sifma
Invested in America

sifma
asset management group

April 24, 2024

Submitted via comments.cftc.gov
Chairman Rostin Benham
Commodity Futures Trading Commission
1155 21st St NW
Washington, DC 20036

Re: **Request for Comment on the Use of Artificial Intelligence in CFTC Regulated Markets**

Dear Chairman Benham:

The Securities Industry and Financial Markets Association and its Asset Management Group (collectively, "SIFMA")[1] welcome the opportunity to respond to the Commodity Futures Trading Commission ("CFTC") staff request for public comment on artificial intelligence ("AI") (the "Request").[2] SIFMA recognizes that maintaining public trust in AI applications is essential to realizing the many benefits that AI has to offer, and that recent developments in AI across economic sectors support the establishment of certain controls.

SIFMA appreciates the staff's thoughtful approach in collecting information to better understand the potential impacts of AI on CFTC-regulated markets. SIFMA encourages the CFTC to continue to engage with market participants before considering new rules or guidance and to engage in domestic and international coordination efforts on AI governance. Consistent with its

[1] SIFMA is the leading trade association for broker-dealers, investment banks, and asset managers operating in the U.S. and global capital markets. On behalf of our members, we advocate for legislation, regulation, and business policy affecting retail and institutional investors, equity and fixed income markets, and related products and services. We serve as an industry coordinating body to promote fair and orderly markets, informed regulatory compliance, and efficient market operations and resiliency. We also provide a forum for industry policy and professional development. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association (GFMA).

SIFMA's Asset Management Group ("SIFMA AMG") brings the asset management community together to provide views on U.S. and global policy and to create industry best practices. SIFMA AMG's members represent U.S. and global asset management firms that manage more than 50% of global assets under management. . The clients of SIFMA AMG member firms include, among others, tens of millions of individual investors, registered investment companies, endowments, public and private pension funds, UCITS and private funds such as hedge funds and private equity funds. For more information, visit http://www.sifma.org/amg.

[2] *Request for Comment on the Use of Artificial Intelligence in CFTC Regulated Markets* (Jan. 25, 2024), https://www.cftc.gov/media/10156/AI_RFC_012524/download.

historical approach, the CFTC should not inhibit innovation that can promote fair and efficient derivatives markets or signal inconsistent approaches across regulators or jurisdictions.

SIFMA believes a cautious and risk-based approach is warranted for any potential future regulation of the use of new technology in CFTC-regulated markets, including AI.

I. Existing Regulations Are Sufficient

The use of AI in financial services is not new—in fact, it has been used by market participants for decades to improve efficiency, accuracy, and analysis in many areas including trading, fraud detection, and investment analysis. Market participants have risk-management frameworks that account for this, as they are built upon existing laws and regulations and are continuously uplifted to cover emerging technologies, including AI.

Likewise, the CFTC has an existing risk-based, technology-agnostic framework for regulating the derivatives markets and market participants in response to the deployment of new technology. This framework is focused on activities and outcomes in the derivatives markets, rather than the technology used to achieve those outcomes.[3] Because most risks posed by AI are not novel, SIFMA believes that the CFTC's existing regulatory framework is sufficient to enable firms to manage the risks of using AI. Accordingly, any regulatory activity should focus squarely on activities and outcomes in the CFTC-regulated markets; the technology itself should not be regulated.

II. Key Principles to Guide Oversight of AI and Other Emerging Technologies in CFTC-Regulated Markets

Any regulatory response to emerging technologies should be balanced and avoid impeding innovation. Future action should only be considered if there are gaps that cannot be addressed by existing rules and guidance. If the CFTC does identify areas that warrant further attention, SIFMA, on behalf of its members, encourages the CFTC to consider the following key principles in evaluating regulatory policies that may involve AI:

- Any future governance framework should focus on activities and outcomes, rather than specific technologies.

- Market participants should retain the flexibility to rely on their existing risk-based governance frameworks to determine how to address AI and other emerging technologies, which are aligned with established regulatory and prudential frameworks[4] and are not overly prescriptive. Adapting these existing risk-management frameworks for new technologies allows market participants to remain focused on outcomes. For example, with respect to AI, such frameworks allow market participants to treat AI models, algorithms, applications, and systems (collectively, "AI applications") appropriately depending on the likelihood or

[3] *See* Written Statement of Daniel S. Gorfine to the U.S. Senate Committee on Banking, Housing, and Urban Affairs, *Artificial Intelligence in Financial Services* (Sept. 20, 2023), available at https://www.banking.senate.gov/imo/media/doc/gorfine_testimony_9-20-23.pdf ("Financial services law and regulations have long governed the adoption of emerging technologies in the sector. . . . These laws and regulations largely apply to conduct and activities regardless of the technological tools used by the regulated entity—in this way they are appropriately technology-neutral.").

