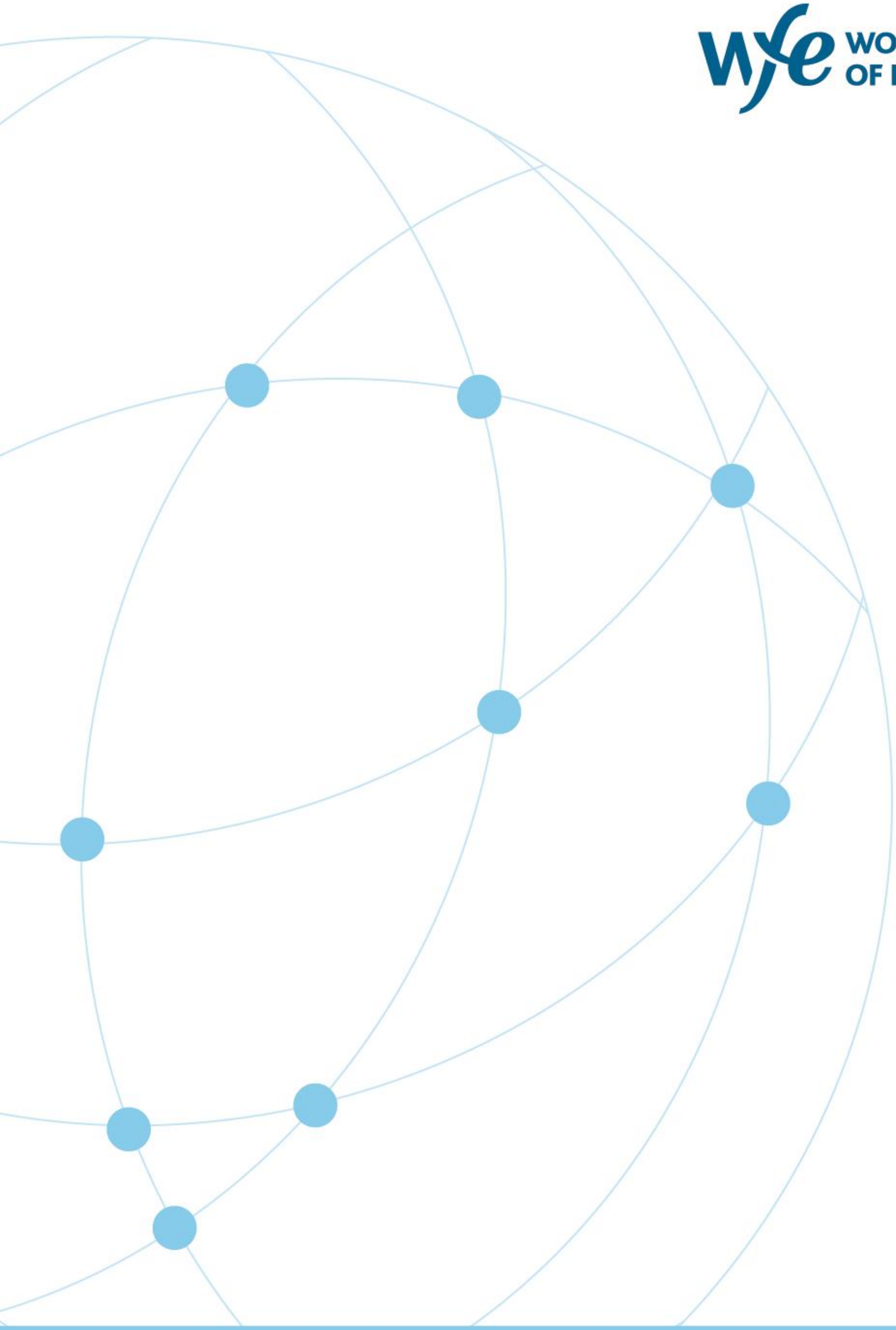

WFE Response to Request for Comment on the Use of Artificial Intelligence in CFTC-Regulated Markets

