June 9, 2021

Chief Counsel's Office
Attention: Comment Processing
Office of the Comptroller of the Currency
400 7th Street SW
Suite 3E–218
Washington, DC 20219

Ann E. Misback
Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Washington, DC 20551

James P. Sheesley
Assistant Executive Secretary
Attention: Comments-RIN 3064–ZA24
Federal Deposit Insurance Corporation
550 17th Street NW
Washington, DC 20429

Comment Intake
Bureau of Consumer Financial Protection
1700 G Street NW
Washington, DC 20552

Melane Conyers-Ausbrooks
Secretary of the Board
National Credit Union Administration
1775 Duke Street
Alexandria, VA 22314–3428

Re: Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, Including Machine Learning

To the Above-Listed Agencies:

The Securities Industry and Financial Markets Association ("SIFMA")[1] welcomes the opportunity to present its views to the Board of Governors of the Federal Reserve System, the Bureau of Consumer Financial Protection, the Federal Deposit Insurance Corporation, the National Credit Union Administration, and the Office of the Comptroller of the Currency (collectively, the

[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).

"Agencies") in response to the Agencies' request for information and comment on financial institutions' use of artificial intelligence ("AI"), including machine learning (the "Request").[2]

SIFMA's response on behalf of its members focuses on general principles and approaches that might usefully guide regulators' consideration of issues that arise in this context. In the sections that follow, the response describes financial institutions' extensive risk identification and mitigation processes that have long focused on technology-related risks specific to the financial services industry. Those risks take many forms, now specifically including AI-related risks. The response also discusses how those processes enable financial service providers to respond to many of the particular concerns and issues raised in the questions posed in the Request, and how those existing and evolving risk management processes enable financial service providers to continue to address emergent AI-related risks. At the same time, financial service providers continue to secure the extensive benefits that AI capabilities provide to consumers and the industry.

I. General Considerations that Might Usefully Guide Oversight of the Use of AI in the Financial Services Sector.

The growing use and capabilities of AI have understandably captured the attention of the public and regulators in a broad range of sectors. It makes sense for financial services regulators to increase their understanding and the public's understanding of how AI is used, evidence related to perceived risks, and how actual risks are being addressed. Close and ongoing discussions and exchanges of information between regulators and industry are especially important. For all these reasons, the Request is an important step in a valuable process. SIFMA and its members welcome the opportunity to participate in this process through this response and on an ongoing basis.

The financial services sector does, however, have unique and important differences, when compared to other major industries, in its treatment of AI-related risks and capabilities. These differences, described below, are particularly relevant for the Agencies to consider as they oversee the regulatory framework that governs the use of AI. In particular, as the Agencies know, established financial institutions already have sophisticated systems in place for overseeing a broad variety of risks, including risks posed by the use of AI in various contexts.

Financial service providers have devised and implemented these risk management frameworks with extensive input from bank regulators, at both the policy and implementation levels. The boards and senior managers of financial institutions, as well as regulators themselves, devote considerable resources to ensuring the adequacy, flexibility, and adaptability of those systems and processes to identify, quantify, and mitigate risks of various types. The resulting risk management systems typically involve both focused accountability and cross-function and cross-divisional processes. Firms measure the resulting effectiveness of these processes with a range of established and evolving tools. As different types of asset, personnel, macroeconomic, and process risks emerge and are addressed, institutions test, refine, and expand the capabilities of their risk management processes.

---

[2] *Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, Including Machine Learning*, 86 Fed. Reg. 16837 (March 31, 2021), https://www.govinfo.gov/content/pkg/FR-2021-03-31/pdf/2021-06607.pdf.

At the same time, financial institutions' uses of AI capabilities are not new, and their consideration and management of risks related to those uses are well developed. The risk management personnel and processes just noted have been focused on risks presented by AI for many years. Machine and automatic processes have long been part of the functions used by financial institutions related to processing customer information, monitoring and protecting against fraud, assessing financial performance and risk, evaluating credit risk, assessing value at risk, and discharging many other functions. In recent years, the software and "artificial" capabilities associated with these processes have grown more sophisticated. Likewise, financial institutions have undertaken an equally long and continuous process of identifying, monitoring, and mitigating risks associated with using those capabilities. To achieve those goals, institutions are already working closely with regulators to ensure that those processes adequately identify and address various types of risks associated with AI. This cooperation, like the underlying processes themselves, takes various forms depending on the context and type of business function at issue.

II. Considerations Related to Managing Risks Associated with Several of the Particular Issues Raised in the Agencies' Request.

a. Model Risk Management and Other Processes are Central to How Financial Institutions Safeguard Their Particular Uses of AI.

