sifma Invested in America

sifma asset management group

August 9, 2024

Submitted via regulations.gov
Moses Kim, Director, Office of Financial Institutions Policy
U.S. Department of the Treasury
1500 Pennsylvania Ave., NW
Washington, DC 20220

Re: **Request for Comment on Uses, Opportunities, and Risks of Artificial Intelligence in the Financial Services Sector**

Dear Director Kim:

The Securities Industry and Financial Markets Association and its Asset Management Group (collectively, "SIFMA")[1] welcome the opportunity to respond to the U.S. Department of the Treasury ("Treasury") request for information ("RFI") on artificial intelligence ("AI").[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 uses, opportunities and risks presented by developments and applications of AI within the financial sector. SIFMA encourages Treasury to continue to engage with financial institutions before recommending new guidance and to engage in domestic and international coordination efforts on AI governance. Treasury should continue to encourage innovation to

[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 Information on Uses, Opportunities, and Risks of Artificial Intelligence in the Financial Services Sector* (June 6, 2024), https://home.treasury.gov/news/press-releases/jy2393.

promote a fair and efficient financial services ecosystem and should encourage consistent approaches across regulators and federal, state, and international jurisdictions.

EXECTIVE SUMMARY

SIFMA believes a cautious and risk-based approach is warranted for any potential future policies, guidance, or regulation related to the use of new technology in the financial services sector, including AI, for the following reasons:

- The existing robust, effective, risk-based and technology agnostic regulatory approach that governs AI and other emerging technologies is sufficiently flexible and robust to cover the use of AI unless novel risks are found in the future.

- Firms currently deploy risk-based governance frameworks that apply to emerging technologies and provide necessary flexibility to balance upside potential with downside risks.

- Any future guidance or regulations should reflect risk-based requirements, similar to those applied to cybersecurity, and should avoid being overly prescriptive. Adopting such a risk-based and flexible approach to the regulation of AI will negate the need to define AI, and instead the most prudent approach is to assess the risk associated with specific implementation and impose obligations that are proportionate to that risk.

- Third-party risk management obligations for AI applications should also be risk-based and reflect the varied responsibilities for in-house developed applications, third-party developers, and the deployment of third-party AI to firms, while allowing firms to utilize and adapt existing risk-based governance frameworks.

- If warranted, any future policies should be informed by a principles-based approach to guide oversight of AI and other emerging technologies in the financial services sector. Financial regulators should focus on activities and outcomes, allow firms to retain the flexibility to rely on existing risk-based governance frameworks, permit financial institutions to adopt governance frameworks covering certain foundational components, and overall avoid an overly prescriptive approach which would be overly burdensome, stymy innovation, waste resources, and prevent new technologies from benefitting investors.

For these reasons, as described further below, SIFMA encourages financial regulators to maintain the application of existing risk-based rules and guidance in the deployment of AI and other emerging technologies in the financial services sector, rather than engage in overly prescriptive technology-specific policy actions.

I. Existing Regulations Address the Use of AI [Re: Q18]

The use of AI in financial services is not new—in fact, it has been used by financial institutions for decades to improve efficiency, accuracy, and analysis in many areas including trading, fraud detection, and investment analysis. Existing regulations that financial institutions operate

under are designed to be risk-based, technology agnostic, and flexible enough to cover AI and other emerging technologies. Specifically, existing laws and regulations already apply to activities and outcomes regardless of the specific technology used and are exhaustive and robust in nature. Financial institutions have risk-management frameworks that are built upon existing laws and regulations and are continuously uplifted to cover emerging technologies, including AI.

Accordingly, a continued risk-based and technology-agnostic approach is warranted for any regulation of emerging technologies in the financial services industry, including AI. Future policy action should only be considered if novel risks are identified that existing regulations and frameworks cannot address.

Furthermore, there is an increasing risk of a patchwork of state laws regulating AI not unlike what has happened with privacy legislation.[3] Such fragmentation will result in uneven requirements on AI developers and users, varied availability of AI products to consumers, and limitations on the ability to innovate in some jurisdictions. These issues will greatly impact the development of AI in financial services and for business more broadly. Treasury should support exemptions and federal preemption of such laws for entities regulated by the SEC or prudential regulators.

II. Risk-Based Governance Frameworks Appropriately Address Technologies Such as AI [Re: Q9, Q17, Q18]

A. A risk-based approach provides accountability by balancing upside potential with downside risks [Re: Q18]

A risk-based, technology-agnostic approach to the governance of AI and other emerging technologies provides the necessary flexibility to balance the potential risks with the many potential benefits, efficiency gains, and opportunities for investors, markets, and economies that come from the use of 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 the innovation that is crucial for investors to achieve their goals. Detering such innovation could prevent consumers from receiving the significant benefits technology like AI has to offer and put U.S. companies at a competitive disadvantage. 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) implementation of risk-mitigation controls and processes where indicated; 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.[4]

---

[3] *See* Colorado AI Act, SB-206.