24 April 2024

Background

Established in 1961, the WFE is the global industry association for exchanges and clearing houses. Headquartered in London, it represents the providers of over 250 pieces of market infrastructure, including standalone CCPs that are not part of exchange groups. Of our members, 36% are in Asia-Pacific, 43% in EMEA and 21% in the Americas. The WFE's 87 member CCPs and clearing services collectively ensure that risk takers post some $1.3 trillion (equivalent) of resources to back their positions, in the form of initial margin and default fund requirements. The exchanges covered by WFE data are home to over 55,000 listed companies, and the market capitalization of these entities is over $111tr; around $124tr in trading annually passes through WFE members (at end-2023).

The WFE is the definitive source for exchange-traded statistics and publishes over 350 market data indicators. Its free statistics database stretches back more than 40 years and provides information and insight into developments on global exchanges. The WFE works with standard-setters, policy makers, regulators and government organisations around the world to support and promote the development of fair, transparent, stable and efficient markets. The WFE shares regulatory authorities' goals of ensuring the safety and soundness of the global financial system.

With extensive experience of developing and enforcing high standards of conduct, the WFE and its members support an orderly, secure, fair and transparent environment for investors; for companies that raise capital; and for all who deal with financial risk. We seek outcomes that maximise the common good, consumer confidence and economic growth. And we engage with policy makers and regulators in an open, collaborative way, reflecting the central, public role that exchanges and CCPs play in a globally integrated financial system.

If you have any further questions, or wish to follow-up on our contribution, the WFE remains at your disposal. Please contact:

James Auliffe, Manager, Regulatory Affairs: jauliffe@world-exchanges.org

Nicolas Höck, Junior Analyst: junior.analyst@world-exchanges.org

Richard Metcalfe, Head of Regulatory Affairs: rmetcalfe@world-exchanges.org

Or Nandini Sukumar, Chief Executive Officer: nsukumar@world-exchanges.org.

Summary

- AI is not new. It has existed for approximately eighty years and has been used in financial services for decades. Gen AI is just the most recent form of AI.
- The WFE is encouraged to see the CFTC taking a careful, considered approach to understanding the benefits, risks, and uses of AI within the financial services sector.
- AI has a significant number of potential use cases that could bring efficiency gains, lower costs, increase productivity, generate revenues, and benefit the market as a whole.
- Our members generally see AI use cases in three broad categories:
  - 1) individual productivity, 2) operational efficiency and 3) new products.
- The use of AI has also created specific risks that financial institutions must address. However, financial institutions and authorities must be clear on those specific risks and develop mitigation strategies to address these risks where possible.
- The risk mitigation of AI in financial services is currently being executed through existing risk management frameworks. However, our members are further developing or using governance frameworks, training programmes, risk management protocols etc. around the use of AI.

Introduction

Artificial Intelligence (AI) encompasses a broad range of technologies and techniques that allow machines to perform tasks that typically require human intelligence, such as visual perception, speech recognition, decision-making, and language translation. Executive Order 14110: The Safe Secure and Trustworthy Development defines AI as: '*A machine-based system that can, for a given set of human defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments, abstracts such perceptions into models through analysis in an automated manner and use model inference to formulate options for information or action.*'[1]

AI is another step in the evolution of automation. Automation involves employing technology to execute repetitive tasks with minimal human intervention. With AI, financial institutions are learning to automate tasks that create efficiencies and generate positive outcomes.

The World Federation of Exchanges (WFE) is encouraged to see the CFTC taking a careful and considered approach to understand the benefits, risks, and uses of AI within the financial services sector.

