shield. RT ASSOCIATES

Surveillance in the Age of AI

INTRODUCTION

In today's increasingly interconnected world, surveillance has become a critical aspect of maintaining market integrity through the detection and prevention of illicit trading behaviour[1] [2]. The introduction of artificial intelligence (AI) technologies has accelerated the pace of change in virtually every industry, and financial services are no exception. This rapid technological evolution has had far-reaching implications for how firms approach surveillance and market abuse detection.

Market abuse is a broad term that encompasses a variety of illegal activities that seek to exploit financial markets for personal gain, ultimately undermining their integrity. Market manipulation, for example, refers to the act of artificially influencing the price or volume of a financial instrument to create a false or misleading appearance of market activity. Insider trading, on the other hand, occurs when individuals use non-public information to make trading decisions, thus gaining an unfair advantage over other market participants.

[1] https://www.shieldfc.com/regulations

[2] Enhancing market integrity | FCA

The detection and prevention of these illicit activities are crucial to maintaining the trust and confidence of investors and other stakeholders in the financial markets. To this end, firms have increasingly turned to trade and electronic communications (eComms) surveillance to identify suspicious activities that may signal potential market abuse.

> **By monitoring and analysing trading data and electronic communications, firms can detect irregular patterns and activities that warrant further investigation.**

The emergence of AI technologies has brought about a significant shift in the capabilities of surveillance systems, transforming the way that firms think about surveillance[3], and raising the bar for what is expected of these systems. AI presents both enormous opportunities and significant challenges for firms. On one hand, the advancements in AI technology enable firms to vastly improve their ability to detect market abuse, providing them with more effective tools to safeguard market integrity.

On the other hand, the rapid pace at which AI has risen to the forefront of technology presents a host of technical, operational, regulatory, and competitive challenges that firms must navigate to remain compliant and competitive.

To explore these opportunities and challenges, RegTech Associates recently hosted a roundtable discussion in partnership with Shield: Surveillance in The Age of AI. This report builds upon the key themes that emerged during the conversation, which involved more than 20 leaders in market surveillance from major financial institutions. By examining the experiences and perspectives of industry experts, this report aims to shed light on the current state of AI in surveillance and chart a path forward for firms seeking to harness the power of this transformative technology.

[3] https://aimagazine.com/articles/machine-learning-critical-for-trade-surveillance-say-banks

THE CURRENT STATE: AN UNCOMFORTABLE EQUILIBRIUM

INCUMBENT SURVEILLANCE SYSTEMS: WHERE ARE WE AND HOW DID WE GET HERE?

Market abuse is an age-old problem that regulatory authorities have been striving to combat for nearly a century. In the United States, the Securities Act of 1933 and the Securities Exchange Act of 1934[4] laid the foundation for market abuse prevention by introducing the first measures to address this issue. Since then, firms have been required to implement surveillance systems and related controls to detect and prevent market abuse from occurring. In the US, the Dodd-Frank Act[5] requires firms to capture, monitor and store trade and communications data, while in the EU and the UK, the Market Abuse Regulation (MAR)[6] and the Markets in Financial Instruments Directive II (MiFID II)[7] provide the necessary regulatory framework for governing surveillance.

Surveillance systems, therefore, evolved in an environment that was technologically primitive by today's standards. Lacking sophisticated technology, it was nearly impossible for firms to effectively detect market abuse amidst the scale and complexity of financial markets.

Consequently, the primary focus of firms was to meet regulatory standards in the most efficient and cost-effective manner possible, rather than actively pursuing optimal market abuse detection.