[4] *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_

Any future policy 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. Such an overly restrictive approach poses a risk 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. Moreover, this risk is amplified if different jurisdictions take conflicting or inconsistent approaches to regulating AI, because a fragmented AI policy landscape will present significant confusion and compliance challenges for firms subject to numerous regulatory regimes.

B. Any future guidelines and regulations regarding emerging technologies should reflect the risk-based requirements in cybersecurity but avoid being overly prescriptive [Re: Q17]

The RFI notes that the Financial Stability Oversight Council ("FSOC") identified AI as a source of cybersecurity vulnerability in its 2023 annual report.[5] 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 have adverse impacts, including on 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. Any approach, as with existing risk-based governance frameworks, should narrowly identify specific undesirable outcomes or risks and provide for principles-based, technology agnostic measures to manage the risk of such outcomes, rather than proactively applying a prescriptive structure to the use of AI or other emerging technologies.

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

---

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").

[5] *See* FSOC, Annual Report (2023), https://home.treasury.gov/system/files/261/FSOC2023AnnualReport.pdf.

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 smaller firms or startups to participate.

C. Adopting a risk-based approach reduces the need to define AI [Re: Q1]

Maintaining a risk-based, technology agnostic approach negates the need to precisely define AI. A definition of AI, while helpful for discussion purposes, is not necessary or required for policy purposes, and it should not be used as the basis for determining which technologies fall within the scope of policymaking. In addition, any definition of AI should not significantly impact regulatory practices, as existing policies and regulations already apply regardless of technology used to engage in regulated conduct. This means that regulators 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. Such regulations already apply to existing uses of AI technology, including more traditional AI applications which have been in use in the industry for decades.

The most prudent policy approach is to assess the risk associated with a specific implementation and impose obligations that are proportionate to that risk. As with other technologies, an AI application can be used to produce vastly different risk profiles depending on the manner and context of its use. Evaluating the activities and outcomes of AI applications, and the associated risks, rather than the AI technology itself, would enable Treasury to focus on high-risk uses in the financial services sector.

That being said, if Treasury does consider defining AI, SIFMA encourages Treasury to adopt a widely accepted definition of AI developed by a standard-setting body,[6] rather than creating its own definition or adopting an overly broad definition, and any definition should algin with, or at a minimum not conflict with, definitions of AI in existing regulatory frameworks for financial institutions.

D. Third-party risk management for AI applications should also be risk-based [Re: Q15, Q16]

AI applications that are provided by or for third parties constitute 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

[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"); White House, E.O. 14110, *Safe, Secure, And Trustworthy Development And Use Of Artificial Intelligence* (Oct. 30, 2023), https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-andtrustworthy-development-and-use-of-artificial-intelligence (adopting a similar definition of AI).

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] Future guidance should reflect the varied responsibilities for in-house developed AI applications, third-party developers of AI, and the deployment of third-party AI by firms, and should allow institutions to utilize and adapt their existing frameworks to use of AI commensurate with the corresponding risks. Such guidance should also indicate what risk-based reasonable testing, monitoring, and diligence is required when deploying third-party technology.

III. Key Principles to Guide Oversight of AI and Other Emerging Technologies in the Financial Services Sector [Re: Q18]

Any policy 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 and should avoid conflicts or duplication with existing risk frameworks. Any action should be informed by ongoing dialogue between policymakers and regulators to prevent regulatory fragmentation and promote coordination. If Treasury does identify areas that warrant further attention, SIFMA, on behalf of its members, encourages Treasury to consider the following key principles in evaluating policies that may involve AI:

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

- Financial institutions should retain the flexibility to rely on their existing risk-based governance frameworks to determine how to manage the risks of AI and other emerging technologies, which are aligned with established regulatory and prudential frameworks[8] and are not overly prescriptive. Adapting these existing risk-management frameworks for new technologies allows financial institutions to remain focused on outcomes. For example, with respect to AI, such frameworks allow financial institutions to treat AI models, algorithms, applications, and systems (collectively, "AI applications") appropriately depending on the likelihood or severity of the potential harm they might cause and subject the use of higher-risk AI applications to stricter compliance obligations than those of low-risk applications.

- Financial institutions 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. Financial institutions should have flexibility on how best to integrate these components with existing policies and functions, including enterprise risk governance programs, model risk, data governance,

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

[8] *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* applicable market and investor protection rules and regulations.

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. It could also lead to inconsistent AI regulations across jurisdictions that pose significant compliance challenges to firms, with potential consequences for consumers and national security.

IV. Conclusion

The risk-based approach in the 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 investors, markets, and financial institutions. While emerging technologies may present certain risks, the already well-established risk-based financial regulatory framework is designed to address these risks, which applies to conduct and activity in the financial services sector regardless of the technology used. Financial institutions also have robust 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, financial regulators should seek to apply its existing risk-based guidance to the deployment of AI and other new technologies in the financial services sector, rather than engaging in new technology-specific guidance that will likely be outdated before it is finalized.

* * *

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

Sincerely,

Melissa MacGregor

Melissa MacGregor
Deputy General Counsel & Corporate Secretary
SIFMA

Kevin Ehrlich

Managing Director & Associate General Counsel
SIFMA AMG