Machine Learning vs. Generative AI

AI is already used in financial services and has been used for at least twenty years. Financial institutions have been using machine learning (ML), a subset of AI that focuses on the development of algorithms and statistical models that enable computers to perform tasks, for a long time. The consultation differentiates between AI and algorithmic trading however, based on the definition of AI in the Executive Order 14110, algorithmic trading is AI. These algorithms execute trades based on predefined rules, strategies, and parameters.

[1] Executive Order 14110: The Safe Secure and Trustworthy Development and Use of Artificial Intelligence (2023) @ pg 4 can be found at: https://www.govinfo.gov/content/pkg/FR-2023-11-01/pdf/2023-24283.pdf

In contrast to traditional AI or ML technologies that focus on classification or prediction, generative AI has the ability to create new content. Large language models (LLMs), like OpenAI's Chat GPT, are the most well-known subset of generative AI. In this example of generative AI, Chat GPT identifies patterns in words and phrases and predicts the word(s) most likely to follow. These predictions are generated from large data sets with numerous computational layers that have been trained on user inputs which gives the appearance of genuine creativity or thought.

It is worth noting that with every innovation there comes a cycle of hype, fear and eventually productivity. Gartner's Hype Cycle is a graphical representation of this well-known phenomenon.[2] According to Gartner, as the technology gains attention, expectations around its potential benefits contribute to the hype which leads to inflated expectations. Reality settles in when the shortcomings or limitations become apparent. Valuable lessons are learned, and finally the technology reaches a level of maturity where it becomes widely adopted and productive. In 2023, Gartner concluded that Generative AI was at the peak of its inflated expectations.[3] Therefore, whilst it is certainly true that Generative AI could have a transformative impact, it is useful to know that it is likely to be less than that which is expected right now.

AI Benefits for Financial Institutions

Like other industries, financial institutions and exchanges have been incorporating AI into their operations for various purposes, and this trend is likely to continue. The risk mitigation of AI in the financial services sector is being executed through existing risk management frameworks. Financial institutions invest in testing, validation, and ongoing monitoring of AI models to ensure their accuracy and reliability.

AI brings valuable contributions in various ways. First, it can identify intricate patterns within data that humans might overlook, aiding in accurately identifying and mimicking behaviours more accurately. Second, AI's ability to handle repetitive tasks can outpace human capabilities, boosting overall efficiency. Furthermore, AI systems ensure consistent task performance without succumbing to fatigue or distractions ensuring reliable results over time. Additionally, AI's ability to manage large datasets without demanding excessive resources highlights its scalability and resourcefulness, further enriching its value.

AI has the potential to reduce costs, generate efficiencies and possibly create new products which could be beneficial to the wider market and the real economy. Our members generally see AI use cases in three broad categories:

1. Individual productivity – tools designed to improve the output of individual employees. Examples could include using generative AI to help develop code, virtual assistants to help staff or automated data entry.
2. Operational efficiency – tools designed to improve the efficiency of the overall operation of exchanges and CCPs. Examples include predictive tools to identify hardware that requires maintenance, automation of repetitive processes or fraud detection and prevention.

[2] https://www.gartner.co.uk/en/methodologies/gartner-hype-cycle

[3] https://www.gartner.com/en/articles/what-s-new-in-the-2023-gartner-hype-cycle-for-emerging-technologies

3. New product developments – these would be products and services that an exchange or CCP could offer to market participants or the broader market. Examples could include market data offerings and regulatory compliance solutions.

Use Cases for AI on Exchanges and CCPs

AI can be used to detect market manipulation, fraud and other nefarious activity on exchanges. By analysing vast datasets, AI models can detect anomalies, flag suspicious activities, and provide SROs and regulators with timely insights to investigate and mitigate potential market abuse. Continuous refinement and augmentation of these AI-based tools could enhance their ability to adapt to evolving market dynamics, contributing to more effective and proactive market supervision, ultimately safeguarding market integrity and investor confidence.