[4] https://www.investor.gov/introduction-investing/investing-basics/role-sec/laws-govern-securities-industry

[5] https://www.cftc.gov/LawRegulation/DoddFrankAct/index.htm

[6] https://www.fca.org.uk/markets/market-abuse/regulation

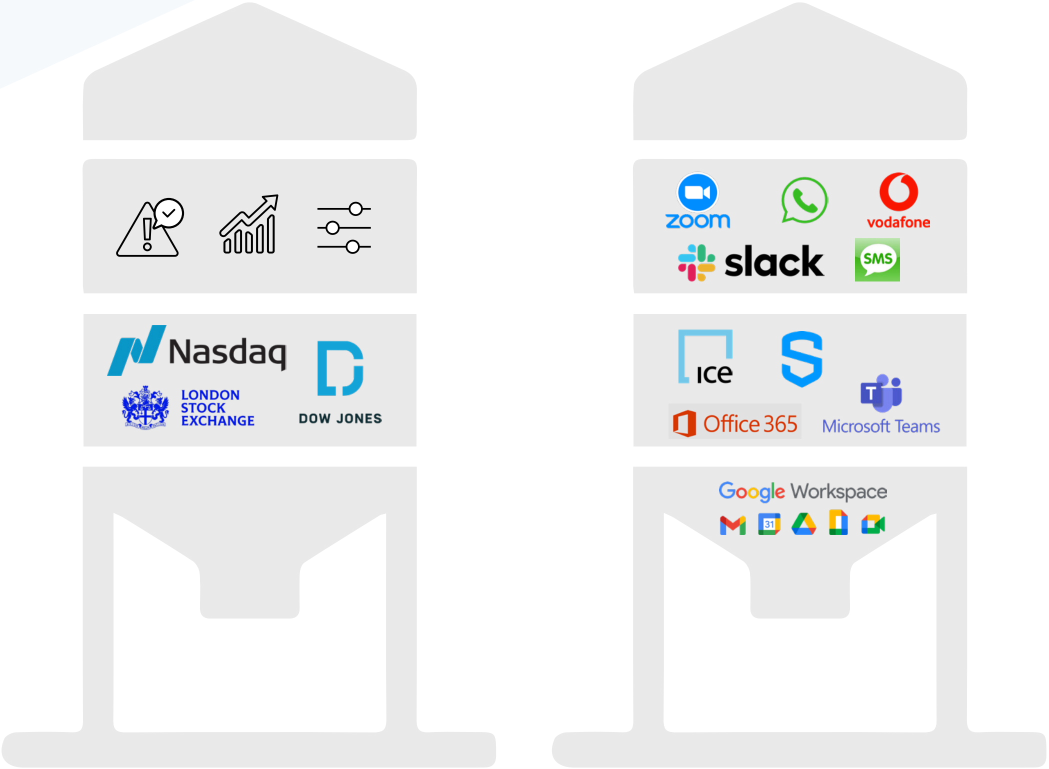
[7] https://www.esma.europa.eu/publications-and-data/interactive-single-rulebook/mifid-ii

Today, the sheer scale and complexity of major financial institutions makes replacing or upgrading those systems and controls a cumbersome and delicate process. As a result, firms remain weighed down by operational and regulatory challenges surrounding their current surveillance systems, with their resources often consumed by governance risk rather than actively tackling market abuse.

Given this context, it comes as no surprise that firms are far from achieving their maximum potential in market abuse detection. The current state of surveillance systems reveals several areas in which firms are struggling. One of the most basic, yet crucial, aspects that many organisations overlook is tracking false positives. For some firms, this is due to the large volume of false positives produced by their current technology. Meanwhile, others find it challenging to establish a practical definition of a false positive which can be operationalised and monitored. The lack of progress surrounding this essential metric highlights the fact that firms have not internally addressed the questions of effectiveness or efficiency in relation to their surveillance systems' ability to detect and prevent market abuse.

Firms also face difficulties in connecting key data sources, limiting the context around any given datapoint. Currently, trade and eComms surveillance are often treated as separate, siloed systems, which limits the effectiveness and adaptability of the overall surveillance strategy.

