H3M.IO

Case Study: Ak Yatırım's AI-Driven Evolution in Detecting Market Manipulation and Financial Crime in Capital Markets

Prepared by

Ferhat Demir, Compliance Manager, Ak Yatırım

Tolga Kurt, Managing Partner, H3M Analytics

Introduction

The financial world, with its vast complexities and intricate dynamics, is a challenging domain. Ak Yatırım, a leading entity in securities trading, recognized the ever-growing threats posed by market manipulations. Manipulation is a serious problem in the securities market and its detection is critical. In 2022, drawing from H3M's successful collaboration with Akbank in retail banking compliance, Ak Yatırım aimed to harness the transformative power of AI and machine learning to not only to anti-money-laundering but also to tackle the multifaceted challenges of market manipulation.

The Challenge

Market manipulation is a vast and intricate domain, rife with a myriad of deceptive tactics that can destabilize the financial ecosystem. These tactics range from the seemingly innocuous to the overtly malicious, each with its unique footprint and impact on the market. These practices are illegal and can result in severe penalties, including fines and imprisonment, as they undermine the integrity of

financial markets. AML compliance is critical to protect the financial system from being used for money laundering and other illicit activities. Brokerage firms that fail to implement robust AML procedures can face significant legal and financial consequences.

- Wash-trading: This involves buying and selling securities without any change in ownership, creating a false impression of active trading to artificially inflate the price. Wash trading can mislead the market and give a misleading impression about the liquidity and supply of a financial instrument.
- Transfer of funds: Manipulators move funds between accounts to obfuscate the origins of money, often to give the illusion of liquidity or to hide illicit gains.
- Spoofing the tape: This tactic involves placing orders with no intention of execution and misleading other traders about the supply or demand of security. Stock prices will instantly jump, creating the impression of high demand, which will cause others to buy this manipulated stock, allowing the manipulator to sell at a higher price.
- Short&distort: Here, manipulators short-sell a stock and then spread false rumors to drive down its price, profiting from the decline.
- Shell accounts: These are accounts that exist only on paper and are used to hide ownership or transactions, often to facilitate other types of market manipulation.
- Pump&Dump; Poop&Scoop: Classic schemes where manipulators inflate (pump) stock prices through false or misleading statements to sell their holdings at a profit. Conversely, they might spread negative rumors to decrease a stock's price (poop) and then buy it at a lower rate (scoop).
- Pooling: This involves several individuals or entities collaborating to manipulate a stock's price.
- Insider trading: Trading based on non-public, material information, giving certain individuals an unfair advantage.
- High closing: Manipulating the closing price of a stock by executing purchase orders at or near the close of trading.
- Circulation of funds: This involves circular trading where funds or securities are traded without any genuine change in ownership.
- Churning: Excessive trading by brokers in a client's account to generate commissions rather than to benefit the client.
- Banned Entities/Stocks: Trading or facilitating trades involving entities or stocks that have been prohibited or blacklisted.

It’s important to engage in ethical and legal trading practices. The overarching challenge was not merely to detect these manipulations. The real test lay in predicting them before they could inflict

damage, preventing their occurrence, and delving deep to provide insights into their origins. This was imperative to ensure market integrity, promote transparency, and safeguard the trust that investors place in the financial system.

The Data: The Foundation of All Solutions

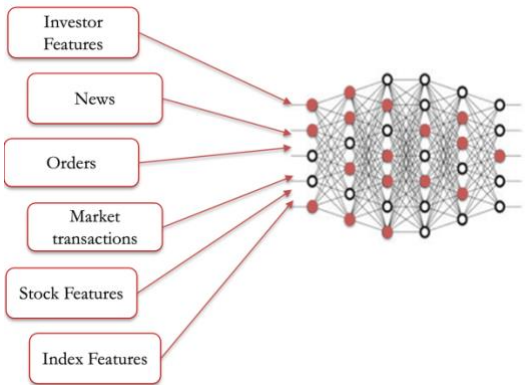
Preventing suspicious transactions in the stock market with an artificial intelligence (AI)--based program is a proactive approach to maintaining market integrity. The backbone of any AI-driven solution is the data it feeds on. For Ak Yatırım, this meant:

- **Investor CRM Features:** A treasure trove of data, capturing investor behaviors, preferences, relationships, and demographic data.
- **Investor Transaction History:** Data related to past orders and transactions of the investors.
- **Stock Market News:** Real-time updates and historical data on news reported to the exchanges through platforms such as KAP, providing context to trading behaviors.
- **Order Data:** Every order, both realized and unrealized, along with its intricate properties, served as a goldmine of information.
- **Historical Values:** Past data on stock and index values, that are essential for trend analysis and pattern recognition.

The Solution

1. Machine Learning in Action

Machine learning algorithms can be trained on historical data to recognize patterns associated with market manipulation. These models can adapt and improve over time as new data becomes available. It is not possible to manually analyze a huge amount of data, so machine learning came to the fore in analyzing data. Machine learning with KROTON Suspect Miner, with its unparalleled ability to analyze vast datasets and recognize intricate patterns, was the cornerstone of our solution. The methodologies employed were both diverse and tailored to the specific challenges of market manipulation.



- **Feature Engineering:** Before training the models, significant emphasis was placed on feature engineering. This involved extracting relevant features from the investor CRM, stock market news, order data, and historical values. Features such as trading frequency, order size, and stock preferences were meticulously crafted to provide the models with the best possible data representation.

- **Anomaly Detection:** Advanced anomaly detection algorithms were employed to identify unusual trading patterns. This was particularly useful in detecting manipulations like insider trading, where trading activities significantly deviate from the norm right before major stock announcements.

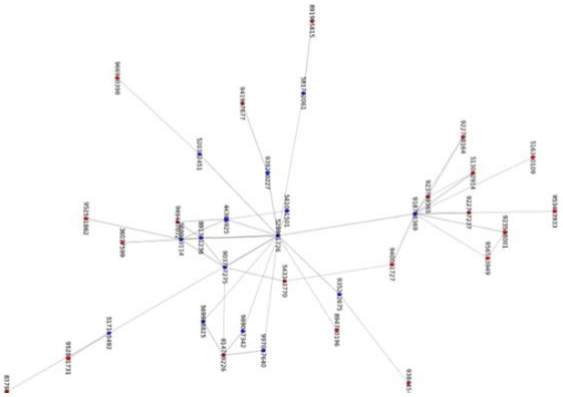
- **Active Learning:** This approach was integrated to enhance the model's capability to detect previously unknown patterns. Active learning, by design, allows the model to query the user for input on the most ambiguous instances, ensuring continuous learning and adaptation to new manipulative tactics.

- **Explainable Algorithms:** Given the critical nature of financial decisions, the importance of model explainability cannot be overstated. Algorithms like Random Forest were chosen for their inherent explainability. These algorithms not only provide predictions but also offer insights into which features were most influential in making those predictions. This transparency is pivotal in building trust and understanding of the system's decisions.

2. Network Analysis for Coordinated Manipulation

Many stock exchange manipulation instances, feature coordination between groups of traders who trade heavily among themselves. Through the utilization of KROTON Link Miner, network analysis provided a fresh, interconnected perspective on the data, especially in the context of stock markets where transactions aren't direct transfers between entities. The methodologies here were focused on identifying relationships, potential collisions, and coordinated manipulations:

- **Graph Theory:** The trading data was represented as a graph, with entities (traders) as nodes and transactions as edges. This representation allowed for the identification of densely connected subgraphs, indicative of coordinated activities. CRM Connections and Transactional Relationships: Unlike traditional AML scenarios, the network analysis for stock markets required a different approach. Using CRM connections, attempts were made to link multiple entities based on transactions in the same stock. The criteria for these connections were based on the percentage of daily volume accomplished by a party, denoted as %X. Specific connection rules were established:
    - Party A and B both sell with at least X%.
    - Party A and B both buy with at least X%.
    - Party A buys and B sells with at least X%.
    - Party A sells and B buys with at least X%.



