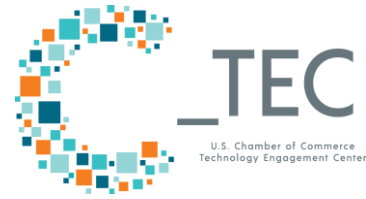




CENTER FOR CAPITAL MARKETS
COMPETITIVENESS



July 1, 2021

Ann E. Misback
Secretary of the Board of Governors of the
Federal Reserve System
Washington, DC 20551

Mr. Robert E. Feldman
Executive Secretary
Federal Deposit Insurance Corporation
Washington, DC 20429

Chief Counsel's Office, Attention: Comment
Processing
Office of the Comptroller of the Currency

Melane Conyers-Ausbrooks
Secretary of the Board
National Credit Union Administration
Alexandria, VA 22314

Comment Intake
Consumer Financial Protection Bureau
Washington, DC 20552

To Whom It May Concern:

The U.S. Chamber of Commerce's ("the Chamber") Center for Capital Markets Competitiveness ("CCMC") appreciates the opportunity to comment on the Request for Information and Comment ("RFI") issued by the Office of the Comptroller of the Currency ("OCC"), the Federal Reserve Board ("FRB"), Federal Deposit Insurance Corporation ("FDIC"), National Credit Union Administration ("NCUA"), and the Consumer Financial Protection Bureau ("CFPB") (collectively, "the Agencies") on "Financial Institutions' Use of Artificial Intelligence, Including Machine Learning."¹

According to the RFI, the purpose of the publication is to understand respondents' views on the use of artificial intelligence and machine learning ("AI") by financial institutions in their customer service and for other businesses or operational purposes; appropriate governance, risk managements, and controls over AI; and any challenges in developing, adopting, and managing the AI. The RFI also requests comment on whether clarification from the Agencies would be helpful for use of AI in a safe and sound manner and in compliance with applicable laws and regulations, including those related to consumer protection. When considering AI oversight, we urge the Agencies to encourage supervisory and examinations teams to be flexible, avoid regulation by enforcement, and engage in any AI policy with full transparency and opportunity for stakeholder feedback.

The Chamber strongly supports a balanced and innovative approach towards AI applications that can mitigate any increased risks posed by AI while maximizing its innovative

¹ See RFI for Information and Comment on Financial Institution's Use of Artificial Intelligence, Including Machine Learning, 86 Fed. Reg. at 16837 (March 31, 2020)

potential. In September 2019, the Chamber released a set of AI policy principles that outline regulatory concepts for AI such as adopting risk-based approach and endorsing sector-specific solutions as opposed to one-size fits all.² The Chamber has also extensively engaged and is supportive of the Office of Management and Budget's ("OMB") memorandum on Guidance on the Regulation of Artificial Intelligence Applications ("OMB Memorandum") that was finalized in November 2020.³ Broadly, the Chamber urges the Agencies to consider the evolving nature of AI when contemplating any new policy options.

The Chamber appreciates the Agencies' interest in the use of AI by financial institutions, including the benefits to consumers, efficiencies presently being realized, and the opportunities for the consumer experience and protections, all while promoting a fair marketplace. There are countless opportunities for AI to improve the financial system.

It is important to recognize at the outset of these discussions that there is not one single definition of AI. The Chamber notes that defining, or trying to define, AI can influence the path of future research and policy. We therefore urge the Agencies to remain flexible in their approach to AI and other developing financial technologies.

We appreciate the Agencies' engagement and interest in how technological advancements are affecting financial institutions and customer engagement. It is important that the Agencies have a holistic understanding of how financial institutions use AI to inform their oversight. To that end, we hope the RFI will be used as a genuine opportunity to discuss how technology can and should be used to improve the financial system.