This separation may be partially attributed to the broader struggles firms face in effectively utilising unstructured data. Right now, unstructured data types, such as various forms of text data, are causing a disproportionate number of false positives. Whilst this is known, it is difficult to solve with slow and disjointed feedback loops between analysts and tech teams, armed with outdated technology. Unless firms can overcome this challenge, attempts to integrate systems containing unstructured data may fail to provide the desired context-enhancing benefits. Firms seeking help from technology vendors have seen progress but have been met with a landscape that is predominantly divided into either trade or eComms surveillance, limiting their access to the full context of customer behaviour. On the flip side, where comprehensive solutions are available, firms grapple with the risks of vulnerability and dependency associated with outsourcing surveillance technology to a single supplier.



REGULATORY PRESSURE: MAKING TODAY'S STATE UNSUSTAINABLE

Market abuse is challenging from a regulatory perspective. Research on regulatory enforcements indicates that it is both widespread[8] and difficult to prove[9]. This has resulted in an uncomfortable, sub-optimal equilibrium where neither regulators nor market participants are satisfied, and illicit activities persist. However, regulators are taking steps to enhance their ability to detect and substantiate market abuse.

ENFORCEMENTS

From trends in market abuse enforcements, we can see a focus in 2022 on systems and controls failures. While these infractions may generally incur smaller penalties than more extensive market abuse violations, eradicating them is crucial, as they contribute to the opacity of firms' activities and consequently hinder regulators' ability to prove more significant cases.

TECHNOLOGY

In recent years, regulators have also invested heavily in trade surveillance data analytics capabilities to better identify market abuse. For example, ASIC's Market Analysis and Intelligence (MAI) Platform is an online system developed to provide market participants with access to ASIC's market surveillance data and analysis tools. Similarly, BaFIN's Automated Alarm and Monitoring System (ALMA) is a surveillance system designed to monitor and detect potential violations of financial regulations in real-time, flagging suspicious transactions and behaviour patterns that may indicate market abuse. Whilst the SEC's ATLAS initiative, launched in 2019, uses advanced data analytics and machine learning techniques to detect potential insider trading, market manipulation, and other fraudulent activities in the securities markets. These initiatives, along with the overarching progress in AI, are prompting regulators to raise their expectations regarding market participants' adoption and use of surveillance technologies and AI capabilities.

[8] https://radar.rtassociates.co/insight/388

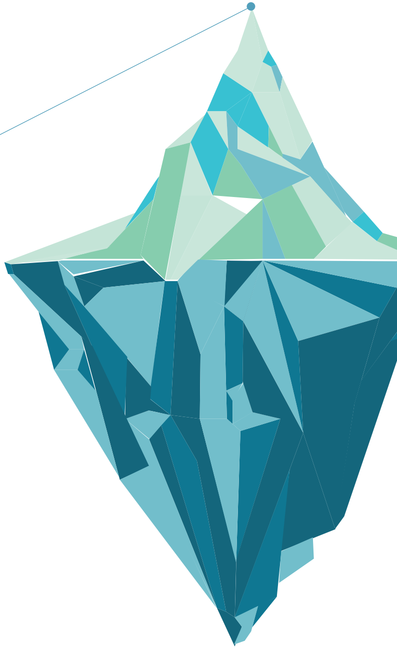
[9] https://radar.rtassociates.co/insight/391

ARTIFICIAL INTELLIGENCE: BECOMING EFFECTIVE

A TECHNOLOGICAL STEP CHANGE

Over the past 12 months, AI has made tremendous strides in effectiveness, transforming once-maligned applications, such as chatbots, into indispensable productivity assistants and subject matter “experts” for millions of users worldwide. The successful launch of products like ChatGPT has garnered significant attention, leading to governmental and corporate scrutiny over whether the system’s security measures match its impressive text generation capabilities.

Many industry experts argue that ChatGPT is just the tip of the iceberg[10], as AI technologies across various domains have experienced remarkable improvements[11] - from image[12] and video[13] generators to generalist AI agents[14]. Importantly, hardware such as AI-specialised microchips, which will allow computationally heavy models to scale, have also taken large leaps forward in power[15] and manufacturing efficiency[16]. These advancements have far-reaching implications that extend to virtually all industries and economies.