[4] *See, e.g.*, *Supervisory Guidance on Model Risk Management*, Federal Reserve SR Letter 11-7, OCC Bulletin 2011-12, and FDIC FIL-22-2017; *see also Risk Management Program for swap dealers and major swap participants*, 17 CFR 23.600.

severity of the potential harm they might cause and subject the use of low-risk AI applications to different compliance obligations than those of high-risk applications.

- Market participants should continue to be permitted to adopt governance frameworks covering certain foundational components, including scoping, inventory, risk assessments, training, documentation, and third-party risk management. Market participants should have flexibility on how best to integrate these components with existing policies and functions, including enterprise risk governance programs, model risk, data governance, privacy, cybersecurity, and product development, as well as third-party risk management practices.
- Any future governance framework should be principles-based and flexible enough to adapt to evolving technology and associated risks. A framework that is overly prescriptive would subject every new technology, including AI applications, to onerous risk assessments and audits that are unnecessary or infeasible, stymy innovation, waste resources on low-risk applications at the potential expense of effectively mitigating high-risk applications, and potentially prevent new technologies from benefitting consumers and businesses.

III. Risk-Based Governance Frameworks Appropriately Address New Technologies Such As AI

A. A risk-based approach provides accountability by balancing upside potential with downside risks

SIFMA believes that a risk-based approach to the governance of AI and other emerging technologies provides the necessary flexibility to balance the potential risks with the many potential benefits and opportunities in deploying AI. Firms' existing risk-based governance frameworks that apply to emerging technologies provide strong accountability measures to reduce risk as needed, while also providing flexibility for innovation. The components of such frameworks include: (1) identification of specific risks a company should consider when assessing level of risk posed by the activity; (2) consideration of risk-mitigation controls and processes; and (3) identification of activities that carry unacceptable risks and should not be pursued.

Granular determinations regarding risk and appropriate mitigation measures pursuant to these frameworks are best made by a firm's management, with guidance from its applicable regulators. Notably, the effectiveness of this type of tailored-yet-flexible approach has been illustrated by the existing collaboration between financial institutions and their regulators on model risk management, which has led to strong accountability measures while also allowing for industry innovation.[5]

Any future regulatory activity for AI, to the extent it is necessary, should base any obligations on the degree of risk posed by using AI or other emerging technologies, rather than the technology itself. Moreover, at the early stages of assessing emerging technologies, regulators should evaluate existing principles-based frameworks as they apply to these technologies and avoid pursuing a one-size-fits-all approach that could stifle innovation. An overly restrictive approach also poses a risk

[5] *See* Alliance for Innovative Regulation, *Applying model risk management guidance to artificial intelligence/machine learning-based risk models* (June 2023), https://services.google.com/fh/files/misc/wp_applying_existing_ai_ml_model_risk_management_guidance.pdf (arguing that the Model Risk Management Guidance continues to provide an appropriate framework for assessing financial institutions' management of risk-based models for AI and machine learning, given its "broad, principles-based approach").

that firms will be dissuaded from innovating or creating new technologies, including AI applications, for U.S. markets, which could cause other countries—which are adopting a more flexible "supervised sandbox" approach—to become the preferred destination for companies that are developing new technologies.

B. *Any future guidelines and regulations regarding emerging technologies should reflect the risk-based requirements in cybersecurity but avoid being overly prescriptive*

The Request asks whether market participants identify AI as a source of cybersecurity vulnerability. While the guidance and regulations around cybersecurity may be instructive for evaluating the regulatory framework around AI, policymakers should recognize the differences between these two areas and that each requires its own tailored risk management approach.

Like the risk-based governance frameworks discussed above, many effective cybersecurity guidelines and regulations adopt a risk-based approach that offers companies the flexibility to implement policies and governance based on the associated risks specific to their products, services, and industry. In addition, overly prescriptive cybersecurity regulation can negatively impact compliance and risk mitigation. Although policymakers can consider these lessons from cybersecurity in evaluating how to assess AI accountability, their applicability is somewhat limited because cybersecurity risks and mitigation tend to be more universally applicable across organizations and industries.

Similarly, the use of AI and other emerging technologies can vary significantly within and across organizations and industries, presenting an extremely broad range of risks and mitigation options from one firm to another. As a result, general AI and other emerging technology guidelines and regulations, to the extent they are warranted, must offer even more flexibility and must be even less prescriptive than cybersecurity guidance and regulations to be broadly effective.