AI can be most valuable in executing tasks that are time-consuming. This could include a number of the possible use cases identified in the request for comment, such as:

- Managing risk – AI can be used to help identify risk, including by analysing historical data.
- Compliance – AI can be used to reduce manual inputs for trade documentation and regulatory reporting, as well as reducing market manipulation as explained above.
- Cyber Security – AI can help improve both phishing tests aimed at employees to raise awareness as well as detection of phishing mails (e.g by making use of Generative Adversarial Networks (GANs).
- Books and records - AI is being used to search records. Standard third-party software providers like Apple or Microsoft include search tools that seek to predict what you are looking for before you find it.

In a regulated world, Chat Bots, for example, could be particularly helpful to answer questions where the answer is split over several different documents. An institution using an exchange or CCP may have to consult primary legislation, regulatory rulebooks, the exchange/CCP rulebook and guidance from industry or the regulator when considering how to act. Despite best efforts, these references are not always easy to find or intuitive. Therefore, a Chat Bot that could be asked to identify and pull out the relevant references in all rulebooks and guidance applicable to the institution in question could be potentially very helpful.

Cybersecurity and AI

AI will be an asset for both cyber professionals and nefarious cyber threat actors. AI is currently being used by cyber professionals primarily through their use of cyber vendors. AI/ML is used by advanced intrusion detection systems to not only detect known malicious activity but also to identify variants of this activity and disrupt these attacks.

Similarly, AI is used by network monitoring tools to identify changes in network traffic behaviour that may, for example, signal an intrusion looking for new hosts. Given that numerous malware strains attempt to do similar actions to gain access to the underlying operating system and the growing number of clients using advanced intrusion detection systems, the ability of these vendors to provide holistic protection across its customer base is greatly benefited by AI technology and the financial institutions that utilize them.

Risks Related to AI

While AI brings numerous benefits to financial services, the industry is cognizant of the importance of managing potential risks and ensuring that AI applications align with ethical and regulatory standards. This approach helps to mitigate risks and establishes a foundation for the responsible use of AI in the financial sector.

Exchanges and CCPs are already incentivised to have the strongest possible risk management because any failures that occur will likely be public, which can harm their reputation. Exchanges and CCPs are valued because they are trusted parties, and reputational risks are of deep concern. Of course, exchanges, CCPs and indeed all financial services firms are regulated too. Due to these potential impacts, financial institutions and exchanges are heavily regulated for their risk and resilience management and financial authorities create principles[4] that are used to guide comprehensive risk management frameworks.

Bias

AI systems can perpetuate biases present in the data on which they are trained or give erroneous results due to data quality or data context issues. Further, AI systems can present latent risks. Without proper controls, AI systems can amplify, perpetuate, or exacerbate inequitable or undesirable outcomes for individuals or communities. A very specific risk to AI is drift where a model's performance deteriorates over time due to changes in the underlying data or environment it was trained to predict or interpret. With proper controls, AI systems can mitigate and manage inequitable outcomes. This bias when combined with a misunderstanding of the AI system context could lead to unintended biases to the AI system output. Lastly, bias risk may be latent at a given point in time and may increase as the AI system adapts and evolves. These biases could be the result of incomplete training data or significant and unexpected data changes.

Explainability and Transparency

When using models, AI or otherwise, financial institutions must be able to provide transparency and explainability for the model outputs. However, for models that are provided by a third party, the ability to provide the required transparency and explainability could be challenging. Data quality and data context are highly important for the success of any model. The failure of either of these elements may cause the model to behave in an unexpected or unanticipated manner. Context matters. The inability to understand the data context may cause the user to believe that the results of the model can be used in all contexts. Therefore, financial institutions must have the ability to understand how data quality is being maintained and the context for which the AI model can be used. Lastly, the use of a third party for the model and computational power can be further complicated if the third party claims that the model is proprietary or is the third party’s intellectual property. These claims could prevent financial institutions from obtaining the transparency needed to explain the model’s results.