Many of the issues presented by the Request might be best understood and analyzed in the context of financial institutions' approaches to model risk management and other measures designed to ensure the integrity of data and data use. In many respects, AI presents risks closely related to reliance on models, and financial institutions address AI-related risks in the course of their model risk management processes and by implementing related safeguards.

Regulators and financial institutions have long understood that institutions' use of models in business operations and decision-making presents risks.[3] At the same time, reliance on those models, including those using AI capabilities, is an inherent and often valuable component of modern financial risk management and service provision. Safeguarding and validating the quality of the data and processes these models rely on—and the benefits they provide to firms and consumers—have also long been important considerations for established financial service providers.

Financial services firms have invested heavily in developing sophisticated frameworks for the management of model risk. They have done so both in response to expanding regulatory requirements, like the Federal Reserve's *SR 11-7* (the FDIC's *Supervisory Guidance on Model Risk Management*) and to secure the benefits to themselves and their customers of accurate and capable models.[4] Firms have implemented safeguards for various aspects of these models' operation, including model lifecycle management (e.g., creating an inventory of models,

[3] Fed. Deposit Ins. Corp., *Supervisory Guidance on Model Risk Management*, at 1 (2017), https://www.fdic.gov/news/financial-institution-letters/2017/fil17022a.pdf.

[4] *See* Ignacio Crespo, Pankaj Kumar, Peter Noteboom, and Marc Taymans, *The evolution of model risk management*, MCKINSEY & CO., Feb. 20, 2017, https://www.mckinsey.com/business-functions/risk/our-insights/the-evolution-of-model-risk-management.

classifying models by risk, and documenting key information about each model) and model control (e.g., validating models annually or more frequently if warranted[5] and requiring approval before models are brought online).[6] These and other risk management efforts benefit from significant oversight from high-ranking officers. A firm's approach to model risk management is typically approved by the firm's Board of Directors, and firms increasingly use senior executives to support model risk management. For example, the model risk management functions within many banks now report directly to the Chief Risk Officer.[7] Of course, firms assess the degree of risk presented by particular models, and they provide for more extensive and senior review of those models and contexts presenting greater risks.

These robust model risk management frameworks allow firms to identify, describe, oversee, and otherwise monitor the risks associated with models. The processes that make up this sophisticated framework are adaptable, and firms rely on and employ existing controls when deploying models that have AI capabilities. In this way, firms mitigate many of the risks associated with AI approaches, including those raised by the Request. For example, the Request notes that undetected overfitting by an AI approach "can result in incorrect predictions or categorizations."[8] However, robust model validation, benchmarking, and testing processes can identify these risks and enable a change of course. Standard cross-validation, out-of-sample validation, and out-of-time validation all minimize the likelihood of overfit, and these tools are flexible, meaning that firms can use more rigorous validation processes for higher-risk AI approaches. Firms also detect model deterioration quickly through ongoing monitoring of model performance. Overfitting risks may particularly arise when an institution implements a model that proves to be less predictive than anticipated. To account for this source of overfitting risk, firms monitor models and periodically refit them when model performance has deteriorated or there is a shift in the relevant population.

Explainability is another risk associated with AI that the model risk management process mitigates. The Request notes that a lack of explainability for a particular AI approach may "inhibit financial institution management's understanding of the conceptual soundness of an AI approach" or "inhibit independent review and audit [of an AI approach] and make compliance with laws and regulations, including consumer protection requirements, more challenging."[9]

---

[5] Crespo, Kumar, Noteboom and Taymans offered helpful insight into model validation efforts conducted by "best practices" institutions: "Best-practice institutions are classifying models (model "tiering") using a combination of quantitative and qualitative criteria, including materiality and risk exposure (potential financial loss), and regulatory impact. Models are typically prioritized for validation based on complexity and risk associated with model failure or misuse. Model risk is defined according to potential impact (materiality), uncertainty of model parameters, and what the model is used for. The level of validation is located along a continuum, with high-risk models prioritized for full validation and models of low risk assigned light validation. In the majority of banks we surveyed, validation is highly centralized and situated in the risk organization." *Id*.

[6] *Model Risk Management, Driving the value in modelling*, DELOITTE, April 2017, https://www2.deloitte.com/content/dam/Deloitte/fr/Documents/risk/deloitte_model-risk-management_plaquette.pdf.

[7] *See* Crespo et al., *supra* note 4 ("Most US banks have strengthened the independence of validation, with the head reporting directly to the CRO.").

[8] *Request* at 16841.

[9] *Id.* at 16840.

Definitions of explainability vary, and the appropriate definition depends on the particular use case. As with overfitting, however, financial institutions address these issues as needed by designing models with appropriate explainability in mind and by testing and assessing models' performance to ensure that the institution's understanding of a model's explainability is appropriate.