[10] https://www.uni-hamburg.de/en/newsroom/im-fokus/2023/0302-chatgpt-ew.html

[11] https://www.freethink.com/robots-ai/ai-breakthroughs

[12] https://www.sciencefocus.com/future-technology/dall-e-2-why-the-ai-image-generator-is-a-revolutionary-invention/

[13] https://arxiv.org/pdf/2302.01329.pdf

[14] https://www.deepmind.com/publications/a-generalist-agent

[15] https://www.cnet.com/tech/computing/meet-nvidias-huge-h100-chip-thats-powering-tomorrows-ai/

[16] https://techhq.com/2023/03/nvidia-claims-breakthrough-in-chip-manufacturing-for-2nm-and-beyond/

Industries with long histories and major incumbents may have the most ground to make up with respect to AI. But this also means that they have the most to gain. The global AI FinTech market, for example, is forecast to experience a massive 41.2% compound annual growth rate from its size in 2020 through to 2026[17]. As more firms and regulatory bodies embrace AI, the expectation for companies to integrate AI into their surveillance systems is rapidly becoming the norm. This technological step change is reshaping the landscape of market surveillance, pushing firms to adapt and innovate to meet the rising standards of market integrity and regulatory compliance.

THE OPPORTUNITY IN SURVEILLANCE

Major financial institutions are currently in one of two distinct stages: some are rapidly integrating AI into their surveillance systems, whilst others are diligently preparing for its eventual implementation. This is driven by a range of significant incentives for those that effectively harness AI technology.

ENHANCED PATTERN RECOGNITION

Market abuse often follows specific patterns, and AI/Machine Learning (ML) models excel in complex pattern recognition. These models have long been used for numerical pattern recognition, but can now be paired with Natural Language Processing (NLP) techniques that are so effective in semantic comprehension that they beat humans on a range of human-centric tasks[18].

[17] https://www.marketdataforecast.com/market-reports/ai-in-fintech-market

[18] https://openai.com/research/gpt-4

By incorporating AI for enhanced pattern recognition and contextual understanding, surveillance systems can more accurately flag relevant information for review and reduce the number of irrelevant cases, thereby improving the balance of true and false positives.

This streamlined process results in a more efficient and enjoyable analyst experience, as they spend less time investigating innocuous cases. This efficiency also leads to cost savings, as a smaller team can effectively manage the high-quality alerts generated by the AI-driven surveillance system.

A more dynamic system that accounts for numerous variables and their interrelations can also be expected to be more resilient to new risks than a traditional system with a limited number of predefined rules. More effective detection and prevention of market abuse over time also reduces other costs, such as regulatory fines and reputational damage.

AGGREGATING CHANNELS

AI can process and establish rules around more variables and their interrelations than traditional systems. It can also connect the dots across different channels and data types. Complex NLP models transform text into large matrices of numbers, highly representative of underlying meaning. This allows for a common language across trade and eComms surveillance, enabling AI to tell a more complete story about a trade and increasing the effectiveness of efforts to detect and prevent market abuse.

TECHNOLOGY VENDORS

Though recent breakthroughs in AI have drawn mainstream attention to these emerging technologies, technology vendors have been developing AI solutions for a number of years. Certain tech vendors specialise in AI for trade and eComms surveillance, helping firms stay ahead of the curve. Staying ahead entails more than implementing out-of-the-box solutions - it also means understanding them at a technical, regulatory and commercial level in order to garner the support of all relevant stakeholders.

THE CHALLENGE OF INNOVATION

ADOPTING A NEW OPERATING MODEL

Embracing AI in market surveillance means adopting a new operating model, which requires significant investment, new skill sets, and extensive collaboration across various areas of the business. AI systems necessitate entirely different processes compared to traditional rules-based systems. This includes risk assessments, data collection and training, implementation, maintenance (including retraining), monitoring, and documentation. These changes affect the way firms run their monitoring and surveillance activities from top to bottom.

