Infosys®
Navigate your next

VIEWPOINT

EFFECTIVE TRADE AND MARKET SURVEILLANCE THROUGH ARTIFICIAL INTELLIGENCE

It's getting harder to catch the bad guys in banking, proving that existing surveillance systems have become outmoded. New artificial intelligence (AI)-based surveillance systems can help, if implemented correctly.

Infosys® | Knowledge Institute

The U.S. Securities and Exchange Commission (SEC) filed enforcement actions against 700-850 odd firms and individuals over FY17-21, imposing average penalties of $1.2 billion annually.[1] Over the same period, the U.K. Financial Conduct Authority (FCA) imposed penalties of $233 million on roughly 14 firms and individuals annually.[2] Such incidents are recurring, with no signs of abating. Then new regulations come up or old ones are revised, further pressurizing the industry.

Existing tools with limited predefined rules are incapable of detecting fraudulent activities in the prevailing capital markets. It is time to consider evolving AI-based solutions with holistic and efficient surveillance capabilities, including communications surveillance, real-time alerts, identification of unknown manipulation techniques, and automation of regulatory compliance, among others.

Market complexities cripple rule-based systems

The trading of financial instruments is highly complex. It involves new asset classes (e.g., cryptocurrencies), new ways of buying stocks (e.g., fractional trading), and mobile-first or mobile-only platforms. Trading volumes have also surged post-pandemic. In the U.S., a record 10 million new trading accounts were opened in 2020.[3] Interestingly, more than half the trading in the U.S. happens through high-frequency trading (HFT), i.e., high-speed trade execution through computer algorithms.[4]

Financial institutions (FIs) are required to comply with several trade monitoring mandates. For example, the Dodd-Frank Swaps Surveillance regulation requires banks to provide a replay of trades and their associated communications within 72 hours of a request. However, the rising pace of suspicious transactions demands a strong surveillance system, especially when traders are working remotely and communicating over social platforms. In 2020, fund management firms (with $20 trillion in assets under management globally) found 6% of their total transactions to be suspicious.[5]

This has crippled the existing rule-based systems, making them ineffective in distinguishing between suspicious and legal trades. A survey of 17 FIs revealed that the ratio of actual suspicious transactions to total identified suspicious transactions can be as low as 0.01%.[6]

> Existing rule-based trade monitoring systems are unable to distinguish between suspicious and legal trades effectively

This is driving about 71% of organizations globally to upgrade their surveillance systems, says Thomson Reuters.[7]

AI-based solutions ensure holistic surveillance

AI-based solutions can process structured and unstructured data, automatically adapt to regulatory changes, and report suspicious incidents in real time.

This architecture (Figure 1) feeds raw data on orders, cancellations, trader communications, and historical alerts into a big data framework. Then, AI-based models analyze the data to identify suspicious activities and raise alerts for dodgy transactions, fraudulent behavior, and potential future incidents. Finally, visualization and reporting tools facilitate easy interpretation of findings, recording of resolutions, status tracking, etc.

> FIs and regulators can effectively monitor suspicious activities through AI-based surveillance systems

AI-based surveillance systems enable FIs and regulators to monitor suspicious activities effectively and to stay updated with the actions of market participants in real time. This leads to increased transparency, efficient case management, and proactive curtailment of market manipulations.

Key benefits of AI-based trade surveillance systems:

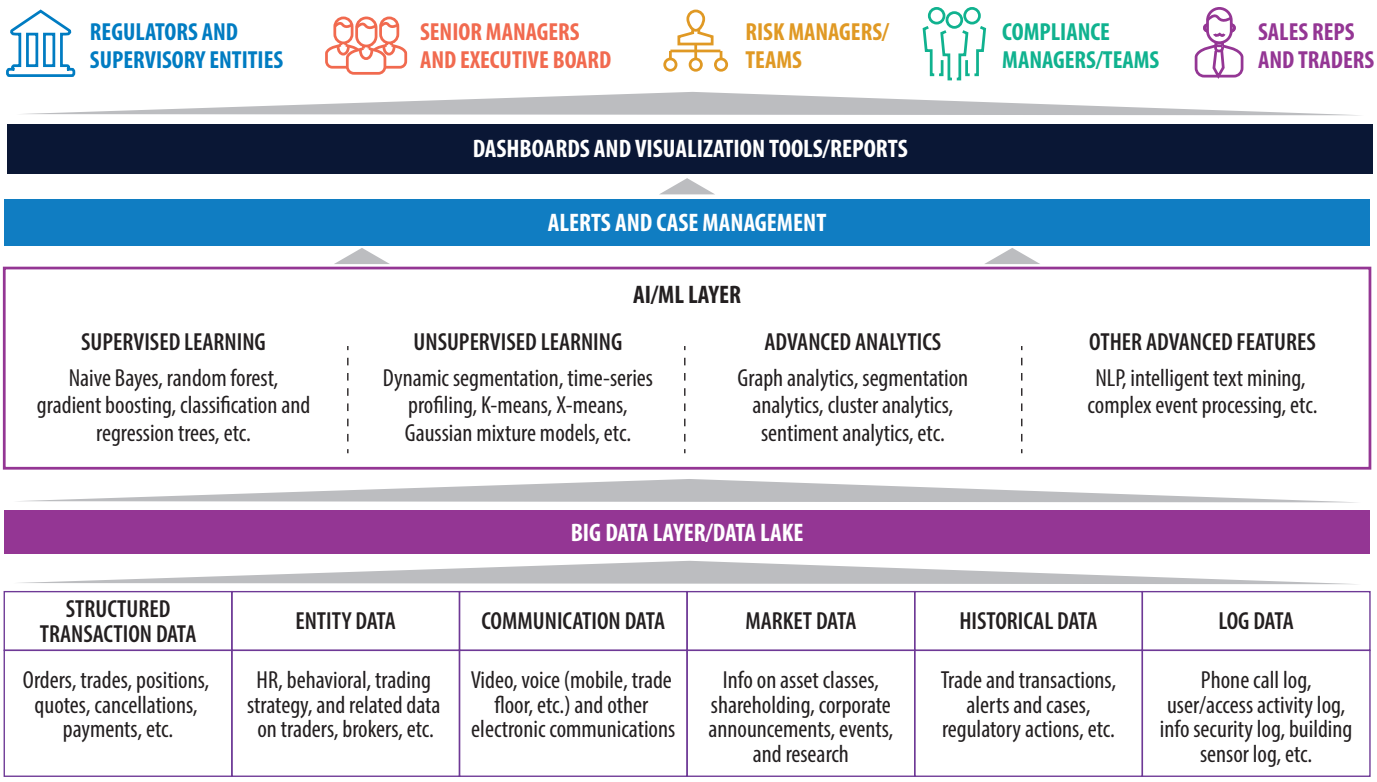
Comprehensive communication surveillance

Surveillance of voice, video, and other electronic communication is essential to identify fraudulent behavior among traders. AI-based tools can contextualize information based on tone, jargon, slang, phrases, and code words to reveal true intent. Based on this surveillance, risk scores are assigned automatically for individual transactions, market players, asset classes, and marketplaces. For example, Nasdaq uses such AI-based systems to identify complex relationships and patterns and detect new types of market manipulations across nearly 60 marketplaces, covering over 160 global participants.[8]

Efficient alert and case management

False positives significantly erode the efficiency of alert investigations. However, AI-based solutions assign risk scores based on several parameters facilitating better prioritization and grouping of incidents. For example, a trade surveillance solution, SURVEIL-X (by NICE Actimize), could reduce false positives by up to 90% through natural language processing (NLP) and other AI capabilities.[9] Similarly, Neurensic

Figure 1: AI-based surveillance architecture



Source: Infosys

(now part of Trading Technologies) has developed a platform "SCORE," which generates an integrity rating for traders based on how their trading patterns match those deemed suspicious by regulators.[10,11] Such tools allow firms to preempt potential market abuse incidents by actively monitoring high-risk market participants. They can also route cases to relevant investigation specialists automatically.

