_{T-1}}{\sigma \Delta P}\right)$$

$$V_T^S = V_{bucket} - V_T^B$$

3. **Order Imbalance (OI):** The absolute difference between buy and sell volume in a bucket:

$$OI_T = |V_T^B - V_T^B|$$

4. **VPIN Calculation:** The metric is the moving average of this imbalance over η buckets, normalized by the total volume:

$$\text{VPIN} = \frac{\sum_{i-1}^{\eta} OI_{T-i}}{\eta * V_{bucket}}$$

Significance: A high VPIN value indicates that trading is heavily one-sided and driven by informed participants. Empirical studies have validated VPIN as a robust predictor of "Flash Crashes" and periods of extreme volatility. For instance, VPIN reached historically high levels hours before the 2010 Flash Crash, providing a warning signal that traditional volatility metrics missed.

Beyond VPIN, several other indicators serve as proxies for market manipulation risk:

- **Bid-Ask Spread Dynamics:** In the presence of insider trading, market makers widen spreads to insure against adverse selection. A sudden, unexplained widening of the spread is a classic indicator of toxicity.
- **Market Depth Erosion:** Manipulators engaged in momentum ignition will often wait for (or cause) a thinning of the LOB. Monitoring the "depth resilience"—how quickly the book replenishes after a large trade—helps identify fragile states where manipulation is more likely to succeed.
- **Price-Volume Divergence:** According to technical analysis principles often incorporated into ML features, price trends unsupported by volume are suspect. Conversely, massive volume with little price movement can indicate "churning" or wash trading.

The evolution of surveillance technology has progressed through three generations: Rule-Based, Statistical/Machine Learning, and Deep Learning.

Static Models: Early surveillance relied on static rules (e.g., "Flag if Price Change > 5%"). While transparent, these are brittle. The second generation introduced **Static Machine Learning**, where individual trading instances (orders or time windows) are treated as isolated data points. Features (VPIN, spread, cancellations) are fed into classifiers like Support Vector Machines (SVM) or Random Forests.

- *Performance:* Studies using datasets from Borsa Istanbul and NASDAQ have shown that supervised static models can achieve F1 scores exceeding 90%.
- *Limitation:* They fail to capture the *sequence* of events. A single cancelled order is not manipulation; a sequence of "Submit -> Wait -> Cancel -> Trade Opposite" is.

Dynamic Models: Dynamic models view manipulation as a process unfolding over time. **Hidden Markov Models (HMMs)** are the archetype here. An HMM assumes the market exists in latent "states" (e.g., Stable, Accumulation, Manipulation, Distribution).

- *Mechanism:* The model calculates the transition probabilities between states based on the observed sequence of trade data. It can identify a "Manipulation State" based on the trajectory of price and volume, even if no single data point is anomalous on its own.
- *Advantage:* HMMs are superior at detecting complex, multi-stage strategies like Pump-and-Dump schemes, where the early accumulation phase looks innocuous to a static model but fits a specific sequential pattern.

The primary bottleneck for Supervised Learning (training a model on "Manipulated" vs "Normal" examples) is data scarcity. Confirmed cases of

World Economics & Finance Bulletin (WEFB)
Available Online at: https://www.scholarexpress.net
Vol. 54, January, 2026
ISSN: 2749-3628,

manipulation are rare (class imbalance), and regulatory investigations are confidential.

- **Synthetic Data Augmentation:** To address this, researchers use techniques like SMOTE (Synthetic Minority Over-sampling Technique) or even Generative Adversarial Networks (GANs) to create realistic "fake" manipulation data to train models. This ensures the classifier doesn't simply bias towards predicting "Normal" 99.9% of the time.
- **Benchmarking:** Standardized datasets like **LOBSTER** (which reconstructs NASDAQ data) are crucial for benchmarking these models, allowing researchers to compare the efficacy of SVMs, Neural Networks, and Decision Trees on identical high-fidelity data.

The third and current generation of surveillance utilizes Deep Learning. These models do not rely on human-engineered features (like VPIN); instead, they learn representations directly from the raw data.