Using various tools in different contexts, financial service providers identify and address explainability concerns associated with higher risk uses of AI, while also preserving the benefits those approaches can provide. The complexity and materiality of a particular use of an AI capability, and thus the explainability issues accompanying that use, vary significantly based on the capability's parameters and sensitivities and the business function it performs. Simple AI methods may be easier to explain but may also provide fewer benefits to financial institutions and consumers. Other methods of AI may be more complex and therefore pose greater challenges to firms, but those challenges are often worth undertaking because the use might also provide substantial benefits to both firms and consumers. Established financial service providers recognize the risks associated with different AI approaches, and tailor and adapt their controls as appropriate to help account for these risks and to comply with regulations applicable to financial institutions.

The financial services industry uses AI capabilities, and focuses on managing AI risks, in many contexts other than financial modeling and risk management. Indeed, firms may deploy AI in various contexts, including as tools used to pinpoint promising sales opportunities, to support human resources tasks, and to underpin analytic services tools (e.g., for identifying industry trends or assessing product or portfolio performance).

In all these contexts, firms have developed procedures to minimize risks associated with these AI capabilities and, in particular, to protect the integrity of the data they address.[10] Firms often employ data governance processes that, alongside firms' model risk management procedures, help to mitigate the risks associated with the firm's uses of AI capabilities. Depending on the particular context, firms might use procedures to verify the sources of their data (especially data that is externally-sourced or open-sourced), to effectively integrate data into their systems, to authenticate users of data, or to promote data security.[11] Firms might also use data quality benchmarks and metrics to monitor their data inputs and outputs. Additionally, some financial institutions employ Chief Data Officers ("CDO") or Data Governance Committees responsible for "operationaliz[ing] data governance, data quality, and other controls to sustain the integrity of the data of an organization."[12]

---

[10] For these purposes, financial services firms are not all similarly situated and do not deal with identical AI capabilities. Nevertheless, firms widely share concerns about addressing the data-related risks associated with AI.

[11] *See* FIN. INDUS. REGULATORY AUTH. ("FINRA"), *Artificial Intelligence (AI) in the Securities Industry*, at 14–15 (June 10, 2020), https://www.finra.org/rules-guidance/key-topics/fintech/report/artificial-intelligence-in-the-securities-industry.

[12] *The evolving role of the chief data officer in financial services*, DELOITTE, at 3 (2016), https://www2.deloitte.com/content/dam/Deloitte/uy/Documents/strategy/gx-fsi-evolving-role-of-chief-data-officer.pdf.

Proper data governance is particularly important for addressing potential risks of unfair bias or discrimination arising from the use of AI capabilities. Financial institutions have tremendous incentives—including ensuring compliance with anti-discrimination laws—to prevent unfair discriminatory effects arising from the use of AI. They, like regulators, seek to develop appropriate safeguards against these risks to ensure that the many benefits AI innovation can bring to consumers in terms of convenience, pricing, and access can continue to grow, while also protecting against discriminatory outcomes. Here, too, existing data governance processes can be, and are, used and expanded to address this risk. Many firms, when applicable, conduct routine testing of AI models and thoroughly assess data sources for discriminatory impact, as appropriate to the use case. They evaluate data inputs into AI algorithms for explicit or implicit bias through validation of the relevant algorithm's output (adjusting the input data or how the output data are used as necessary), as appropriate to the use case. Additional steps may also safeguard how output data are used—for example, by using continuous monitoring and oversight as new data are processed by the AI capabilities.

b. AI and Cybersecurity Risks.

The Request notes that member firms' use of "AI may be exposed to risk from a variety of criminal cybersecurity threats."[13] While this is true, these risks are often similar to the broad range of cybersecurity risks that confront financial institutions and for which they have for many years adopted extensive countermeasures. Indeed, AI capabilities have proven to be an important and often essential component of cyber defense measures, and regulatory or other efforts to curtail the use of AI to address cybersecurity concerns could prove counterproductive.

In particular, an institution's risk profile is not automatically broadened by using AI capabilities. Complex and significant legal requirements apply to how firms ensure customer privacy, store information, defend against cyberattacks, and protect particularly sensitive types of information. To comply with these requirements—many of which apply specifically to financial institutions—financial institutions work closely with the Agencies and other regulators to design and implement comprehensive risk management controls. These controls include, for example: maintaining data quality and integrity policies; maintaining policies and procedures governing the firms' use, storage, or processing of personal identifying information; extensive IT testing and countermeasures; and cybersecurity and operational resiliency frameworks including access entitlements, encryption, API security compensating controls, and third-party risk frameworks for third-party AI models. The risks the Agencies identify as peculiar to AI, such as "poisoning" data pools, are generally encompassed and addressed within these broader cybersecurity measures and processes.