The Chamber believes that SR 11-7: "Guidance on Model Risk Management" ("SR 11-7") is broadly applicable to AI and addresses many of the questions raised by the Agencies in the RFI.⁴ SR 11-7 instructs banking organizations to be attentive to the possible adverse consequences (including financial loss) of decisions based on models that are incorrect or misused, and should address those consequences through active model risk management. SR 11-7 further provides detailed guidance on "model development, implementation, and use," "model validation," and "governance, policies, and controls" that can be used by financial institutions as they manage risks that may be associated with the use of AI. The banking industry often relies on SR 11-7 to conduct thorough model risk management to help alleviate potential increased risks posed by AI.

The Chamber also believes it is important for the Agencies to be broadly aware of other policy developments across the federal government as they relate to AI. It is important for the Agencies to remain coordinated and consistent in their approach for regulating the financial sector. Agencies must also remain cognizant of how any standards they develop could impact

² The U.S. Chamber of Commerce (2019, September 23). Principles on Artificial Intelligence. <https://americaninnovators.com/news/u-s-chamber-releases-artificial-intelligence-principles/>

³ Vought, R. T. (2020, November 17). Memorandum for Heads of Executive Departments and Agencies: Guidance for Regulation of Artificial Intelligence Applications. Office of Management and Budget. <https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-06.pdf>

⁴ Federal Reserve Board of Governors. (2011, April 4). SR 11-7: Guidance on Model Risk Management. <https://www.federalreserve.gov/supervisionreg/srletters/sr1107.html>

other sectors outside of their jurisdiction. There may be lessons that the Agencies can draw from other governmental entities, or elsewhere in the private sector, to avoid a disjointed approach to policymaking regarding AI. Such an approach would lead to competing and conflicting standards that could impede innovation.

The Chamber wishes to provide the below feedback on the following topics raised by the RFI:

- I. Coordinated and Consistent Oversight of AI Across the Federal Government
- II. Explainability (Q. 1-3)
- III. Risks from Broader or More Intensive Data Processing and Usage (Q. 4-5)
- IV. Overfitting (Q. 6)
- V. Cybersecurity Risk (Q. 7)
- VI. Dynamic Updating (Q. 8)
- VII. Oversight by Third Parties (Q. 10)
- VIII. Fair Lending (Q. 11-16)
- IX. Additional Considerations (Q. 16-17)

I. Coordinated and Consistent Oversight of AI Across the Federal Government

The Agencies should coordinate with OMB to ensure that any policymaking related to artificial intelligence is consistent with the 2020 OMB Memorandum. As a general-purpose technology, AI can be used in a wide range of contexts and sectors. Consequently, the oversight of AI applications will cross multiple regulators.

The Chamber endorses the approach taken by the OMB Memorandum that seeks to establish a comprehensive regulatory approach to AI through outlining common principles for the responsible governance of AI applications. Importantly, the OMB Memorandum incorporates several broad themes including scrutinizing the impact of potential AI regulations on economic growth and competitiveness, focusing on non-regulatory alternatives, such as pilot projects and voluntary consensus standards, and taking a risk-based approach accounting for the full suite of costs and benefits. While the Chamber supports sectoral oversight of AI applications, interagency coordination and consistency are necessary to share best practices, ensure common definitions and concepts when practicable, and prevent duplication or overlap. Consequently, the OMB Memorandum applies to all federal agencies, including independent regulatory agencies, to help advance this objective. The Chamber strongly suggests that the Agencies adhere to OMB Memorandum to the greatest extent practicable to comply with its requirements, including the mandatory production of agency plans to provide transparency into Agencies' activities.

In addition to the OMB Memorandum, the Agencies should also prioritize intergovernmental cooperation in other contexts that implicate the governance of commercial AI applications. Some of these include the White House Office of Science Technology Policy's interagency committee to implement the National Artificial Intelligence Initiative and the

National Institute of Standards Technology’s (“NIST”) work on AI standards and best practices such as the AI risk management framework.