However, most AI models are based on a set of predefined rules so they are highly transparent and interpretable. These older, more classical machine learning models use decision trees, linear

[4] The CPMI-IOSCO Principles For Financial Market infrastructures (2012) set risk and resilience management principles for market infrastructures. These Principles can be found at: https://www.bis.org/cpmi/publ/d101a.pdf

regression and support vector machines that are more interpretable than complex deep learning models.

Concentration

As stated earlier, AI systems may require large computational power with large data sets to produce expected and accurate results. The ability to provide the computational power necessary for complex models may reside with a handful of large technology companies which may drive further concentration and interconnectedness with these providers. Since the AI model marketplace has not fully matured, it is not clear if this risk will materialize.

Cybersecurity

While AI will be used to provide enhanced protections to financial institutions, this technology will also be used by threat actors. The financial services industry has already witnessed how deep fakes can be used to trick unwitting employees to erroneously send payments.[5] In addition, generative AI and LLMs allow for better phishing emails to increase the impact and success of these attacks. Meanwhile, phishing attacks continue to be a primary method for threat actors to gain initial access to a financial institution's systems. Cyber professionals continue to explore different ways that can be used to enhance their protections using AI tools and threat actors will continue to explore how to develop new attack vectors by enabling this technology.

Risk Management of AI

Financial institutions currently are using existing risk management frameworks to manage AI risks. Risk management techniques, such as those involved in identifying risk or analysing the extent of a risk, remain relevant to managing AI risks.

These risks in many ways are similar to risks exchanges, CCPs and the broader financial services industry are already accustomed to managing. For example, discrimination and bias in decision-making by humans are longstanding risks across all business sectors. Due to its capabilities, AI can amplify these risks if the training data is biased or the opacity of the AI system prevents explainability and accountability.

Our members are actively taking steps to manage the risks associated with AI. Exchanges and CCPs are developing or using governance frameworks, training programmes, and risk management protocols to manage and mitigate risk.

Emerging standards, such as NIST's AI Risk Management Framework,[6] have recently been introduced to provide pillars for the comprehensive management of AI risks. Currently, the NIST AI Risk Management Framework provides a framework to manage risks identified through the AI development process. However, this and other frameworks do not provide any detail on 'how' to identify potential risks to AI models. This framework will evolve with this information over time to be a critical piece in the consistent application of AI risk management.

[5] In 2024, a deep fake AI video conference was used to trick an employee send an improper payment. More about the incident can be found at: https://www.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html

[6] https://www.nist.gov/itl/ai-risk-management-framework

The following is a non-exhaustive list of the techniques our members use:

- Firms maintain detailed documentation of AI applications including the purpose, function, data sources and intended outcomes.
- Governance frameworks define roles and responsibilities, decision-making processes and accountability for AI applications.
- Training programmes are implemented to educate employees about AI systems, which helps employees understand the importance of responsible AI practices and the limitations of the current technology.

Our members understand the importance of the principle of a "human in the loop," where human oversight, intervention, or decision-making is incorporated into an AI system's workflow. AI currently informs or complements human action, it does not replace it. This is one of the key elements of risk mitigation that firms currently operate. Theoretically, it is possible that an AI could reach capabilities greater than human beings, but not currently. Therefore, for the foreseeable future, all AI will inform rather than supplant human action.

Our members consider their journey's towards becoming more reliant on AI as a multi-year effort that requires slow, careful and methodical consideration. Pursuing targeted projects focused on individual productivity as their first target allows them to develop AI tools in a relatively low stakes environment before taking those lessons learned to develop higher risk tools.

Third Parties and AI

Third parties in the area of AI are typically subject to vendor risk management. Depending upon what sort of tool they offer, they may be subject to enhanced vendor risk management. Where third parties are involved, exchanges and CCPs conduct due diligence including assessing the provider's reputation, regulatory compliance, security measures and transparency of their AI techniques. Firms monitor their third-parties through vendor management processes to ensure continued compliance and risk mitigation. The involvement of a third-party does not necessarily imply a loss of control over the activity by the regulated firm. This underscores the importance of implementing robust third-party risk management protocols.