As importantly, AI capabilities provide invaluable assistance to financial institutions as they seek to combat cybersecurity attacks and increase the effectiveness of their monitoring and prevention systems. As the Agencies note in their request for information in this matter, "AI may be used to detect threats and malicious activity, reveal attackers, identify compromised systems, and support

[13] *Request* at 16841.

threat mitigation."[14] This point cannot be overemphasized, and regulatory oversight in this context should be designed to facilitate and increase the effectiveness of the use of AI as a defense measure rather than necessarily focused on the vulnerabilities that AI creates for cyberattacks. For both concerns, building on existing processes remains very important. To the extent the Agencies have identified particular cybersecurity vulnerabilities that arise from the use of AI, productive regulatory approaches include continuing to develop a widely employed taxonomy, and might also take the form of disseminating information regarding vulnerabilities, coordinating with other U.S. government agencies that have cyberdefense as their principal mission, and facilitating coordination among financial institutions and between them and those government institutions.

III. Securing AI Benefits and Reducing Risks by Building on Existing Institutional Practices.

As the preceding discussion indicates, substantial benefits arise when institutions and regulators rely and build on existing institutional risk management processes to meet the challenges posed by increasing AI capabilities. These processes are sophisticated, well-established and understood, flexible, effective, and already focused on addressing potential AI risks.

Likewise, the Agencies might usefully adopt a relatively high threshold for requiring a factual showing of unaddressed harm or risk before considering or prescribing new regulations. They might tread lightly where no significant problems or abuses have surfaced despite their own and financial institutions' acute focus on the possible risks. Regulation may especially cause adverse and unintended consequences if it departs from, or requires institutions to depart from, these traditional context- and process-specific approaches, or prescribes novel and categorical approaches to addressing aspects of AI used by financial institutions. The characteristics and uses of different AI capabilities vary tremendously, as do the risks presented by their particular applications. It would be extremely difficult to craft and implement regulations, especially prescriptive regulations, that would effectively apply to these varied circumstances.

Continued reliance upon, and development of, existing risk management processes used by established financial institutions also has the potential to most effectively foster the very significant benefits that AI holds out for the financial system, industry, and consumers. A range of federal and international officials have recognized these benefits, including those set forth in the Request itself.[15]

As with the benefits and risks associated with AI, many of these benefits arise in contexts that may also present elements of risk. For example, many potential institutional and consumer benefits arise from standardizing and systematizing decision-making. With appropriate oversight and

[14] *Id.* at 16839. The Request also provides several examples of the cybersecurity applications of AI. These examples include: "real-time investigation of potential attacks, the use of behavior-based detection to collect network metadata, flagging and blocking of new ransomware and other malicious attacks, identifying compromised accounts and files involved in exfiltration, and deep forensic analysis of malicious files."

[15] *See e.g.*, FINRA, *supra* note 11; Eur. Comm'n, *White Paper on Artificial Intelligence – A European approach to excellence and trust*, COM(2020) 65 final, 2020; Eur. Comm'n, *Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*, COM(2021) 206 final, 2021.

internal checks and balances, such decision-making can be more fair, efficient, and sophisticated—all yielding important consumer benefits. AI can, and does, play an important role in achieving these benefits. Likewise, AI can assist institutions in drawing on "alternative data," with corresponding consumer benefits. For example, data related to environmental and social considerations, or reflecting consumer behavior or preferences, often can be integrated into broader decision-making and may assist in ensuring the accurate and effective development and management of risk models and service provision. More generally, whatever the sources of data, AI can assist institutions in identifying, analyzing, and employing that data in the course of the development and delivery of services.

Established financial institutions have incentives to develop these AI-related benefits in a responsible manner, and they will continue to do so by employing many of the same risk-identification and management processes that assist them in developing other products and capabilities. Those risk management processes have often been developed in conjunction with regulators' input and subject to their continued, often extensive oversight and regulation. Many are distinct to the financial industry and provide financial firms with unique and uniquely suitable ways to address AI-related risks. Those processes are flexible and have proved suitable for addressing issues and risks surrounding AI capabilities and related data integrity concerns. Until, and unless, clear evidence shows that these processes and mechanisms are insufficient, both regulators and established financial service providers are well served by continuing to have firms develop and rely on those capabilities.

* * *

SIFMA greatly appreciates the Agencies' consideration of these comments and would be pleased to discuss any of these views in greater detail if that would assist the Agencies' deliberations. Please feel free to contact me at (202) 962-7385 if you would like to discuss further.

Sincerely,

Melissa MacGregor

Melissa MacGregor
Managing Director and Associate General Counsel

cc: Alan Charles Raul, Richard Klingler, and Christopher Joyce, Sidley Austin LLP
Counsel to SIFMA