> AI-based monitoring tools can preempt market abuse incidents

Automated compliance procedures

With the ability to read rulebooks automatically, AI-based solutions can enable the effective implementation of new regulations. In the U.K., the FCA and the Bank of England are making their rulebooks machine-readable, with the goal of swifter incorporation of new rules into firms' regulatory intelligence systems.[12]

Such solutions can facilitate the automation of compliance with regulatory orders to provide time-stamped trade histories (trade reconstruction). They can also provide a replay of order placements and cancellations across marketplaces. Advanced solutions can also support the automated submission of suspicious transaction and order report filings, along with supporting data and analysis for supervisory agencies to evaluate incidents. Misselling and aggressive selling by financial advisers and broker-dealers are also a major concern. These solutions can help identify such practices. The FCA is already experimenting with machine learning (ML) techniques that help determine the probability of misselling and aggressive selling to catch miscreants.[13]

Identification of novel manipulations

AI-based solutions can spot behavior that is not readily identifiable as risky or fraudulent. They can flag complex HFT manipulations such as electronic front running[14], rebate arbitrage,[15] and various spoofing activities (which mislead other traders with the placement of large orders absent any intention to execute them). These systems also generate alerts during abnormal spikes in order placements and cancellations. They identify money laundering techniques such as excessive trading with the same counterparties and remote booking (executing trades from a different location than the one where the business is conducted). Some advanced solutions can even ascertain connections between trades and entities across asset classes and marketplaces.

Intuitive reporting and visualization

With billions of transactions and thousands of market players to track, organizations find it increasingly hard to drill down into the important stuff. This is where intuitive, intelligent, and easy-to-use visual interfaces can help. These solutions can produce dashboards and scorecards (e.g., heatmaps and outlier charts) that facilitate easy tracking of metrics such as alert volumes, case statuses, investigation histories, and false positives.

Implementation matters: Four key considerations

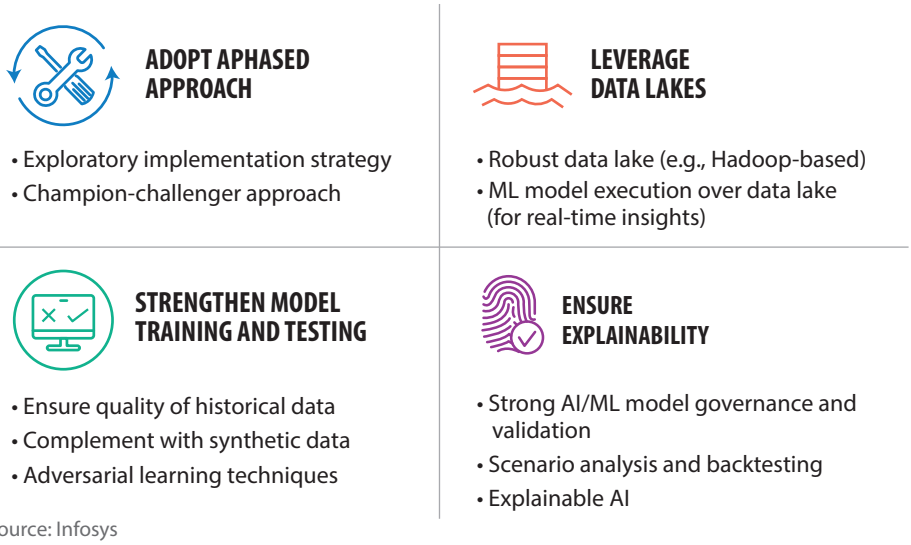
While it is evident that AI-based solutions can boost trade monitoring processes, the implementation process also matters. Hasty or technically fallacious implementation would probably do more harm than existing rule-based systems.

For effective adoption of holistic AI-based solutions, FIs must ensure four key requirements (Figure 2):

1. **Adopt a phased approach:** A champion-challenger approach is ideal while onboarding a new AI-based system. The firm should initially use the solution with existing rule-based systems and utilize learnings from all systems. Once the AI solution starts delivering superior results, existing systems can be phased out.
2. **Leverage data lakes:** A data lake brings disparate data sources together, ensures data integrity, minimizes data loss, and processes a massive variety and volume of data economically. In some instances, AI models can be directly executed over the data lake instead of as a separate layer. This enables the generation of real-time insights.
3. **Strengthen model training and testing:** The accuracy of AI models is dependent on high-quality data, which is typically hard to come by. In some cases, it helps to generate data synthetically using algorithms to overcome the shortage of labeled data. Firms can use fake, malicious inputs to train their AI models on new types of market abuses.
4. **Ensure explainability:** The core problem with most AI-based algorithms is that even the developers creating them often don't know how they arrived at a particular decision. Therefore, firms should adopt explainable AI, which calls for strong model governance practices such as built-in functionality to monitor and evaluate model outputs continuously. They should also conduct rigorous back testing and scenario analyses to further improve and test the accuracy of AI models. This involves training and testing models across different periods of historical data, which ultimately helps define the algorithms' decision-making processes.