II. Explainability (Q. 1-3)

The RFI refers to explainability as “how an AI approach uses inputs to produce outputs” and notes “some AI approaches can exhibit a ‘lack of explainability’ for their overall functioning (sometimes known as global explainability) or how they arrive at an individual outcome in a given situation (sometimes referred to as local explainability).” While there is no broadly accepted definition for “explainability,” there is a common understanding that AI explainability relates to how humans can understand how a model generates a certain output or outcome, and whether the output or outcome merits close review or scrutiny.

Overall, the Chamber believes that the degree of explainability for AI systems will differ depending on several factors including context, the degree of risk, and the user type involved (e.g. consumer, regulator). Not all AI applications pose risk, or the same risks. Consequently, not all AI applications will need to be explainable to all user types. Explainability may also be catered to different audiences depending on the level and type of interaction with the model. Data scientists who regularly interact with the model may benefit from more detailed information while other stakeholders would benefit from different or simpler explanation of how the model operates.

Financial institutions are committed to improving methods to address conceptual soundness, and they already have substantial experience identifying and mitigating any such risks. Effective model risk management systems can help financial institutions protect consumers by ensuring that they understand, and can explain, how the AI they employ function as appropriate to the use case. Techniques to explain or interpret models have improved significantly in recent years, and this trajectory is expected to continue as financial institutions continue their investments. The Agencies should not issue any broad-based guidance regarding explainability, however. Financial institutions are already highly regulated as it relates to AI and explainability: for example, they are subject to Supervisory Guidance on Model Risk Management.⁵ This guidance is principles-based and applicable to the risks regarding explainability. The Chamber encourages the Agencies to engage in dialogue with the academic communities, industry, and other organizations researching explainability.

III. Risks from Broader or More Intensive Data Processing and Usage (Q. 4-5)

The RFI points out there may be risks from broader or more intensive data processing and usage due to AI, but the Agencies must also recognize there are numerous benefits. For example, the RFI notes that AI may use alternative datasets in certain applications. In the case of credit underwriting, AI can be used to expand lending to individuals with no/limited credit profiles, including those in underserved communities.

In July 2020, lead policymakers at the CFPB issued a blog post, “Innovation spotlight: providing adverse action notices when using AI/ML models.”⁶ The blog post notes “AI may have a profound impact” in credit underwriting. Specifically, the blog post references a 2015 “Credit Invisibles Data Point issued by the CFPB before stating, “AI has the potential to expand credit access by enabling lenders to evaluate the creditworthiness of some of the millions of consumers who are unscorable using traditional underwriting techniques. These technologies typically involve the use of models that allow lenders to evaluate more information about credit applicants.” It points out some of the fair lending risks regarding the explainability of AI models, which are addressed in Section IX of our comments.

Non-traditional data is very effective at filling in the gaps left by traditional data as it relates to rendering decisions regarding credit-worthiness. The U.S. Chamber of Commerce issued a report in 2021, “*The Economic Benefits of Risk-Based Pricing for Historically Underserved Consumers in the United States*” finding, among other things, that companies are innovating and using alternative data to reduce the credit-invisible population and improve credit scores for those who currently have them. The report also found that incorporating more predictive data into pricing models generates positive economic benefits, especially for underserved populations.⁷ An Organization for Economic Co-operation and Development (OECD) study revealed that underserved populations including minorities and low-income groups in the U.S. benefit from having more information incorporated into credit decisions.

As the amount of data increases, risk management approaches adapt appropriately. Financial institutions can apply Supervisory Guidance on Model Risk Management to manage the risks from broader or more intensive data processing and usage that may result from using AI, including for analyzing large data sets using alternative data. The Supervisory Guidance on Model Risk Management appropriately notes, “As is generally the case with other risks, materiality is an important consideration in model risk management. If at some banks the use of models is less pervasive and has less impact on their financial condition, then those banks may not need as complex an approach to model risk management in order to meet supervisory expectations.”