Accordingly, a one-size-fits-all approach to cybersecurity for AI would be a significant impediment to developing an effective accountability ecosystem for AI and other emerging technologies, particularly within the already heavily regulated financial services industry. Subjecting each AI application to a complicated, expensive, and time-consuming compliance process is not scalable, would waste resources on low-risk applications, and would prove to be an ineffective approach to addressing the real concern: the mitigation of risks associated with high-risk uses of AI and other emerging technologies. Such a cost-heavy approach would also run the risk of centralizing the use of AI and other emerging technologies among large firms and limit the ability of startups to participate.

C. *Adopting a risk-based approach reduces the need to define AI*

Adopting a risk-based approach will have the additional benefit of reducing the importance of crafting a precise definition for AI. As an initial matter, even if a definition was achieved, it would likely become outdated in the near term due to the evolving nature of technology. That being said, if the CFTC does consider defining AI, SIFMA encourages the CFTC to follow a broadly accepted definition of AI developed by a standard-setting body, rather than creating its own definition.[6] Ultimately, however, any definition of AI that the CFTC chooses to adopt should not make a difference, because existing CFTC regulations apply to any technology that is used to engage in CFTC-regulated conduct. This means that the CFTC would have the ability to regulate the use of AI in these circumstances based on its existing regulations, regardless of how—or whether—it defines the term.

As with other technologies, an AI tool can be used to produce vastly different risk profiles depending on the manner and context of its use. Evaluating the activities and outcomes of applying AI, and the associated risks, rather than assessing the risk of the AI tool itself, would enable the CFTC to focus on high-risk uses in the markets it regulates.

D. Third-party risk management for AI applications should also be risk-based

AI applications that are provided by or for third parties constitute what the Request identifies as the "AI value chain." As with other technologies, firms can leverage their existing third-party risk management processes to address the provision of AI applications and other emerging technologies by third parties. Firms should use the same principles applied to AI applications that are developed in-house for identifying risks associated with third-party AI applications and mitigate those risks through commercially reasonable diligence, audits, and contractual terms.

SIFMA notes that there are many parallels between the third-party risks for AI applications and cybersecurity, and that regulatory requirements for third-party cybersecurity risk mitigation may be instructive for AI applications. For example, the FRB, OCC, and FDIC issued guidance on managing risks associated with third-party relationships to support all stages in the life cycle of third-party relationships.[7] In addition, the CFTC has issued a rule proposal on operational resilience, which includes third-party relationships, which would cover third-party risk management for AI applications.[8]

IV. Conclusion

The risk-based approach in the CFTC's existing regulatory framework appropriately ensures accountability and trust in connection with new technologies, including AI. This approach also avoids stifling innovation or wasting resources on low-risk applications of AI and other technologies at the expense of the important work that needs to be done to ensure that high-risk applications are meaningfully reviewed and effectively mitigated.

AI and other new technologies offer many potential benefits and opportunities to better serve market participants. While emerging technologies may present certain risks, the CFTC already has a well-established risk-based regulatory framework designed to address these risks, which applies to conduct and activity in CFTC-regulated markets regardless of the technology used. Market

[6] *See, e.g.*, National Institute of Standards and Technology, *Artificial Intelligence Risk Management Framework* (Jan. 2023), available at https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf (defining an "AI system" as "an engineered or machine-based system that can, for a given set of objectives, generate outputs such as predictions, recommendations, or decisions influencing real or virtual environments").

[7] FRB, OCC, FDIC, *Interagency Guidance on Third-Party Relationships; Risk Management,* 88 Fed. Reg. 37920 (June 9, 2023).

[8] CFTC, *Operational Resilience Framework for Futures Commission Merchants, Swap Dealers, and Major Swap Participants*, 89 Fed. Reg. 4706 (Jan. 24, 2024).

participants also have risk management frameworks built upon these existing regulatory policies and guidance, which are continuously updated to address the use of emerging technologies, such as AI. Thus, the CFTC should seek to apply its existing risk-based rules and guidance to the deployment of AI and other new technologies in its regulated markets, rather than engaging in new technology-specific rulemakings that will likely be outdated before they are finalized.

*   *   *

SIFMA appreciates the CFTC's consideration of these comments and would be pleased to discuss any of these views in greater detail if that would assist CFTC's deliberations on this issue. SIFMA would welcome the opportunity to continue to participate in this valuable process. Please feel free to contact me at mmacgregor@sifma.org if you would like to discuss these issues further.

Sincerely,

Melissa MacGregor

Melissa MacGregor
Deputy General Counsel & Corporate Secretary
SIFMA

Kevin Ehrlich

Kevin Ehrlich
Managing Director & Associate General Counsel
SIFMA AMG

cc: Kyle Brandon, Managing Director & Director of Derivatives Policy, SIFMA