- **Order vs. Transactions Analysis:** In addition to actual transactions, the analysis also considered open and canceled orders. For instance, if Party A placed a large order, driving the price up, and then Party B sold at this inflated price, any subsequent cancellation of Party A's orders would be flagged as potential manipulation.

- **Centrality Measures:** By calculating various centrality measures, such as degree centrality and eigenvector centrality, influential entities in the trading network were identified. These entities, due to their significant influence, were monitored closely for potential manipulative behaviors.

- **Community Detection**: Algorithms like the Louvain method were employed to detect communities within the trading network. These communities, or clusters of closely connected entities, were analyzed to identify potential collusions or coordinated manipulations.

- **Temporal Analysis:** Time-stamped transaction data was analyzed to detect patterns that emerged over specific intervals. This was crucial in identifying manipulations that were spread out over time, such as pump and dump schemes.

Network analysis demonstrated how KROTON Link Miner can analyze various data sources, patterns, and behaviors to detect suspicious transactions in the stock market.

By continuously monitoring and applying machine learning algorithms, it can play a crucial role in maintaining market integrity and identifying potential market abuse.

3. RUMI: The Compliance Search Engine

In the intricate web of stock market trading and potential manipulations, having a dedicated search engine like RUMI became indispensable. Tailored specifically for market manipulation-related searches, RUMI was designed to complement the methodologies employed in the Suspect Miner and Network Analysis sections.

- **Deep Dive into Company Relationships:** Understanding the intricate relationships between companies is crucial in detecting potential market manipulations. RUMI was equipped to explore these relationships, identifying affiliations, partnerships, or any other connections that might be used for coordinated manipulations.

- **Security Exchange Commission Bans**: Keeping abreast of the latest bans and restrictions imposed by the Security Exchange Commission is vital. RUMI ensured that any recent bans, especially those related to market manipulations, were immediately flagged and brought to attention. This information was particularly useful in corroborating suspicions raised by machine learning models or network analysis.

- **Adverse Media Scanning:** In today's digital age, news spreads rapidly. RUMI was adept at scanning adverse media reports, which could provide early warnings or additional context to potential manipulative behaviors. A sudden spike in negative news about a company, for instance, could be indicative of an impending manipulation. Information-based manipulation is a type of manipulation that can be applied more easily than transaction-based manipulation and can be done at less cost than transaction-based manipulation.

- **Enhancing Network Analysis:** While the primary network analysis focused on CRM connections and transactional relationships, RUMI added another layer by identifying potential connections through external sources. Entities that might not have an apparent connection through CRM or direct transactions could be linked through shared adverse media reports or social media interactions. This expanded the scope of the network analysis, ensuring a more comprehensive detection mechanism.

By seamlessly integrating with the other tools and methodologies, RUMI ensured that no stone was left unturned in the quest to detect, predict, and prevent market manipulations.

H3M.IO

Results

The KROTON The implementation of our comprehensive solution yielded tangible results in detecting market manipulations. Here's a breakdown of our detection rates for various manipulative behaviors:

Insider Trading: We detected activities that consistently generated profits within 24 hours before public announcements causing significant stock price changes. The suspect rate for such activities stood at approximately 15%.

Deviation From Behaviour: We identified behavior deviations, such as a trading volume increase in the last week compared to the average of the previous two months. This metric generally didn't raise many alarms, with a suspect rate of less than 5%.

Price Manipulation: High stock price changes influenced by high-volume trades had a suspect rate of around 11%.

Contrary market movements: (e.g., significant sales during high buying periods and vice versa) had a suspect rate of about 6%.

Creating demand illusions by making numerous small-lot [1:3] trades in a single day had a high suspect rate of approximately 70%.