IV. Overfitting (Q. 6)

The RFI correctly notes that overfitting is not unique to AI, but can be more pronounced in AI than with traditional models. Overfitting can be managed appropriately as a part of well-established model risk management procedures consistent with the Supervisory Guidance on Model Risk Management. While the risk of AI should be evaluated and accounted for in the

⁶ Ficklin, P., Pahl, T., & Watkins, P. (2020, July 7). Innovation spotlight: Providing adverse action notices when using AI/ML models. <https://www.consumerfinance.gov/about-us/blog/innovation-spotlight-providing-adverse-action-notices-when-using-ai-ml-models/>.

⁷ Pham, N. D., & Donovan, M. (2021, Spring). The Economics of Risk-Based Pricing for Historically Underserved Consumers in the United States. The U.S. Chamber of Commerce. https://www.centerforcapitalmarkets.com/wp-content/uploads/2021/04/CCMC_RBP_v11-2.pdf.

context of its use case, there are some generally accepted practices that are being implemented by financial institutions to appropriately manage the risk of overfitting.

V. Cybersecurity Risk (Q. 7)

Cybersecurity risks are not unique to AI and financial institutions already adhere to applicable guidance. Information security standards, policies, and procedures apply to AI just in the same way they apply to other technologies. The RFI points out that AI “may be exposed to risk from a variety of criminal cybersecurity threats,” but there have not been any significant cybersecurity incidents reported specifically related to the use of AI. This is not to say there are no cybersecurity risks, but that practices presently used by financial institutions have been effective. These risks are similar to other emerging technologies and can be managed accordingly.

Financial institutions are subject to the Gramm-Leach-Bliley Act⁸ and adhere to issuances from the Federal Financial Institutions Examinations Council and NIST as it relates to cybersecurity. Financial institutions are committed to robust cybersecurity protections and dedicate vast resources to ensure their data – including the data used in AI models – is protected. AI -based cybersecurity tools, notable for their speed and accuracy, may be deployed to prevent, detect, and remediate compromise of information systems containing training data and ML models

VI. Dynamic Updating (Q. 8)

The Chamber is encouraged by the RFI distinguishing between the risks for static AI models and models that make use of dynamic updating. It is important to distinguish between models which are trained online, i.e. real-time, in live use, and models which are updated offline (i.e. when not in live use) often with guardrails. The Chamber does not consider such “offline” updating to be dynamic updating.

Dynamic models can bring certain benefits but may require additional or different controls than non-dynamic models such as more regular monitoring and/or guardrails. The Supervisory Guidance on Model Risk Management is sufficiently flexible to address dynamic updating.

The Chamber encourages the Agencies to work collaboratively with financial institutions to understand the risks it has identified for dynamic AI models. Financial institutions primarily rely on non-dynamic AI models at this time, but as innovation accelerates, it is very likely they will more regularly make use of dynamic models where helpful and appropriate. The Agencies should provide an open-door to understand the benefits and risks of dynamic models.

⁸ 12 C.F.R. pt. 30, App. B.

VII. Oversight of Third Parties (Q. 10)

Financial institutions have extensive experience with managing oversight of third parties and adhere to well-established third-party risk management guidance. Effective third-party risk management processes can control for risks from AI in similar ways as they have controlled for risks for other emerging technologies. Financial institutions require a certain degree of visibility into vendor's models to appropriately account for risk.

SR 11-7 applies to both internal and third-party models. Specifically, it states, "Whenever a banking organization uses *external resources [emphasis added]* for model risk management, the organization should specify the activities to be conducted in a clearly written and agreed-upon scope of work, and those activities should be conducted in accordance with this guidance." Additionally, the Federal Reserve Board has issued "Guidance on Managing Outsourcing Risk," which supplements existing guidance on technology service provider (TSP) risk, that "describe the elements of an appropriate service provider risk management program."⁹

The OCC recently published, "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29," which specifically addresses risk management when using a third-party model or when using a third party to assist with model risk management.¹⁰ On this topic, the OCC states, "The principles in OCC Bulletin 2013-29 are relevant when a bank uses a third-party model or uses a third party to assist with model risk management, as are the principles in OCC Bulletin 2011-12, 'Sound Practices for Model Risk Management: Supervisory Guidance on Model Risk Management.' Accordingly, third-party models should be incorporated into the bank's third-party risk management and model risk management processes."

