FINANCIAL & INTERNATIONAL BUSINESS ASSOCIATION

August 12, 2024

UPLOADED VIA FEDERAL E-RULEMAKING PORTAL

Departmental Offices
U.S. Department of the Treasury
P.O. Box 39
Vienna, VA 22183

Re: Request for Information on Uses, Opportunities, and Risks of Artificial Intelligence in the Financial Services Sector ("**RFI**") – *Comment Letter of the Financial and International Business Association, Inc.*

Ladies and Gentlemen:

The U.S. Department of the Treasury ("**Treasury**") has requested comments though the RFI from stakeholders in the financial sector on the uses, opportunities and risks presented by developments and applications of artificial intelligence ("**AI**") within the financial sector, as well as the risks and other concerns related to the use of AI.

The Financial and International Business Association, Inc. ("**FIBA**"), a not-for-profit Florida corporation, appreciates the opportunity to provide these comments to Treasury in response to the RFI. Founded in 1979, FIBA is a trade association and international center for financial excellence whose membership includes the largest financial institutions from the United States, Latin America, Europe, and the Caribbean. FIBA's members are principally cross-border bankers (consisting of U.S. and non-U.S. depository institutions, trust companies, securities broker-dealers, and investment advisers, among others) with internationally active businesses. FIBA has had the privilege of enjoying a long history of collaboration with Treasury and other U.S. federal financial regulators in those regulators' efforts to adopt and implement a broad range of policy objectives.

By way of this letter, FIBA wishes to provide comments to various questions presented by Treasury in the RFI. For ease of review, the RFI sections and questions are reproduced below in bold type, with the numbering used in the RFI maintained for each question and are followed by FIBA's comments.

A. <u>General Use of AI in Financial Services</u>

<u>Question 2</u>: **What types of AI models and tools are financial institutions using? To what extent and how do financial institutions expect to use AI in the provision of products and services, risk management, capital markets, internal operations, customer services, regulatory compliance, and marketing?**

FIBA member institutions generally utilize AI tools in a limited capacity for the purpose of financial modeling. While not a majority, a number of FIBA members have adopted new technologies, including AI, for purposes of supporting their compliance with Bank Secrecy Act/Anti-Money Laundering and sanctions program requirements. These uses include transaction monitoring, alert screening, sanctions programs sanctions screening and customer due diligence. FIBA member institutions have expressed interest in expanding AI use to a number of other areas throughout their institutions, including Risk Management, Internal Audit, Finance, Legal, IT, Information Security, and Marketing.

In addition to the above, many institutions already use AI tools albeit indirectly as a result of their use by external service providers such as CrowdStrike (End Point Protection) and Artic Wolf (SIEM).

<u>Question 4</u>: **Are there challenges or barriers to access for small financial institutions seeking to use AI? If so, why are these barriers present? Do these barriers introduce risks for small financial institutions? If so, how do financial institutions expect to mitigate those risks?**

The principal barriers to access are those of cost and expertise. With respect to cost, the expenses associated with implementing and validating AI tools presents a significant challenge to community banks, which already devote considerable financial resources to their existing IT infrastructure. Beyond costs, the lack of AI expertise within smaller institutions presents considerable challenges to reasonably understanding the functionality of AI tools and their associated models, and this, as a result, makes it difficult to determine what measures a small institution must implement to control the risks associated with AI tools.

One particular concern presented by AI is data security risk, especially the risk presented by those AI tools that are cloud-based and/or connect to systems outside of the institution's own network. Data breaches present not only significant reputational risk to institutions but can also cause institutions to incur considerable costs including costs associated with contacting affected customers, as well as costs necessary to address legal and regulatory requirements and expectations. These costs can seriously impact smaller institutions, especially. Therefore, small institutions are hesitant to implement AI tools that they are unable to fully assess through their own risk management programs and as a result, they must rely heavily on vendors and third-party consultants to perform tasks that may otherwise be performed by AI tools.

B. <u>Actual and Potential Opportunities and Benefits</u>

<u>Question 5</u>: **What are the actual and expected benefits from the use of AI to any of the following stakeholders: financial institutions, financial regulators, consumers, researchers, advocacy groups, or others? Please describe specific benefits with supporting data and examples. How has the use of AI provided specific benefits to low-to-moderate income consumers and/or underserved individuals and communities (e.g., communities of color, women, rural, tribal, or disadvantaged communities)?**

Despite the risks presented by AI tools, financial institutions recognize that their use can provide considerable operational benefits from increased productivity through automation of various back-office functions, enhanced compliance monitoring and information security tools, which are better able to defend against AI-directed attacks. In cases where criminals and hackers deploy AI to gain access to data or commit fraud, the use of AI tools can help prevent these attacks through early identification and data protection.