Making a single trade with a volume significantly above the market average had a suspect rate of around 12.5%.

Outlier from Profile: High-volume trades by risky customer groups, such as an unemployed individual trading stock worth millions, had a suspect rate of about 6%. We flagged executing intensive transactions of high amounts from a customer's account that are not by the customer's characteristics such as age, professional qualifications, financial situation, experience, and knowledge in capital markets.

Other important cases were also investigated and currently under investigation for future AI work are related to:

Front Running: This involved making trades on one's account before placing known large-volume orders in the market. This method goals to take advantage of the possible price effect by conducting a transaction before the order, which may affect the market price of a market actor, is transmitted to the stock market.

Insider Trading Policy: We ensured compliance by detecting whether individuals, legally restricted from trading certain stocks, were doing so.

Fake Algorithmic Trading: We identified patterns where orders were continuously placed and a significant portion was canceled shortly after.

Money Laundering through Spread Costs: This involved bearing spread costs and laundering money through dual-sided orders.

Currency-based Transaction Monitoring: We recorded transactions made in the last month based on currency and set controls based on this range for subsequent trades.

Unusual Deposit Patterns: We flagged transactions where the deposited amount exceeded the customer's usual deposit range.

Unusual Trading Patterns: We detected when customers traded in currency pairs or future contracts different from their usual patterns.

High-Risk IPs: We monitored and flagged transactions made from IPs that were deemed risky. We controlled that accessing from the same IP address to perform transactions on behalf of different customers who were not related to each other.

Continuous Trading in Illiquid Pairs: We detected patterns where trades were consistently made in illiquid currency pairs.

Unusual Orders in Option and Future Markets: We flagged regular limit orders placed significantly above or below the spot price in option and future markets with low trading volumes.

These results underscored the effectiveness of our solution in maintaining market integrity and protecting investor interests.

Conclusion

The KROTON software platform, a culmination of H3M's efforts, became an integral part of AkYatırım's operations. Generating daily suspicious activity alerts, KROTON served as a vigilant watchdog, ensuring market integrity for over a year. This not only fortified Ak Yatırım's reputation of compliance and openness to novel technologies but also showcased the potential of AI-driven solutions in the financial world.

Ak Yatırım's journey with H3M is a testament to the transformative power of AI in the financial world. This collaboration not only ensured market integrity but also set a benchmark for other securities trading companies. As we look to the future, this case study serves as a beacon, illuminating the path forward in the ever-evolving world of finance.

About H3M

H3M is at the forefront of leveraging AI and machine learning to address complex challenges in the financial sector. With a commitment to innovation and excellence, H3M has successfully collaborated with industry leaders, offering solutions that are both cutting-edge and practical for AML, Sanctions Screening, Fraud detection, and market manipulation detection.

About Ak Yatırım

Ak Yatırım is 100% Akbank T.A.Ş. affiliate, and has a paid capital of 80.000.000 TL. Growing consistently and rapidly since the day it was established, Ak Yatırım offers domestic and foreign capital markets products to retail and commercial customers with its experienced sales department, comprehensive research reports, and customer-oriented service approach. In the scope of

intermediation services for public offering, Ak Yatırım provides its customers with a range of services including pre-initial structuring for public offering, valuation, management of SPK (CMB) and BIST processes, management of public offering publicity and promotion campaigns, management of domestic and overseas marketing and sales. Since 2005, Ak Yatırım has successfully mediated numerous public offerings worth over 3 billion US Dollars.

Ak Yatırım offers fast, reliable, investor-friendly, and high-quality services in all capital markets through its expert staff working in the headquarters and 10 offices located in major cities. "TradeAll" brand of Ak Yatırım allows easy, quick, and secure transmission of all investor transactions in domestic and foreign capital markets.

The Compliance Department at Ak Yatırım, within the framework of Law No. 5549 and its related legislation, conducts the compliance program created to ensure compliance with the regulations and performs the duties and responsibilities determined.