The FDIC has also issued guidance that "provides a general framework that boards of directors and senior management may use to provide appropriate oversight and risk management of significant third-party relationships."¹¹ The FDIC evaluates activities conducted through third-party relationships as though the activities were performed by the institution itself.

VIII. Fair Lending (Q. 11-16)

Regarding fair lending, the RFI notes that "there may be uncertainty about how less transparent and explainable AI approaches align with applicable consumer protection legal and regulatory frameworks, which often address fairness and transparency."¹² We agree that consumer protection is an important consideration, but caution against attempting to broadly interpret laws designed for credit products to a specific technology. As noted elsewhere in the

⁹ Federal Reserve Board of Governors. (2013, December 5). Guidance on Managing Outsourcing Risk. <https://www.federalreserve.gov/supervisionreg/srletters/sr1319a1.pdf>

¹⁰ Office of the Comptroller of the Currency. (2020, March 5). OCC Bulletin 2010-10 - Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29. <https://www.occ.gov/news-issuances/bulletins/2020/bulletin-2020-10.html>

¹¹ Federal Deposit Insurance Corporation. (2008, June 6). Financial Institution Letters: Guidance for Managing Third-Party Risk. <https://www.fdic.gov/news/financial-institution-letters/2008/fil08044.html>

¹² See RFI, 86 Fed. Reg. at 16841

RFI, and within this letter, AI contributes significant benefits to consumers, and a rigid regulatory framework runs the risk of stifling future benefits that have yet to be realized.

Financial institutions are aware of and many are supervised for their obligations under these consumer protection laws, including the applicability of these laws to their use of artificial intelligence. Compliance management systems currently expected of financial institutions for managing and fair lending risk are applicable to AI-based credit approaches. SR 11-7 is also applicable.

The Chamber appreciates the inclusion of Question 15 in the RFI which notes there may be a lack of regulatory clarity regarding adverse action notices for credit under the Equal Credit Opportunity Act (ECOA) and the Fair Credit Reporting Act (FCRA) as it relates to AI. Regulation B requires a creditor, when denying credit or taking other adverse action, to provide an adverse action notice to an applicant and provide or make available upon request a statement of the specific reasons for the action taken.¹³ The RFI rightly recognizes that models using AI raise new questions about how credit providers can meet this obligation under Regulation B.

The Chamber recommends that the CFPB work with credit providers to assist them with understanding how to meet their obligations under Regulation B and FCRA to provide adverse action notices when making use of AI for credit decisions.¹⁴ The Chamber agrees with a statement in a 2020 blog post from the CFPB that, “The existing regulatory framework has built-in flexibility that can be compatible with AI algorithms.” However, guidance through avenues such as the CFPB’s “tech sprints” may be helpful – this is a pro-innovation approach to policymaking. The CFPB recently launched its first tech sprint to help improve consumer adverse action notices.¹⁵ This exercise brought together regulators, software providers, consumer groups, and financial entities to collaborate on ideas to inform policy options for electronically-delivered actions notices.

IX. Additional Considerations (Q. 16-17)

Finally, it is worth mentioning some of the other additional uses of AI by financial institutions that benefit consumers, businesses, and the overall financial system. As already discussed, AI can expand access to credit, especially for analyzing large data sets including alternative data, but has many other benefits to consumers. AI is being used by financial institutions to improve the consumer experience as it relates to marketing, servicing, and fraud detection, and is also being used by financial institutions to meet their anti-money laundering obligations under the Bank Secrecy Act.