Third-party involvement can play a pivotal role in expanding the reach of AI technologies within financial markets. It is likely that technology companies will develop AI tools that have a general level of applicability across the whole economy, as we have seen in the past or can see with LLMs now. These tools can then be tailored to the regulated environment in financial services.

The AI tools developed with a more general level of applicability by technology firms may benefit from being exposed to various sectors of the economy. The potential for AI to create large economies of scale is not much different from the potential of any technological advancements to create economies of scale. This may be done with third parties that specialise in technology and AI, working with other industries to deliver large economies of scale and significant expertise.

Regulators are correct to be cognisant of the risks of AI to competition and market concentration; however, these are not new risks or specific to AI. Market concentration can contribute positively to economic growth and industry development when it facilitates efficiency gains and innovation. This is an area where we encourage regulators to monitor for negative outcomes but not one that we consider requires regulatory action.

Barriers to AI

Our members are experiencing a number of the more generic barriers. AI solutions are very costly and require sufficient skilled workers. The projects often involve high sunk costs without guarantee of success. This is another one of the reasons that our members are approaching the development of AI cautiously and focusing on individual productivity gains first.

Regulations that are written on a principle's basis can be equally applied to AI use. For example, the System Safeguard rules (17 CFR 39.18 and 17 CFR 38.1050) would have straight forward applicability. These generally require DCOs and DCMs to "Establish and maintain a program of risk analysis and oversight to identify and minimize sources of operational risk, through the development of appropriate controls and procedures, and the development of automated systems, that are reliable, secure, and have adequate scalable capacity." This includes rigor around enterprise risk management/governance, information security, operations, systems development and quality assurance. Functions that already benefit from AI/ML and stand to benefit further as the technology evolves further, are already adequately reviewed under existing regulations.

Ensuring Success for the Market

In the request for comment, the CFTC asks questions about how firms ensure success, but it is worth thinking about how we as an industry can achieve broader success. At its simplest, the key measure is whether AI is delivering better outcomes for the market, end users and the real economy.

AI could help reduce costs, increase revenues and generate efficiencies. This might come from reduced costs in operations for market infrastructure providers and market participants. Alternatively, this may come in the form of new, innovative products. This can benefit end users by offering increased value.

As a whole, technological advancement and automation have typically provided benefits for humanity. We have reduced the need for human labour which has resulted in increased quality of life and also allowed humans to focus on more productive or innovative tasks. AI is merely the next step in automation rather than a radical departure from the norm.

Proposed Way Forward

We should focus on adapting to emerging technologies. More broadly, we as firms, regulators and governments need to upskill our workforces to be able to use AI and to be able to understand the associated risks. In financial services, a continued dialogue between industry and regulators can help foster good practices. It will help firms continue to be compliant with regulation and provides assurance for regulators that firms are managing the risks adequately.

Regulatory co-ordination, both nationally in the United States and internationally with other regulators and standard setters, can be beneficial for firms and the broader economy. The CFTC is not alone in considering its approach to AI and we recognise that, like local authorities across the world, need to design regulations that are right for them. The CFTC can benefit from engaging with other regulators on AI. Furthermore, engaging with international standard setters like the International

Organization of Securities Commissions (IOSCO) and other regulators can help keep effective oversight and supervision globally.

At this time, we do not see the need for new regulations, at least in wholesale markets. We consider that existing regulations that are primarily principles-based and technology neutral provide a good framework for the development of AI. While acknowledging the dynamic nature of technology, it is important to recognise the enduring principles that underpin regulatory compliance. Market abuse, for instance, remains a steadfast concern irrespective of the tools employed, whether traditional or AI-driven. In other words, AI does not fundamentally change the responsibility that regulated entities have.