C. Actual and Potential Risks and Risk Management

1. Oversight of AI — Explainability and Bias.

Question 6: **To what extent are the AI models and tools used by financial institutions developed in-house, by third-parties, or based on open-source code? What are the benefits and risks of using AI models and tools developed in-house, by third-parties, or based on open-source code?**

Rather than developing their own tools and models in-house, because of their resource and expertise constraints, smaller institutions that have begun to implement AI are doing so using tools developed by third-party vendors. Doing so allows such institutions to benefit from the expertise and resources of their vendors. However, these tools present various risks, including data security risks as noted above.

Question 7: **What challenges exist for addressing risks related to AI explainability? What methodologies are being deployed to enhance explainability and protect against potential bias risk?**

A major challenge for financial institutions in addressing risks related to AI explainability is the general lack of AI experts who are knowledgeable of the subject area and can accurately describe AI tools and models or respond to risk-related questions. For example, financial institutions often experience difficulties in determining how AI outputs and decisions are made, mainly due to a lack of transparency on the part of vendors. Part of this challenge is rooted in the fact that much of the information presented to financial institutions regarding AI tools comes from salespersons who lack the technical knowledge to fully address concerns raised by institutions. Financial institutions would greatly benefit from greater access to the experts who developed the tools which they are assessing, as well as from greater input and guidance from experts in the field generally. This would allow financial institutions to obtain a better understanding of the potential risks presented by a given AI tool, the reasons for those risks, and thus inform the development of appropriate controls to mitigate such risks.

2. Fair Lending, Data Privacy, Fraud, Illicit Finance, and Insurance.

Question 12: **How are financial institutions, technology companies, or third-party service providers addressing and mitigating potential fraud risks caused by AI technologies? What challenges do organizations face in countering these fraud risks? Given AI's ability to mimic biometrics (such as a photos/video of a customer or the customer's voice) what methods do financial institutions plan to use to protect against this type of fraud (e.g., multifactor authentication)?**

Financial institutions are increasingly aware of the potential fraud risks associated with AI, particularly with the rise of tools that are able to mimic the voices of customers in order to circumvent authentication procedures. FIBA members are therefore taking proactive steps to invest in security enhancements, such as multi-factor authentication, physical security devices, and biometrics. Institutions are also introducing training for their staff which specifically addresses emerging trends in AI-powered fraud in order to help identify fraudulent activity and mitigate losses to the institution and its customers.

3. Third-Party Risks

<u>Question 15</u>: **What challenges exist to mitigating third-party risks related to AI, and in particular, emerging AI technologies, for financial institutions? How have these challenges varied or affected the use of AI across financial institutions of various sizes and complexity?**

As discussed above, the principal challenge that exists to mitigating third-party risk related to AI is the general lack of AI experts who are knowledgeable of the subject area and can accurately describe AI tools and models or respond to risk-related questions so that institutions can understand the potential risks presented by a given AI tool and develop appropriate controls to mitigate identified risks.

To mitigate third-party risk relating to AI and emerging AI technologies, member institutions have begun to incorporate AI-specific reviews into their vendor management process in order to identify those vendors that utilize AI and, for those vendors that do utilize AI, to perform additional diligence with the aim of assessing the potential risks to the institution. However, such assessments are regularly hindered by the inability of vendor sales personnel to knowledgeably respond to inquiries regarding the technical aspects of AI tools. In addition, financial institutions, especially smaller institutions with limited resources, lack personnel within their own organizations with the requisite knowledge and expertise to review third-party AI tools to adequately assess risks to the institution.

<u>Question 16</u>: **What specific concerns over data confidentiality does the use of third-party AI providers create? What additional enhancements to existing processes do financial institutions expect to make in conducting due diligence prior to using a third-party provider of AI technologies?**

The use of third-party AI providers create significant concerns regarding the security of data processed through AI tools as well as concerns regarding general access to internal systems. Of particular concern is the inability of institutions to obtain from their vendors sufficient information to fully evaluate the potential risks associated with AI tools, such as risks related to storage, leakage, and misuse of data. It is often the case that vendor salespersons and, when available, systems engineers, are not qualified to satisfactorily respond to security concerns presented by institutions.

Additionally, AI tools developed outside of the United States present security concerns and particularly, concerns that data will be transmitted outside of the country and become accessible to foreign authorities or other persons outside of the United States. Many institutions also report that lack of knowledge regarding legal or regulatory controls over AI tools in foreign jurisdictions impact their ability to appropriately evaluate risks associated with AI tools developed or deployed outside of the United States.

* * * *

FIBA hopes that Treasury finds these comments helpful to the dialogue between the industry and its regulators. We welcome the opportunity to further discuss these points at Treasury's convenience.

Very truly yours,

David Schwartz
President & CEO
Financial and International Business Association, Inc.