> Explainable AI is key to ensuring firms know how exactly a trade is marked suspicious

Figure 2: Four requirements of an enterprise-wide surveillance strategy



Source: Infosys

Responsible AI

Evidently, regulators have become more watchful amidst the rising complexity in financial markets and slack trading behavior of industry participants. Through both warnings and the imposition of fines, regulators are consistently sending out the message that financial misconduct won't be tolerated. For instance, amid COVID-19 restrictions across Europe, the FCA last year reiterated that people with access to insider information should continue to act with integrity.[16]

Thankfully, AI capabilities are growing with time. Industry leaders should make concerted efforts to introduce the technology at scale. Surveillance software has been on the rise since the onset of the pandemic. Technology has already gained sufficient hold in recruiting, managing, and disciplining workers.[17] Therefore, firms must ensure that AI-based systems work as intended, respect privacy, and implement unbiased decision-making.

References

1 Addendum to division of enforcement press release fiscal year 2021, Nov. 18, 2021, U.S. Securities and Exchange Commission.

2 Enforcement reports for FY19, FY20, and FY21, 2019-2021, Financial Conduct Authority.

3 New army of individual investors flexes its muscle, Caitlin McCabe, Dec. 30, 2020, The Wall Street Journal.

4 Volatile markets: Are high-frequency traders to blame?, Feb. 26, 2019, Franklin Templeton.

5 'Red flags' over market abuse rise at asset managers during lockdowns, Katie Martin and Philip Stafford, Feb. 14, 2021, Financial Times.

6 Winning the compliance battle on multiple fronts: tackling market abuse and false positives, Anurag Mohapatra, May 4, 2020, NICE Actimize.

7 Trade surveillance and market abuse: COVID, costs and compliance, Stefan Queck, July 8, 2021, Refinitiv.

8 Nasdaq launches artificial intelligence for surveillance patterns on U.S. stock market, Nov. 7, 2019, GlobeNewswire.

9 NICE Actimize revolutionizes trade-related surveillance with SURVEIL-X, the industry's first AI-powered, cloud-native, true holistic solution, Sept. 18, 2019, NICE Actimize.

10 Neurensic releases SCORE, the trading industry's first cloud-based, AI-powered surveillance solution, Oct. 19, 2016, Business Wire.

11 Trading Technologies acquires Chicago AI firm Neurensic, John McCrank, Oct. 10, 2017, Reuters.

12 FINRA requests comment on financial technology innovation in the broker-dealer industry, July 30, 2018, FINRA.

13 Innovative technology in financial supervision (suptech) – the experience of early users, Dirk Broeders and Jermy Prenio, July 2018, Financial Stability Institute.

14 Electronic front-running involves buying securities across exchanges, just beating a large buy order, to sell them to that very buyer at a higher price and pocketing the difference.

15 Rebate arbitrage involves benefiting from the cost advantages offered by exchanges for creating liquidity in the market without actually creating liquidity.

16 'Red flags' over market abuse rise at asset managers during lockdowns.

17 Growth of staff monitoring software stokes debate over rights and morals, Andrew Jack, Sept. 22, 2021, Financial Times.

Authors

Anjani Kumar

Principal Consultant, Global Risk, Regulatory Tech, and Computational Finance Practices, Financial Services Domain Consulting Group, Infosys Limited

Jitesh Gera

Infosys Knowledge Institute

Harry Keir Hughes

Infosys Knowledge Institute

About Infosys Knowledge Institute

The Infosys Knowledge Institute helps industry leaders develop a deeper understanding of business and technology trends through compelling thought leadership. Our researchers and subject matter experts provide a fact base that aids decision making on critical business and technology issues.
To view our research, visit Infosys Knowledge Institute at infosys.com/IKI

For more information, contact askus@infosys.com

Infosys®
Navigate your next