In this approach, the LOB is visualized as a heatmap or image: the X-axis is time, the Y-axis is price level, and the color intensity is volume.

- **Architecture:** CNNs, originally designed for image recognition (like identifying cats in photos), are applied to these "market images." Convolutional filters slide across the LOB history, learning to recognize spatial patterns.
- **Application:** A CNN can learn the "shape" of a layering algorithm—a specific geometric configuration of orders in the book—without being explicitly programmed to look for it. This allows for the detection of novel, previously unseen manipulation algorithms.
- **Results:** Research indicates CNN-based detectors significantly outperform Logistic Regression and standard Multi-Layer Perceptrons (MLPs) in identifying non-linear patterns in high-frequency data.

While CNNs excel at spatial patterns, they struggle with long-range temporal dependencies (e.g., an event at 10:00 AM influencing an event at 2:00 PM). The **Transformer** architecture (the basis of GPT models) addresses this via the **Self-The LiT (LOB-in-Transformer) Model:** This novel architecture treats segments of LOB data as "patches" (similar to words in a sentence). The attention mechanism assigns weights to different patches, learning which historical market states are most relevant to the current prediction.

- **Advantage:** LiT models can capture the "narrative" of a trading day. They might "attend" strongly to a liquidity imbalance that occurred 500 timesteps ago, recognizing it as the precursor to a current price spike.
- **Performance:** Empirical benchmarks show LiT models achieve state-of-the-art results in LOB forecasting and anomaly detection, outperforming LSTM (Long Short-Term Memory) networks, which suffer from "forgetting" over long sequences.

Insider trading is fundamentally a relational problem. It involves networks of entities (tippers, tippees, accounts, companies) and their interactions. Tabular data (rows and columns) cannot effectively model these relationships. **Graph Neural Networks (GNNs)** are designed for this exact purpose.

Graph Construction:

- **Nodes:** Traders, Bank Accounts, IP Addresses, Phone Numbers, Stock Tickers.
- **Edges:** Transactions, Shared Device Logins, Familial Ties, Social Media Connections.
- **Edge Features:** Time of interaction, value of transfer.

Detection Mechanism: GNNs (such as GraphSAGE or Relational-GCNs) propagate information across the edges.

1. **Node Embedding:** The model learns a vector representation for each trader based on their neighbors.
2. **Contextual Anomaly Detection:** If Trader A is legitimate but connects to Trader B (who is suspicious), the embedding of Trader A shifts. The GNN can identify a "ring" of insiders who trade in sync before Price Sensitive Events (PSEs), even if their individual trading volumes are small enough to evade static filters.
3. **Implicit Graphs:** Advanced models not only look at explicit transactions but construct "implicit" edges between traders who exhibit similar behavioral patterns (e.g., two strangers who always buy the same stock 10 minutes before an announcement).

- **Impact:** GNNs drastically reduce false positives by providing *context*. A large trade is not suspicious; a large trade by a node 2 hops away from the CEO's brother is..

Technological detection must be enforced by regulatory frameworks. The approach to market abuse varies significantly across jurisdictions, particularly between the United States and the European Union.

Prevention is the first line of defense. Exchanges and brokers implement "gatekeeper" controls to block manipulative orders before they reach the matching engine.

World Economics & Finance Bulletin (WEFB)
Available Online at: https://www.scholarexpress.net
Vol. 54, January, 2026
ISSN: 2749-3628,

- **Price Banding:** Limits the price at which an order can be entered relative to the last traded price, preventing "fat finger" errors that cause flash crashes.
- **Kill Switches:** Automated protocols that disconnect a trading firm if their algorithm malfunctions (e.g., executing excessive volume in seconds).
- **Self-Match Prevention (SMP):** A critical control for preventing wash trading. If a firm's buy order matches its own sell order, the exchange's matching engine automatically cancels one or both, ensuring no artificial volume is printed.