EXPLAINABILITY: AI AS A BLACK BOX

One of the challenges in adopting AI technology is its perceived “black box” nature. This can create difficulties in gaining internal support for AI adoption, as stakeholders may require a deeper understanding of the technology before approving budgets. Externally, firms may need to demonstrate compliance to regulators who may harbour concerns about the technology’s transparency and effectiveness.

RESOURCES

Adopting AI technology also demands a range of resources, including skilled personnel, underlying technology infrastructure, and data. Among many other intricacies, these resources are necessary for:

- **Building the AI system (if developed internally)**
- **Supporting implementation**
- **Training and retraining staff**
- **Maintaining the system**
- **Monitoring alerts**
- **Assessing performance**

The competition for skilled professionals in AI can drive up costs, as large tech firms offer attractive packages to attract top talent. Moreover, the true extent of market abuse may be better or worse than what current monitoring alerts indicate, making it uncertain whether AI, by improving the balance of true and false positives, will ultimately increase or decrease the total number of alerts. With a wide array of such considerations, there is a general uncertainty regarding the full cost of innovation, as firms navigate the complexities of integrating AI into their surveillance operations.

CONCLUSION: AI IS INEVITABLE

Under the right circumstances, firms would be keen to implement AI in their surveillance systems imminently. Beyond the excitement and fears associated with AI lies the need for a practical, pragmatic, and safe approach to adopting this transformative technology.

- **Gradual Implementation:** Just because technology has experienced a step change does not mean its implementation must follow the same pace. Firms can adopt AI gradually to ensure a smooth transition and minimise disruptions.
- **Avoiding Scope Creep:** Being clear on the project's boundaries from the beginning helps maintain focus and avoid unexpected expansion of the project's scope.
- **Parallel Systems:** Running AI models alongside traditional rules-based models can provide valuable insights and comparisons, allowing firms to optimise their surveillance systems over time.
- **Small Sample Testing:** Initially deploying AI models on a small sample of cases helps organisations gain confidence in the technology and identify any areas that may require further refinement.

Our recent roundtable discussions highlighted the inevitability of AI in trade and eComms surveillance as a key takeaway. The questions of where AI can be most effective are becoming increasingly clear, thanks to highly capable and dynamic AI models. This clarity is driving firms to shorten their timelines for implementation. What remains, and what we aim to address in collaboration with the industry, is the question of "how?" We have much more to share on this topic, so keep an eye out for our upcoming pieces on what it takes to successfully implement industry-defining AI in market surveillance.

About RegTech Associates

RegTech Associates is a research company using its analysis to provide strategic insight and advice to RegTech vendors, regulated institutions and global industry bodies. We bring all sides of the market together to help vendors grow and regulated firms manage compliance more effectively. Founded in 2017, RegTech Associates is a privately held company based in London. Our experienced team has extensive industry and regulatory knowledge and often collaborates with leading regulators to foster dialogue and industry collaborations. RegTech Associates are also the creators of Radar, the go-to platform for professionals working in legal, risk, or compliance. Our digital platform houses thousands of data points for over 1,500 products, an enriched and researched-backed insights library, and a curated industry news feed.

e. info@rtassociates.co | w. www.rtassociates.co @rt_associates | l. /regtechassociates

About Shield

Shield enables compliance teams in financial services and other highly regulated industries to read between the lines to see what their employee communications are really saying. Many of these organizations struggle with compliance because they are unable to gain visibility into the mass of scattered data across all of their communication channels to mitigate against market abuse, internal bad actors and increasing regulatory risk. By applying advanced AI, NLP, and visualization capabilities, Shield is enabling enterprises and financial institutions to more effectively manage and mitigate communications compliance risks. Shield has helped customers from UBS to FIS to reduce false positive alerts by 97%, conduct faster investigations, and reduce compliance costs. Learn more at **shieldfc.com**.

shield. RT ASSOCIATES