AI improves the consumer experience by assisting financial institutions with the marketing of products. Using AI, financial institutions can improve their understanding of the

¹³ 12 C.F.R. § 1002.9

¹⁴ Chang, A., Lambert, T., & Lasiter, J. (2020, September 1). CFPB’s first tech sprint on October 5-9, 2020: Help improve consumer adverse action notices. <https://www.consumerfinance.gov/about-us/blog/cfpb-tech-sprint-october-2020-consumer-adverse-action-notice/>

¹⁵ Ibid.

types of products consumers need. They can then use targeted marketing to improve consumer awareness of these opportunities. Similarly, AI can be used to reduce friction for the origination process and servicing given it can assist with confirming a consumer's identity, employment status, income, and other information. AI is also used in servicing departments. For example, speech recognition technology is used in call centers by financial institutions to assist with verifying a customer's identity.

AI makes it possible for financial institutions to analyze large sums of data to detect and prevent fraud in real time. Financial institutions have been analyzing data for fraud detection for decades but have been able to significantly expand their capabilities as new AI tools have been developed. Fraud detection models benefit from the experience of reviewing millions or even billions of examples that consist of both legitimate and illegitimate transactions. This analytical capability enables financial institutions to alert customers about fraudulent activity that may be happening on their account.

Finally, the application of AI can be used by financial institutions to detect money laundering and comply with their obligations under the Bank Secrecy Act. As noted in the background information of the RFI on "flagging unusual transactions," AI is used by financial institutions to identify potentially suspicious, anomalous, or outlier transactions for Bank Secrecy Act/anti-money laundering investigations.¹⁶

The Agencies recently issued a "Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing," extolling the benefits of artificial intelligence.

*"Some banks are also experimenting with artificial intelligence and digital identity technologies applicable to their BSA/AML compliance programs. These innovations and technologies can strengthen BSA/AML compliance approaches, as well as enhance transaction monitoring systems. The Agencies welcome these types of innovative approaches to further efforts to protect the financial system against illicit financial activity. In addition, these types of innovative approaches can maximize utilization of banks' BSA/AML compliance resources."*¹⁷

The Financial Crimes Enforcement Network (FinCEN) has begun shifting towards a risk-based approach to preventing money laundering. On September 17, 2020, FinCEN issued an ANPR on "Anti-Money Laundering Program Effectiveness" with the stated purpose to "provide financial institutions greater flexibility in the allocation of resources and greater alignment of priorities across industry and government, resulting in the enhanced effectiveness of and efficiency of anti-money laundering (AML) programs." Reforms, such as those outlined in this ANPR, would enable financial institutions to assist law enforcement with responding to and

¹⁶ See RFI, 86 Fed. Reg. at 16839

¹⁷ FRB, FDIC, FinCEN, NCUA, OCC. (2018, December 3). Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing. Financial Crimes Enforcement Network. https://www.fincen.gov/sites/default/files/2018-12/Joint%20Statement%20on%20Innovation%20Statement%20%28Final%2011-30-18%29_508.pdf.

preventing money laundering, through leveraging new technology, such as artificial intelligence and machine learning, to identify illicit activity.¹⁸

* * * * *

We appreciate the Agencies' interest in the use of AI by financial institutions. The technology holds significant promise for enhancing the operations of financial institutions and increasing opportunities for consumers. As is true with any new technology, we urge the Agencies to be flexible in their regulatory approach, so innovation is not unnecessarily stifled. To that end, we would encourage the Agencies to closely engage with financial institutions as they consider the need for policy clarifications. We thank you for your consideration of these comments and would be happy to discuss these issues further.

Respectfully,



Bill Hulse
Vice President
Center for Capital Markets Competitiveness



Jordan Crenshaw
Vice President
Chamber Technology Engagement Center

¹⁸ Hulse, B. (2020, November 16). Anti-Money Laundering Program Effectiveness – FinCEN-2020-0011 – RIN 1506- AB44. Center for Capital Markets Competitiveness. U.S. Chamber of Commerce.
<http://www.centerforcapitalmarkets.com/wp-content/uploads/2020/11/CCMC-Comment-Letter-FinCEN-ANPR-Final-11.16.20.pdf?#>.