Feature	United States (SEC/CFTC)	European Union (MAR)
Legal Basis for Insider Trading	**Fiduciary Duty:** Based on case law (Chiarella, Dirks). Requires proving a breach of duty or misappropriation of information.	**Parity of Information:** Statutory definition. Focuses on the possession of inside information, regardless of how it was obtained.
Scope of Reporting	**SARs (Suspicious Activity Reports):** Filed by broker-dealers for suspicious transactions.	**STORs (Suspicious Transaction and Order Reports):** Broader scope. Requires reporting of *attempted* manipulation (unexecuted orders) and executed trades.
Sanctions	Civil penalties (up to 3x profit), criminal fines, imprisonment. Heavy emphasis on disgorgement.	Harmonized administrative and criminal sanctions across member states. Fines can be up to 15% of turnover.
Commodities/Derivatives	**CFTC Principles:** Specific "Electronic Trading Risk Principles" mandate pre-trade controls and system safeguards for DCMs.	**MAR Extension:** Explicitly covers spot commodities and derivatives markets to prevent cross-market manipulation.

The Cross-Market Challenge: A major regulatory gap is fragmentation. A manipulator might buy a stock on Exchange A to profit from a derivative on Exchange B. The US "Consolidated Audit Trail" (CAT) and EU cross-venue surveillance initiatives aim to aggregate data to see the holistic footprint of such strategies.

The efficacy of AI surveillance is inextricably linked to data quality. The **LOBSTER** dataset (Limit Order Book System - The Efficient Reconstructor) has emerged as the academic standard. By processing NASDAQ's historical TotalView-ITCH data, LOBSTER provides a tick-by-tick reconstruction of the order book up to 200 levels deep. This allows researchers to train models on the exact sequence of events that occurred during historical manipulation cases, providing a rigorous ground truth for benchmarking.

However, challenges persist. Financial data is **non-stationary**; the statistical properties of the market change over time (e.g., pre-COVID vs. post-COVID volatility). A model trained on 2019 data may fail in 2024. Consequently, "Online Learning" algorithms, which continuously update their weights with new data, are becoming essential for maintaining detection accuracy in dynamic environments.

The detection and prevention of market manipulation have evolved from a compliance obligation into a complex technological arms race. The integration of high-frequency algorithmic trading has necessitated a move beyond simple rule-based surveillance to sophisticated AI-driven ecosystems.

The theoretical insights of Kyle and Glosten have been successfully operationalized into real-time metrics like VPIN, providing quantitative measures of order flow toxicity. Simultaneously, the application of Deep Learning—specifically Transformers and CNNs—has unlocked the ability to detect manipulation by analyzing the "shape" and "narrative" of the Limit Order Book, rather than just isolated trade prints. Furthermore, the deployment of Graph Neural Networks addresses the opaque nature of insider trading, illuminating the hidden social and transactional webs that facilitate collusion.

However, technology alone is not a panacea. It must be underpinned by robust regulatory frameworks like the EU's Market Abuse Regulation and the US electronic trading principles, which mandate strict pre-trade controls and cross-market transparency. As manipulators increasingly leverage Generative AI to design evasive strategies, the defense must continue to

World Economics & Finance Bulletin (WEFB)
Available Online at: https://www.scholarexpress.net
Vol. 54, January, 2026
ISSN: 2749-3628,

innovate, moving towards explainable, context-aware systems that ensure the financial markets remain a mechanism for fair and efficient capital allocation, rather than a playground for predatory algorithms.

References:

1. NICE Actimize. (2024). AI Adoption Accelerates: Smarter Surveillance, Faster Action.
2. Congressional Research Service. (2024). AI Use and Derivatives: Background. In Focus, IF13072.
3. Bouchaud, J. P., et al. (2022). Kyle's Lambda and Market Microstructure.
4. Ahern, K. R. (2018). Do Proxies for Informed Trading Measure Informed Trading? NBER Working Paper No. 24297.
5. Easley, D., López de Prado, M. M., & O'Hara, M. (2012). Flow Toxicity and Liquidity in a High-Frequency World. Review of Financial Studies.
6. Haas School of Business. (2021). Stochastic Liquidity and Kyle's Lambda Dynamics.
7. Ravagnani, A. (2025). Statistical and machine learning for market abuse detection and limit order book modeling. SNS Theses.
8. LOBSTER Data. (2013). LOBSTER: Limit Order Book System - The Efficient Reconstructor. NASDAQ TotalView-ITCH.
9. FMSB. (2022). Behavioural Cluster Analysis: Misconduct Patterns in Financial Markets.
10. Investopedia. (2024). Wash Trading: Definition, Mechanism, and Regulations.
11. FCA. (2015). Thematic Review TR15/1: Asset management firms and the risk of market abuse.
12. eFlow Global. (2024). High Impact Market Manipulation Tactics: Red Flags for Modern Surveillance Teams.
13. Krypton Labs. (2023). VPIN: The Coolest Market Metric You've Never Heard Of. Medium.
14. Abad, D., & Yagüe, J. (2012). From PIN to VPIN: An introduction to order flow toxicity.
15. Easley, D., et al. (2013). Volume-Synchronized Probability of Informed Trading (VPIN).
16. Tsay, R. S. (2023). VPIN Calculation and Volume Bucketing Methodology.
17. Corcoran, C. (2013). Systemic Liquidity Risk and Bipolar Markets.
18. Ahern, K. R. (2018). Bid-Ask Spread and Insider Trading Detection. NBER.
19. Goz, M., et al. (2022). Trade-based manipulation detection using supervised machine learning. Computational Economics.
20. Zhai, J., Cao, Y., & Ding, X. (2018). Data analytic approach for manipulation detection in stock market.
21. Cao, Y., et al. (2018). Static and dynamic models: A framework for price manipulation detection.
22. Golmohammadi, K., et al. (2021). Hidden Markov Models for Market Manipulation Detection.
23. Chullamonthon, P., & Tangamchit, P. (2023). Ensemble of supervised and unsupervised deep neural networks for stock price manipulation detection.
24. Sirignano, J., et al. (2019). Deep Learning for Limit Order Books.
25. Poutré, C. (2023). Transformer model for limit order book anomaly detection. HEC Montréal.
26. LiT Architecture. (2025). LiT: A Novel Transformer-based Model for LOB Forecasting.
27. Zhang, Z., et al. (2025). Temporal dependencies in LOB: Transformers vs LSTM.
28. Tamersoy, A., et al. (2013). Inside Insider Trading: Patterns & Discoveries from a Large Scale Exploratory Analysis. Georgia Institute of Technology.
29. AWS Machine Learning. (2022). Detect financial transaction fraud using a Graph Neural Network with Amazon SageMaker.
30. Eberle, W., et al. (2011). Graph-based anomaly detection in social networks.
31. Ambairam, M. (2025). Temporal Quantum Neural Networks for Insider Threat Detection.
32. eftsure. (2024). Graph Neural Networks in Finance: Nodes, Edges, and Fraud Detection.
33. Ravagnani, A. (2025). Contextual anomaly detection in insider trading rings.
34. FIA. (2024). Automated Trading Risk Controls.
35. Gevurtz, F. A. (2025). Duty Bound: A Comparison of Insider Trading Law in the United States and the European Union.
36. Gevurtz, F. A. (2016). The New EU Market Abuse Regulation: Impact on US Issuers.
37. FCA. (2015). Suspicious Transaction and Order Reports (STORs).
38. Skadden. (2016). The New EU Market Abuse Regulation: Impact on US Issuers.
39. Ventoruzzo, M. (2014). Comparing Insider Trading Sanctions: US vs EU.

World Economics & Finance Bulletin (WEFB)
Available Online at: https://www.scholarexpress.net
Vol. 54, January, 2026
ISSN: 2749-3628,

40. CFTC. (2020). Electronic Trading Risk Principles. Federal Register.
41. IOSCO. (2022). Market Manipulation in Cross-Border and Cross-Market Contexts.
42. LOBSTER Data. (2023). LOBSTER Academic Data Provider Info.